NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

The Cyber Security Order 706 Version 5 CIP Drafting Team thanks all commenters who submitted comments on the first formal posting of Project 2008-06 - CSO706 Version 5 CIP Standards. These standards were posted for a 60-day public comment period from November 7, 2011 through January 6, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 131 sets of comments, including comments from approximately 294 different people from approximately 191 companies representing all 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:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html

Note: In March 2012, in consideration of the extremely large volume of comments received during the formal comment period and initial ballots that ended January 6, 2012, the Standards Committee authorized the following:

Waive the requirement that the Cyber 706 SDT provide individual responses and direct the team to focus on providing detailed summary responses to each question subject to the following conditions:

- *Each summary response should address the comments submitted, in aggregate, such that the summary response clearly addresses all of the comments submitted.*
- *As part of the Consideration of Comments report, add a paragraph that clarifies that the drafting team developed summary responses rather than individual responses with the approval of the Standards Committee and invite any stakeholder who believes his or her comment was not adequately addressed to submit a written request for additional clarity within 15 calendar days [of the posting date] to the team's advisor with a commitment that the team will provide a written response within 15 calendar days. (The standards staff will post any requests for additional clarity and associated responses on the project's web page.)*
- *When the standards staff posts the revised standards for stakeholder comment, staff will include in the announcement the same offer to provide stakeholders with a more detailed response and commitment to publicly post these requests and associated responses.*

If you feel that your comment has been overlooked, please let us know immediately. Special instructions for submitting a request for additional clarification were provided in the announcement of this posting, which is posted on the project page. 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 of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

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	Connie Lowe	Dominion	X		X		X	X				

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

2.	Group	Brian Millard	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Larry Akens			1
2.	Ian Grant			3
3.	David Thompson			5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
4. Marjorie Parsons		6										
3. 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.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
5.	Brian Evans-Mongeon	Utility Services	NPCC	8
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	Chantel Haswell	FPL Group, Inc.	NPCC	5
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1
10.	Michael Lombardi	Northeast Utilities	NPCC	1
11.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
12.	Bruce Metruck	New York Power Authority	NPCC	6
13.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
14.	Rogert Pellegrini	The United Illuminating Company	NPCC	1
15.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
16.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
17.	Saurabh Saksena	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.	Donald Weaver	New Brunswick System Operator	NPCC	2

4.	Group	Brent Ingbrigtson	PPL Corporation	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda Truhe	PPL Electric Utilities Corp.	RFC	1
2.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	WECC	5
3.	Mark Heimbach	PPL EnergyPlus	MRO	6
4.	Annette Bannon	PPL Generation, LLC on behalf of its NERC Registered Entities	RFC	5
5.	Mark Heinbach	PPL EnergyPlus, LLC	NPCC	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
6. Mark Heinbach	PPL EnergyPlus, LLC	SERC 6										
7. Mark Heinbach	PPL EnergyPlus, LLC	SPP 6										
8. Mark Heinbach	PPL EnergyPlus, LLC	RFC 6										
9. Mark Heinbach	PPL EnergyPlus, LLC	WECC 6										
5. Group	Lesley Bingham	SPP RTO and listed members		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.		Sunflower Electric Power Company	SPP	
2.		Nebraska Public Power District	SPP	
3.		Grand River Dam Authority	SPP	

6. Group	Steve Alexanderson P.E.	Pacific Northwest Small Public Power Utility Comment Group			X	X				X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dave Proebstel	Clallam County PUD No.1	WECC	3
2.	Russell A. Noble	Cowlitz County PUD No. 1	WECC	3, 4, 5
3.	Ronald Sporseen	Lincoln Electric Cooperative	WECC	3
4.	Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC	3
5.	Ronald Sporseen	Central Electric Cooperative	WECC	3
6.	Ronald Sporseen	Consumers Power	WECC	1, 3
7.	Ronald Sporseen	Clearwater Power Company	WECC	3
8.	Ronald Sporseen	Douglas Electric Cooperative	WECC	3
9.	Ronald Sporseen	Fall River Rural Electric Cooperative	WECC	3
10.	Ronald Sporseen	Northern Lights	WECC	3
11.	Ronald Sporseen	Lane Electric Cooperative	WECC	3
12.	Ronald Sporseen	Raft River Rural Electric Cooperative	WECC	3
13.	Ronald Sporseen	Lost River Electric Cooperative	WECC	3
14.	Ronald Sporseen	Salmon River Electric Cooperative	WECC	3
15.	Ronald Sporseen	Umatilla Electric Cooperative	WECC	3
16.	Ronald Sporseen	Coos-Curry Electric Cooperative	WECC	3
17.	Ronald Sporseen	West Oregon Electric Cooperative	WECC	3
18.	Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC	3, 4, 8
19.	Ronald Sporseen	Power Resources Cooperative	WECC	5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
7.	Group	Bob Case - NERC Compliance Manager (605) 721-2716	Black Hills Corporation Registered Entities (NCR00089, NCR05030, NCR05031 & NCR11186)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	NCR00089 (BHCE)		WECC	1, 3, 4, 5, 6
2.	NCR05030 (BHP)		WECC	1, 3, 4, 5, 6
3.	NCR05031 (BHW)		WECC	5
4.	NCR11186 (BHCI)		WECC	5

8.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tino Zaragoza	IID	WECC	1
2.	Jesus Sammy Alcaraz	IID	WECC	3
3.	Diana Torres	IID	WECC	4
4.	Marcela Caballero	IID	WECC	5
5.	Cathy Bretz	IID	WECC	6

9.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Glen Chason	EPRI		
2.	Scott Sternfeld	EPRI		
3.	Andrew Wright	N-Dimension Security		
4.	Chan Park	N-Dimension Security		
5.	Dan Widger	N-Dimension Security		
6.	Stacy Bresler	NESCO		
7.	Carol Muehrcke	Adventium Enterprises		
8.	Josh Axelrod	AlertEnterprise!		
9.	Mladen Kezunovic	TLI		
10.	Tomo Popovic	TLI		
11.	Art Conklin	University of Houston		
12.	Elizabeth Sisley	Calm Sunrise Consulting		
13.	Annabelle Lee	EPRI		
14.	Marc Child	Great River Energy		

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
15. Scott Hughes	Great River Energy											
10. Group	Will Smith	MRO NSRF										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	OPPD	MRO	1, 3, 5, 6
2.	Chuck Lawrence	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.	Alice Ireland	XCEL	MRO	1, 3, 5, 6
7.	Dave Rudolph	BEPC	MRO	1, 3, 5, 6
8.	Eric Ruskamp	LES	MRO	1, 3, 5, 6
9.	Joe Deporter	MGE	MRO	3, 4, 5, 6
10.	Scott Nickels	RPU	MRO	4
11.	Terry Harbour	MEC	MRO	1, 3, 5, 6
12.	Marie Knox	MISO	MRO	2
13.	Lee Kittelson	OTP	MRO	1, 3, 4, 5
14.	Tony Eddleman	NPPD	MRO	1, 3, 5
15.	Mike Brytowski	GRE	MRO	1, 3, 5, 6
16.	Richard Burt	MPC	MRO	1, 3, 5, 6

11.	Group	Rick Terrill	Luminant					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brad Jones	Luminant Energy	ERCOT	6
2.	Mike Laney	Luminant Generation		5

12.	Group	Ronnie Hoeinghaus	City of Garland			X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Billy Lee		ERCOT	3
2.	Heather Siemens		ERCOT	3

13.	Group	Michael Quinn, Chair	Members Representative Committee	X	X	X		X		X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Soles	Occidental Power Services	ERCOT	5
2.	Bruce Wertz	Wertz & Associates, Inc.	ERCOT	5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Pam Zdenek	Sweetwater Wind 2 LLC	ERCOT 5										
4. Jose Escamillia	CPS Energy	ERCOT 9										
14. Group	Tim Hattaway	PowerSouth CIP Review Team				X	X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Craig Kilpatrick		SERC										
2. Mark Dayton		SERC										
3. Brian Fleming		SERC										
4. Jon Harrison		SERC										
5. Greg Hataway		SERC										
15. Group	Roger Powers	CWLP	X		X		X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Steve Rose		SERC	5									
2. Shaun Anders		SERC	1									
16. Group	Emily Pennel	Southwest Power Pool Regional Entity										X
ditional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.		Sunflower Electric Power Company	SPP									
2.		Nebraska Public Power District	SPP									
3.		Grand River Dam Authority	SPP									
17. Group	Mary Jo Cooper	ZGlobal on behalf of City of Lodi, City of Ukiah, Alameda Municipal Power, Salmon River Electric Coop, California Pacific Electric Company			X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Katie Spence	Salmon River Electric Coop	WECC	3									
2. Colin Murphey	City of Ukiah	WECC	3									
3. Douglas Draeger	Alameda Municipal Power	WECC	3									
4. Sam Rohn	California Pacific Electric Coop	WECC	3									
5. Elizabeth Kirkley	City of Lodi	WECC	3									
18. Group	David Batz	Edison Electric Insititute	X				X					
http://www.eei.org												

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
19. Group	Michael Mertz	PNM Resources (Includes Public Service Co. of New Mexico and Texas New Mexico Power	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Laurie Williams	Public Service Co. of New Mexico	WECC	1
2.	Roger Dickens	Texas New Mexico Power	ERCOT	1
3.	Michael Mertz	PNM Resources	WECC	3

20.	Group	Kevin Cyr	Seattle City Light	X		X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dana Wheelock	Seattle City Light	WECC	3
2.	Pawel Krupa	Seattle City Light	WECC	1
3.	Hao Li	Seattle City Light	WECC	4
4.	Dennis Sismaet	Seattle City Light	WECC	6
5.	Mike Haynes	Seattle City Light	WECC	5

21.	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.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
3.	Jim Howard	Lakeland Electric	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

22.	Group	Steve Rueckert	Western Electricity Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brent Castagnetto	WECC	WECC	10
2.	Liz Brereton	WECC	WECC	10
3.	Don Pape	WECC	WECC	10

23.	Group	Jason Marshall	ACES Power Marketing Member Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. Bill Hutchison	Southern Illinois Power Cooperative	SERC	1, 3, 5, 6									
2. James Jones	AEPCO/SWTC	WECC	1, 5, 6									
3. Bob Solomon	Hoosier Energy	RFC	1, 3, 5, 6									
4. Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4, 5, 6									
5. Patrick Woods	East Kentucky Power Cooperative	SERC	1, 3, 5, 6									
6. Lindsay Shepard	Sunflower Electric Power Corporation	SPP	1, 3, 5, 6									
7. Mohan Sachdeva	Buckey Power	RFC	4, 5, 6									
8. Shari Heino	Brazos Electric Power Cooperative	ERCOT	1, 3, 5									
24. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Steve Osvath	FE	RFC	
2.	Cindy Sheehan	FE	RFC	
3.	Tim Sheerer	FE	RFC	
4.	Mary Jane Linn	FE	RFC	
5.	Dan Irwin	FE	RFC	
6.	Mark Koziel	FE	RFC	
7.	Troy Rhoades	FE	RFC	
8.	Betsy Hostert	FE	RFC	
9.	Peter Buerling	FE	RFC	
10.	Nathaniel Maier	FE	RFC	
11.	Larry Raczkowski	FE	RFC	
12.	John Olszewski	FE	RFC	
13.	Nathan Sterritt	FE	RFC	
14.	Don Miller	FE	RFC	
15.	David Griffin	FE	RFC	
16.	Ken Dresner	FE	RFC	
17.	Jim Simpson	FE	RFC	
18.	Robert Loy	FE	RFC	
19.	Ron Ross	FE	RFC	
20.	Phil Bowers	FE	RFC	
21.	Heather Herling	FE	RFC	
22.	Vicki Magni	FE	RFC	

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
25.	Group	Andrew Gallo, Chair	NERC Standards Review Subcommittee - ERCOT Region			X		X				X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Soles	Occidental Power Services	ERCOT	5
2.	Bruce Wertz	Wertz & Associates, Inc.	ERCOT	5
3.	Pam Zdenek	Sweetwater Wind 2 LLC	ERCOT	5
4.	Jose Escamillia	CPS Energy	ERCOT	9

26.	Group	Scott Harris	Kansas City Power & Light	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jennifer Flandermeyer	Kansas City Power & Light	SPP	1, 3, 5, 6
2.	Michael Gammon	Kansas City Power & Light	SPP	1, 3, 5, 6
3.	Alan Kloster	Kansas City Power & Light	SPP	1, 3, 5, 6
4.	Dean Larson	Kansas City Power & Light	SPP	1, 3, 5, 6
5.	Tony Mann	Kansas City Power & Light	SPP	1, 3, 5, 6
6.	Monica Strain	Kansas City Power & Light	SPP	1, 3, 5, 6
7.	Paul Schiemege	Kansas City Power & Light	SPP	1, 3, 5, 6
8.	John Breckenridge	Kansas City Power & Light	SPP	1, 3, 5, 6

27.	Group	Paul M. Skare	Paul Skare, et al									X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	A. David McKinnon	Pacific Northwest National Laboratory	NA - Not Applicable	9
2.	Samuel L. Clements	Pacific Northwest National Laboratory	NA - Not Applicable	9

28.	Group	Marianne Swanson	Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)									X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Victoria Yan Pillitteri	Booz Allen Hamilton	NA - Not Applicable	NA
2.	David Dalva	Booz Allen Hamilton	NA - Not Applicable	NA

29.	Group	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
No additional members listed.													
30.	Group	Christine Hasha	ISO/RTO Council Standards Review Committee		X								

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Charles Yeung		SPP	SPP	2									
2. Al DiCaprio		PJM	RFC	2									
3. Marie Knox		MISO	RFC	2									
4. Ben Li		IESO	NPCC	2									
31.	Group	Donald Brookhyser	EPUC, CAC and NCA										
No additional members listed.													
32.	Group	Travis Metcalfe	Tacoma Power			X							
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Chang Choi	Tacoma Power	WECC	1									
2.	Keith Morisette	Tacoma Power	WECC	4									
3.	Mike Hill	Tacoma Power	WECC	6									
4.	Max Emrick	Tacoma Power	WECC	5									
33.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
34.	Individual	John Souza	Turlock Irrigation District			X							
35.	Individual	Richard Malloy	Idaho Falls Power			X		X					
36.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
37.	Individual	Ed Croft	Puget Sound Energy	X		X		X					
38.	Individual	John.Brockhan@CenterPointEnergy.com	CenterPoint Energy	X									
39.	Individual	Ed Nagy	LCEC CIP Team	X		X							
40.	Individual	Patricia Lynch	NRG Energy Inc.	X				X					
41.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
42.	Individual	Cynthia Oder	Salt River Project	X		X		X	X				
43.	Individual	Summer C. Esquerre	Corporate Compliance	X		X		X	X				
44.	Individual	James Eckelkamp	Progress Energy	X		X		X	X				
45.	Individual	Scott Bordenkircher	Arizona Public Service Company	X		X		X	X				
46.	Individual	Doug Peterchuck	Omaha Public Power District	X		X		X	X				
47.	Individual	Jennifer Wright	San Diego Gas & Electric	X		X		X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
48.	Individual	Roger Pan	Emerson Process Management										
49.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
50.	Individual	Tom Bowe	PJM		X								
51.	Individual	Chris Higgins / BPA CIP Team	Bonneville Power Administration	X		X		X	X				
52.	Individual	Daniel Duff	Liberty Electric Power, LLC					X					
53.	Individual	Joanna Luong-Tran	TransAlta Centralia Generation					X					
54.	Individual	Mario Lajoie	Hydro-QuÃ©bec TransÃ‰nergie	X									
55.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
56.	Individual	Dan Roethemeyer	Dynegy					X					
57.	Individual	J. S, Stonecipher, PE	City of Jacksonville Beach dba/Beaches Energy Services	X									
58.	Individual	Thomas Lyons	Owensboro Municipal Utilities			X							
59.	Individual	Randy Hahn	Ocala Utility Services	X									
60.	Individual	Tracy Richardson	Springfield Utility Board			X							
61.	Individual	Kirit Shah	Ameren	X		X		X	X				
62.	Individual	Aliza Dewji P.Eng	ATCO Power Canada Ltd.										
63.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
64.	Individual	Thomas M. Haire, P.E.	Rutherford EMC			X	X						
65.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
66.	Individual	Saurabh Saksena	National Grid	X		X							
67.	Individual	MIchael Johnson	APX Power Markets								X		
68.	Individual	Scott Bos	Muscatine Power and Water	X		X		X	X				
69.	Individual	Robin W. Blanton	Piedmont EMC			X							
70.	Individual	Marc Child	Great River Energy	X		X		X	X				
71.	Individual	Michael Falvo	Independent Electricity System Operator		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
72.	Individual	Rodney Luck	Los Angeles Department of Water and Power	X		X		X	X				
73.	Individual	Jack Stamper	Public Utility District No. 1 of Clark County	X									
74.	Individual	Paul Crosby	Platte River Power Authority	X		X		X	X				
75.	Individual	Nathan Smith	Southern California Edison	X		X		X	X				
76.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)										
77.	Individual	William O Thompson	NIPSCO Northern Indiana Public Service Company	X		X		X	X				
78.	Individual	Curt Wilkins	Douglas County PUD No.1				X	X					
79.	Individual	Brenda Frazer	Edison Mission Marketing & Trading	X				X					
80.	Individual	David Kiguel	Hydro One Networks Inc.	X		X							
81.	Individual	Michelle Denike	Wolverine Power Supply Cooperative, Inc.	X									
82.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
83.	Individual	Michael Schiavone	Niagara Mohawk (National Grid Company)			X							
84.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
85.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
86.	Individual	John Bee	Exelon	X		X		X					
87.	Individual	David Martorana	Tenaska, Inc.					X					
88.	Individual	Robert Solomon	Hoosier Energy	X		X		X					
89.	Individual	Tracy Sliman	Tri-State G&T Inc.	X									
90.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
91.	Individual	Rich Vine	California ISO		X								
92.	Individual	Richard Salgo	NV Energy	X		X		X	X				
93.	Individual	John Martinsen	Public Utility District No. 1 of Snohomish County	X		X	X	X	X				
94.	Individual	Bo Jones	Westar Energy	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
95.	Individual	Bruce Metruck	New York Power Authority	X		X		X	X				
96.	Individual	Edward Bedder	Orange and Rockland Utilities Inc.	X		X							
97.	Individual	Thad Ness	American Electric Power	X		X		X	X				
98.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
99.	Individual	David Burke	Orange and Rockland Utilities, Inc.	X		X							
100.	Individual	Martin Kaufman	ExxonMobil Research and Engineering	X				X					
101.	Individual	Mikhail Falkovich	PSEG	X		X		X	X				
102.	Individual	David Dockery	Associated Electric Cooperative, Inc	X		X		X	X				
103.	Individual	Shari Heino	Brazos Electric Power Cooperative, Inc.	X				X					
104.	Individual	Joe Tarantino	Sacramento Municipal Utility District	X		X	X	X	X				
105.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
106.	Individual	Andrew Z. Pusztai	American Transmission company, LLC	X									
107.	Individual	David S. Revill	Georgia Transmission Corporation	X									
108.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
109.	Individual	John Tolo	Tucson Electric Power	X									
110.	Individual	Tony Eddleman	Nebraska Public Power District	X		X		X					
111.	Individual	Mark B Thompson	Alberta Electric System Operator		X								
112.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric Company					X					
113.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
114.	Individual	Don Jones	Texas Reliability Entity										X
115.	Individual	Roger Fradenburgh	Network & Security Technologies Inc								X		
116.	Individual	Kevin Koloini	AMP				X						
117.	Individual	Nathan Mitchell	American Public Power Association			X							
118.	Individual	Greg Rowland	Duke energy	X		X		X	X				
119.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
120.	Individual	Richard Powell	JEA	X		X		X					
121.	Individual	Rebecca Moore Darrah	MISO		X								
122.	Individual	Michelle D'Antuono	Ingleside Cogeneration LP					X					
123.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
124.	Individual	Christine Hasha	Electric Reliability Council of Texas, Inc.		X								
125.	Individual	Gregory Campoli	New York Independent System Operator		X								
126.	Individual	David Grubbs	City of Garland	X									
127.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									
128.	Individual	Jose H Escamilla	CPS Energy	X		X		X					
129.	Individual	Adam Menendez	Portland General Electric	X		X		X	X				
130.	Individual	Scott Miller	MEAG Power	X		X		X					
131.	Individual	Maggy Powell	Constellation Energy on behalf of Baltimore Gas and Electric, Constellation Power Generation, Constellation Commodities Group and Constellation Energy Control and Dispatch	X		X		X	X				

Summary Consideration and Common Responses to Issues and Comments Frequently Repeated in Q1-Q49

There were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than responding separately in each question, the SDT addresses many of those general comments here, while noting that submission of a comment only once by an entity, or repeated multiple times by that same entity in response to several questions, did not influence the manner in which the SDT considered the issue.

Measures

Some commenters had questions about the measures in the Version 5 standards, particularly regarding the use of "must" versus "may," and why there were differences of use in certain instances. The SDT tried to make a distinction by using the word, "must" for instances where the Responsible Entity "must" have something as evidence – variations are not expected to be acceptable. This would be the case for a requirement that says the Responsible Entity "shall" have a documented procedure – the entity must have that procedure to demonstrate compliance. Where the requirement says the Responsible Entity shall implement a documented procedure, then that entity must have the procedure. Since there are typically many ways of demonstrating "how" an entity has implemented a procedure, the word "may" has been used ahead of samples of performance that may be acceptable.

Furthermore, some commenters noted that some measures appeared technology specific, or specified that something must be "dated." The SDT tried to craft requirement language that speaks to results or to particular capabilities, without being technology specific; yet, the SDT fully realizes that certain technologies exist that serve to meet the requirements. The intent of any specific type of technology listed in the measures, which is generally limited, is to provide a non-inclusive example of high-quality evidence. The SDT contemplates that technology will change, and it did not want to specify certain technologies in the requirement language. Similarly, the word "dated" in the measure reflects a characteristic of high-quality evidence, but its use in the measure does not imply any additional obligation to the Registered Entity.

Initial occurrence of periodically required performance

In several instances in the Version 5 requirements, the SDT indicated certain periodic performance requirements, and they specified in the first posted draft's requirement language that the first iteration must be performed "initially upon

the effective date." Several commenters raised concerns with this language, and they suggested that not all initial performances should occur upon or before the effective date. The SDT agrees, and it has evaluated each periodic performance requirement. Furthermore, it has removed "initially upon the effective date" throughout the standards, and references to the initial performance in the requirements have been moved to the Implementation Plan as a separate section.

Technical Feasibility Exceptions

Some commenters asked whether the Technical Feasibility Exception ("TFE") process in the NERC Rules of Procedure, Appendix 4D, will be revised upon changes made to these standards. The SDT notes that requirements that require the submission of a TFE are identified in the NERC Rules of Procedure, and changes to that document are outside of the scope of this SDT. Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a TFE when alternative measures are implemented. It is expected that the NERC TFE process will be modified to specify which requirements of Version 5's standards will require TFE submissions once the standards are finalized and submitted to the Commission.

Other commenters were concerned that "where technically feasible" suggests that an entity may unilaterally decide that a requirement does not apply, without filing a TFE. The SDT respectfully notes that entities are required to be compliant with all NERC reliability standards applicable to their function and Facilities. In some cases compliance is demonstrated by showing that the entity has no applicable assets; in other cases compliance is demonstrated through the TFE process. In no case does any language in a NERC reliability standard grant an exemption from compliance to applicable Responsible Entities.

Confidentiality of evidence used to demonstrate compliance

Some commenters questioned how they could demonstrate compliance when the subject matter may be high risk or confidential; inquiring how the SDT ensures that data will be protected. While outside the scope of this SDT, the SDT notes that the audit process requires strict adherence by auditors to confidentiality, which is part of the compliance process.

"As a minimum" and similar phrases

There were comments that suggested that phrases similar to "as a minimum" are not necessary; however, the SDT uses "as a minimum," e.g., in certain cases to distinguish from the concept of "exactly and no more," which the SDT does not intend. The SDT notes that most input to the drafting process by observers and through informal comment on this topic suggests that such a distinction is necessary for audit purposes.

Applicability

Some commenters asked for clarification on whether the rest of the Version 5 requirements applied if there was no determination of classification under CIP-002-5. The SDT intends that if a Responsible Entity determines that it does not have any BES Cyber Systems that meet CIP-002-5, Attachment 1 criteria, most of CIP-003-5 through CIP-011-1 would not apply to them (*but see* CIP-003-5, Requirement 2, as modified for the next formal comment period). Furthermore, applicability throughout CIP-004-5 through CIP-011-1 varies depending on BES Cyber System categorization under CIP-002-5, Attachment 1. Note, however, that BES Cyber Systems not categorized as 'high' or 'medium' impact are 'low' impact under CIP-002-5, Attachment 1. Responsive to FERC Order No. 706's directives concerning the NIST model, the Version 5 CIP standards require that all levels, including 'low' impact, receive some level of cyber security protection. Those are now programmatically covered under CIP-003-5, Requirement 2, in the next draft; so the SDT encourages each entity to evaluate carefully whether the standards apply to its own facts and circumstances.

Many commenters raised concerns over how the first draft of the Version 5 standards addressed low impact BES Cyber Systems. As discussed in the immediately preceding paragraph, the SDT agrees and notes that in the next posting of the CIP Version 5 standards, the 'low' impact requirements will be grouped together as one policy requirement, CIP 003-5, Requirement 2. The requirement specifies that Responsible Entities must address 'low' impact BES Systems at the policy/program level. Furthermore, and in recognition of the very significant volume of assets anticipated to be classified as "low impact," that requirement will be handled separately via the Implementation Plan, allowing approximately three years (one year longer than the rest of the requirements) for implementation.

The SDT notes that moving the 'low' impact requirements to one standard, along with extending the implementation period, mitigates some of the concern regarding costs to implement Version 5, particularly for smaller entities. The SDT has attempted to tailor requirements focused on results and a culture of security in support of reliability, and it believes that the system-level scoping throughout the requirements helps to accomplish that.

As to applicability, in response to several commenters' concerns, the SDT has modified the applicability sections of all of the CIP Version 5 standards so that they are consistent.

One entity repeated in almost all questions concern over the lack of an exemption in the Version 5 standards for smaller entities. With respect, the SDT emphasizes that there has never been an "exemption" specifically for small entities. In some cases, compliance can be achieved by taking an "exception" (e.g., non-routably connected assets) to the CIP standards, or by falling below compliance registry thresholds. However, Section 215 of the Federal Power Act does not allow exemptions from any reliability standards by anyone who qualifies as a "user, owner, or operator" of the "bulk power system." The proposal by the drafting team includes all BES Cyber Assets as in scope, but provides for

programmatic requirements for 'low' impact BES Cyber Systems, and accounts for gradated rigor or reach of the requirements for 'medium' impact assets, particularly between those with a routable connection and those without. Furthermore, the SDT has modified the standards so that CIP-004 through CIP-011 only applies to Responsible Entities having 'high' or 'medium' impact BES Cyber Systems. The policy-level requirements in CIP-003-5 still apply to all Responsible Entities. This, in part, addresses the directive in the FERC Order No. 706, Paragraph 25, to consider applicable features of the NIST Risk Management Framework, where it is fundamental that all BES Cyber Systems receive some level of protection.

Requirements for Documentation

Some commenters suggested that the Version 5 standards should not have any documentation requirements. In general, the SDT has endeavored to remove or minimize requirements that exist solely for purposes of creating documentation. However, there are other factors that support the use of requiring documentation in certain instances. The SDT has attempted to strike the appropriate balance. The SDT notes that many NERC standards require some level of procedure documentation to support the pre-thought responses to known conditions, or to ensure consistent responses when known events happen. Furthermore, certain documentation is essential to measure what needs to be secured. The SDT has sought to minimize such documentation requirements, and it has tried to provide detailed guidance. However, guidance alone is not a sufficient place for such documentation needs, as guidance is not mandatory nor enforceable.

Evidence Retention

Some commenters raised concerns about the evidence retention periods in the standards; to include concern that they are not the same as those in Version 4, that they increase the period from one to three years, or that they have a general misunderstanding over retention when the period between compliance audits may exceed the frequency stated. The evidence retention periods in the compliance section of the standards have been modified to make clear the expectation from the CMEP that entities have compliance evidence for the entire audit period. Furthermore, in some cases, compliance retention is different than records retention for the purpose of security analysis. The "requirement" level retention, where applicable, relates to maintaining records long enough to analyze them for security purposes, anomalous behavior, etc. The "compliance" retention, as specified in the Compliance section of the standard, deals with demonstrating that the requirement has been met (e.g., to demonstrate that the entity has maintained a "rolling" 90-day set of logs throughout the entire compliance audit period where the requirement specifies logging for 90 days). With respect to increases in the evidence retention periods from one to three years, the SDT notes that the initial evidence retention language pre-dates the establishment of the compliance program and its associated documented procedures. The NERC Rules of Procedure require that entities must "demonstrate compliance" for the entire compliance period (not that they must maintain all records for the entire compliance period). Note the distinction between demonstrating

compliance and maintaining all records noted in the requirements (e.g., again, to maintain records for 90 days for security analysis vs. demonstrating that records have been kept for a rolling 90-day period for an entire compliance period, whether three or six years).

'Annual' vs. 15 months

The SDT believes that some entities misunderstood the SDT's approach with respect to the SDT's attempt to provide flexibility to the industry on requirements that generally must be completed approximately every 12 months. Rather than specify exactly 12 months (or 365 days, etc.), which would create a very inflexible rolling period that would not allow for exception because of operational concerns, and which would not necessarily allow the use of a calendar reminder on the same day each year (e.g., because of weekends on the first or last day of the period), the SDT uses a convention of once per calendar year, not to exceed 15 months between occurrences. The SDT created this convention particularly because it appreciates the reality in implementing periodic requirements, and it believes that a short grace period beyond a strict 12 months makes the most sense. Nevertheless, some entities expressed concern that it would be difficult to implement a requirement on a 15-month period, that merely "annual" was preferred, or that the SDT should allow the convention explained in the CAN on the topic to govern.

The SDT believes that it has created a time convention that is practical and flexible. First, with respect to CANs, the CAN addressing "annual," CAN-0010, should not be necessary for Version 5, and the standards always supersede a CAN if different. As a general rule, a drafting team should always seek to provide sufficient clarity, such that using a CAN is not necessary. Thus, the SDT anticipates that CAN-0010's guidance on "annual" will not be applicable for these standards.

Next, the actual performance specified in the requirement language allows for the required performance to be performed generally on a 12-month cycle, which is not inconsistent with using a calendar reminder on the same date each year. The SDT included the 15-month time reference, however, specifically for the purpose of providing flexibility to Responsible Entities so that something that is generally accomplished on a 12-month schedule will not be in non-compliance if operating conditions, holidays, etc., cause the next period to occur slightly more than 12 months since the previous iteration. The alternative is an approach that does not contain such flexibility. In contrast, merely once per calendar year, or just "annually," allows for bookending that the SDT believes is contrary to reliability, as intervals that are too long affect the ability of the activity to protect reliability. Consider this example → Year 1 performance: January 1; Year 2 performance: December 31; Year 3 performance: January 1; Year 4 performance: December 31. In that example, the strict "once per calendar year" has been accomplished, and one might argue that the activity occurred "annually;" but in practice, almost 2 years elapse before immediate, quick succession performance in Years 2 and 3, and so on. The intent of the SDT is to accomplish these "annual" type performances on a schedule that approximates once every 12 months, while allowing some semblance of flexibility so that the requirement does not strictly require 365 days

between performances. There is absolutely and emphatically no preclusion in the standards for a Responsible Entity to harmonize its performance of these requirements to once every 12 months in a manner that makes the most sense to it (for example, every March 1), as long as the performance is accomplished once per calendar year, but not more than 15 months between occurrences. In this manner, the SDT has created a time parameter so that an entity can do precisely what some commenters suggest: automate a calendar reminder at the same time each year. But that same calendar reminder will not result in noncompliance if, for example, it falls on a Saturday and the Responsible Entity does not complete the performance until the next Monday; or during operational conditions for which conducting the performance risks instability, etc., the Responsible Entity waits until the operational condition has passed.

Definitions

Some commenters expressed a desire to maintain all legacy definitions in Version 5 on the basis that new terms require entities to dedicate resources in modifying existing policies, procedures, and evidence. The SDT appreciates this concern, and it has reevaluated changes to terms and reverted to previous terms in some cases. For example, the SDT has eliminated the "Defined Physical Boundary" term used in the initially-posted draft, and it reverted to the currently in-use "Physical Security Perimeter" term, albeit with a new definition for that term. However, the significant changes in response to addressing fully all of the remaining FERC Order No. 706 directives, along with adopting key features of the NIST risk management framework, do result in a paradigm shift in Version 5. To that end, and, for example, in the case of "Critical Cyber Asset" used in Versions 1 through 4, the conceptual changes in moving to "BES Cyber Assets" and "BES Cyber Systems" enable a more granular and appropriate scoping in Version 5 that render the use of the "Critical Cyber Asset" model inapplicable.

Consideration of NERC Quality Review Feedback

In addition to reviewing stakeholder-provided comments and modifying the standards in response to that consideration, the SDT submitted the ten standards and associated documents for a NERC Quality Review ("QR") in preparation for posting the draft Version 5 standards for formal comment and successive ballot. As a result of QR feedback, the SDT made substantive changes to improve the standards as described in the following paragraphs. The SDT also made several QR-suggested clarifying changes to conform grammar, style, and consistency throughout the standards, which are not individually described (e.g., rewording, consistency or terms, synchronization of Measures to Requirements, synchronizing listed rationales to Requirements and Requirement parts, hyphenation of certain words, numbering corrections to numbered lists, minimizing passive language, usage of commas in table references, confirming correct time horizons, typographical and grammatical corrections, updated Guidelines and Technical Basis sections of the standards, and other suggestions that are not as substantive in nature as the topics in the paragraphs that follow).

The QR noted that the mapping to previous versions, the VRF/VSL justifications, and the Version 5 Consideration of Issues and Directives documents were not complete. In response, the SDT revised those documents for accuracy and to match the revisions that accompany this posting.

The QR identified that the evidence retention sections of the standards varied and were not consistent with the suggested language in the Quality Review Background Document. In response, the SDT clarified the evidence retention periods and made that section consistent in all ten standards. In particular, the SDT clarified that for non-compliance, a Responsible Entity shall keep information related to the non-compliance "until mitigation is complete and approved . . ." as opposed to "until found compliant." The SDT also clarified that the evidence retention periods apply "for each requirement in the standard" for each standard.

The QR inquired about the CIP Cyber Security Standards' applicability to NERC and the Regional Entities. Specifically, NERC and the Regional Entities will not have any Facilities identified in CIP-002-5, attachment 1. Even though applicability to NERC and the Regional Entities would presumably be for purposes of protecting information submitted by the industry, because NERC or the Regional Entities are not users, owners, or operators of the bulk power system, that protection is not accomplished through application of the CIP standards. Rather, that protection is found in NERC's Rules of Procedure, Section 1500, and such protection applies regardless of applicability of the CIP standards to NERC or the Regional Entities. Since the Rules of Procedure provide for the protection that the SDT intended in originally proposing applicability to NERC and the Regional Entities, the SDT modified the standards' applicability sections to remove NERC and the Regional Entities.

The QR also identified language in the applicability section that referenced "required by a NERC or Regional Reliability Standard," where it was unclear whether the phrase applied to a protection system or to Transmission. The SDT clarified that the "required by . . ." language is in reference to a protection system.

The applicability qualifiers for Distribution Providers ("DPs") and Load-Serving Entities ("LSEs") were the same as those qualifiers in the Facilities section of the applicability sections. For clarity and brevity, the applicability qualifier for DPs and LSEs now reference the appropriate and corresponding Facilities reference rather than duplicating it. There are also many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes clarify and ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.

In response to QR and industry comments, the SDT also reworked most of the VSLs in the standards. In general, and as described in the VSL question summaries, the SDT explains that it tried significantly to align the VSL language with the requirement language, and it also thoroughly reviewed binary VSLs to make them graduated where possible.

QR identified that the portions of the Background section of the standards explaining the applicability of the table items could be improved. Specifically, reference to mere "applicability" was potentially confusing, as there is an "Applicability" section of the standards. The SDT clarified in each instance that it means the "Applicability Columns in Tables," distinct from "applicability" of each standard as a whole. The SDT reviewed usage of applicability terms in the tables, and the SDT lists in the "Applicability Columns in Tables" section only those BES Cyber Systems and associated Cyber Assets for which a particular standard's tables apply. The SDT also moved the phrase relating to implementing common controls for multiple high and medium impact BES Cyber Systems from the "High Impact BES Cyber System" explanation into the more general background narrative.

The SDT clarified the purpose statements in all ten of the CIP standards in response to QR to clarify the reliability purpose of each standard. The SDT used the feedback from QR to reevaluate each standard in order to make each purpose statement conform to the correct style and form while specifying each standard's reliability-related benefit and tie to reliability principles.

In CIP-003-5, the QR identified several phrases that were unnecessary and unenforceable (e.g., "represents the Responsible Entity's commitment to the protection of . . ."). The SDT agreed and removed those phrases.

Removal of Restoration Facilities from CIP-002-5, Attachment 1's Medium Impact Rating (M)

The SDT notes that it has removed restoration facilities from CIP-002-5, Attachment 1's "Medium Impact Rating (M)" category. The SDT made this decision after receiving input from commenters, from industry, and following discussions about the issue as presented to NERC's Operating and Planning Committees. The SDT learned that Blackstart Resources face reduction because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool. Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed. The SDT explains this change in more detail in the Guidelines and Technical Basis section of the posted draft CIP-002-5.

QUESTION 1 - Definitions:

Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement.

SUMMARY:

The SDT modified all of the definitions based on stakeholder comments. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

BES Cyber Asset

Commenters requested that the drafting team consider revising the definition of BES Cyber Asset to consider the Facility the Cyber Asset is associated with, and the SDT has made changes to the definition to clarify that point.

Commenters noted concern that the term "adversely impact" is not well defined, and in response the SDT has made changes to the definition to further qualify this term with impact on the reliable operation of the BES.

Some commenters noted that the drafting team should consider removing the statement, "A Maintenance Cyber Asset is not considered part of a BES Cyber System," from the definition of BES Cyber System, since the definition of a BES Cyber Asset excludes Transient Cyber Assets, and modify the statement to exclude Transient Cyber Assets or to define "Maintenance Cyber Asset." In response, the SDT has removed undefined terms from the definition, and it has included the description of these devices as part of the definition itself. (Note that the SDT also removed "Transient Cyber Asset" as a defined term).

Commenters asked about the phrase "unavailable, degraded, or misused." These describe states of a BES Cyber Asset which could result from a Cyber Security Incident. Unavailable means that the BES Cyber Asset is unable to perform the service it is providing to the BES Facility, System, or equipment. Degraded means that it is able to provide the service, but in a degraded way (below specified capabilities). Misused means that it is being used for a purpose other than its designed use.

Commenters also asked about the phrase “when required.” The phrase “when required” is used in the context of a BES Cyber Asset: It is meant to distinguish between the time of the cyber security compromise, which could be earlier than the actual operation, misoperation, or nonoperation. The phrase means the time of the actual operation, misoperation, or non-operation when it is required to perform its designed operation. The drafting team has made changes to the definition which no longer uses this term, but uses “when needed” instead.

With respect to the 15-minute threshold, some commenters asked whether there is a need for a 15-minute test to “verify” the impact of the BES, and, if so, how an entity would demonstrate compliance. Furthermore, some commenters requested removal of the criterion. The SDT notes that, in using 15 minutes, it is attempting to articulate a time boundary for “Real-time” impact. The term “Real-time” in the Glossary of Terms used in NERC Reliability Standards did not provide enough specificity in the definition for this purpose. The SDT scoped the CIP standards to those Cyber Assets that would have an effect on Real-time operations. Misoperation or non-operation of systems that do not have a Real-time impact provide enough time for operators of the BES to perform mitigating, compensating, or corrective action to counteract the compromise. Some commented on the use of “could” versus “would” too, and the drafting team has discussed the use of both terms and has determined that the term “would” is the more appropriate term.

Some commenters requested removal of the second and third sentence in the previously posted definition of BES Cyber Asset because they do not provide clarity to the time frame stated above. The SDT has clarified and simplified the definition.

Some commenters noted concern with the applicability as applied to UFLS devices when those devices would not be BES Cyber Assets. The SDT notes that Section 4 specifies Facilities, Systems, and equipment. In the case of UFLS/UVLS, they include Elements (equipment) that provide the reliability tasks that are necessary to perform the functions of a Distribution Provider or Load Serving Entity, all tasks necessary for the reliability of the BES. The BES Cyber Assets are those Cyber Assets that support these elements for this function.

Commenters noted that the definition included a time frame qualifier that references sending or receiving "instructions to operate," and that such qualifier is too narrow (entities may take the stance that the BES Cyber Asset must be directly involved in a supervisory control function and would eliminate non-supervisory control systems, including those providing situational awareness, from designation as a BES Cyber Asset). The time frame qualifying term is no longer used in the amended definition.

Some commenters asked for changes from a perceived conflict that the third sentence that describes the 15-minute time frame relies on the asset being operational, yet the first sentence states that the asset may be rendered unavailable. The 15 minutes describes the time from the non-operation or Misoperation and the resulting impact on the BES. The

definition has been amended to clarify the distinction.

Some commenters noted concern with the definition's absence of "BES" relative to Reliability Operating Services, and the SDT notes that the term has been removed from the definition. BES Reliability Operating Services is no longer a defined term and has been moved to the Guidelines and Technical Basis section.

Some commenters asked for "BES Cyber Asset" to reinstate the phrase, "and causes a Disturbance to the BES" that was in earlier drafts approved by the SDT to clarify the phrase "adversely impacts." In response, the SDT reviewed the definition of Disturbance in the NERC Glossary and determined that the term was too broad for use in this context.

Commenters noted that the definition of BES Cyber Asset also includes a statement that redundancy shall not be considered when determining availability, and that the statement should be modified. The definition has been amended to use impact.

Commenters asked that the BES Cyber Asset definition take into consideration redundant systems in determining availability. The clause has been clarified to specify that redundancy is not used to determine impact. The purpose of the clause is to determine whether these systems are scoped in because of their "Real-time" impact. The Guideline and Technical Basis section discusses why redundancy is not considered for the purpose of cyber security vulnerability; and, therefore, the need for cyber security protection.

Some commenters asked for clarification on whether the drafting team's intent is for the definition to include auxiliary assets related to Facilities where the assets reside (e.g., Fire systems, HVAC, Halon system, etc.). In response: No, these do not directly support (BES) Facilities, Systems, and equipment that perform a BES reliability function. They may be included, however, if they meet qualification for other types of Systems that must be protected under CIP (e.g., in the same ESP).

Some commenters asked for a different category for assets that can be misused versus those that can only be rendered inoperable. The SDT notes that, from the impact determination standpoint, it does not make a difference whether they are unavailable or misused: Each has a potential and different impact that determines its categorization with the high watermark principle (worst impact).

Many commenters proposed the SDT abandon this definition and revert back to the existing Critical Cyber Asset term and its definition. The term Critical Cyber Asset was used in Versions 1, 2, 3, and 4 in an "in or out" paradigm. Version 5 uses a multilevel categorization where the use of this legacy term is inappropriate.

In various other capacities, some commenters indicated difficulty understanding certain aspects of the definition. The SDT notes that the definition has been amended since the last formal comment period in response to comments, and the

SDT believes that it is now simpler and clearer.

Some commenters asked the SDT to add the statement, "Support Systems, such as voice communication (e.g., 900 MHz radio System), ventilation, power supply systems, and similar supporting systems are not considered BES Cyber Assets." However, these do not directly support (BES) Facilities, Systems, and equipment that perform a BES reliability function. They may be included if they meet qualification for other types of Systems that must be protected under CIP (e.g., in the same ESP).

Based on these comments, the SDT has revised the definition as follows:

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation~~, when required~~, adversely impact one or more ~~BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in~~Facilities, Systems, or equipment, which~~ that~~, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation ~~occurs and impacts~~of the ~~BES~~Bulk Electric System. Redundancy of affected Facilities, Systems, and equipment shall not be considered when determining ~~availability.~~ adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A ~~Transient~~Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset ~~is not considered~~ within an ESP, or to a BES Cyber Asset~~.~~, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber Security Incident

For BES Cyber Security Incident, most individuals or organizations that commented indicated an overall vagueness of the definition because of the terms "attempt to disrupt" and "suspicious event." They commented that these terms are too subjective. In response, we note the proposed definition does not significantly modify the glossary definition. In addition, we are reverting to the previous term "Cyber Security Incident" based on other commenter feedback and to align with the EOP-004-2 drafting effort. There is not at this time a compelling need to significantly modify or introduce new terminology in the existing definition. The triggering langue, "disrupt or attempt to disrupt," must also be read in context with the qualifying phrase of "a malicious act or suspicious event." While this does not provide absolute certainty in the compliance evidence to demonstrate whether or not an act or event was a Cyber Security Incident, there must always be a degree of subjectivity in the entity's understanding of what constitutes a BES Cyber Security Incident.

Based on these comments, the SDT has revised the definition as follows:

~~BES~~ Cyber Security Incident

~~Any~~A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset,~~ or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System~~, or~~.
- ~~Results in unauthorized physical access into a Defined Physical Boundary .~~

BES Cyber System

Commenters noted concern with the distinction between BES Cyber Asset and BES Cyber System, and that the similarities created confusion between what is a "System" and what is an "asset." Furthermore, there was confusion over whether each BES Cyber Asset must be part of a BES Cyber System, or if BES Cyber System can include other assets or communications equipment. The SDT has thoroughly reviewed all comments on the issue, and it amended both definitions to make them clearer. The SDT has also made the relationship between BES Cyber Assets and BES Cyber Systems clearer. Additionally, it is now clear that every BES Cyber Asset must be part of a BES Cyber System. Whether the BES Cyber System includes Cyber Assets and communication equipment depends on how the BES Cyber System is defined. The Responsible Entity has discretion on how BES Cyber Assets are grouped, as long as they meet the definition of a BES Cyber System; including the option of defining BES Cyber Systems that only include a single BES Cyber Asset.

Some commenters noted that the loss of Critical Assets removes Facilities from consideration, presenting challenges in assessing BES Cyber Systems as they provide services to a Facility which provides BES Reliability Operating Services - not the BES Cyber System independently. The SDT notes that BES Reliability Operating Services is no longer a defined term, and the SDT has removed it (referencing functional tasks of the functional entity instead). Furthermore, for clarity, the definition of BES Cyber Asset now includes Facilities, Systems, and equipment as part of the definition.

Finally, some commenters noted concern with how one determines if Cyber Assets are "typically grouped together," particularly in the rapidly evolving security field, and they noted the absence of logical groupings in the definition. The definitions of both BES Cyber Assets and BES Cyber Systems have been modified for better clarity and include the concept of logical grouping to support a reliability functional task by a functional entity.

Based on these comments, the SDT has revised the definition as follows:

One or more BES Cyber Assets ~~that are typically grouped together,~~ logically ~~or physically,~~grouped by a responsible

entity to ~~operate~~perform one or more ~~BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System~~reliability tasks for a functional entity.

BES Cyber System Information

The SDT received several comments about the definition of BES Cyber System Information, and a primary concern was that "BES Cyber System Impact" was not a defined term. The SDT agrees and modified "impact" to be lower case. Additionally, the SDT received numerous concerns about specific items included in the list of items that defined BES Cyber System Information. A few comments, however, pointed out that there was not, in fact, a definition, but only a list of examples. The SDT agreed and modified the definition clarifying that BES Cyber System Information includes information "…that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."

Based on these comments, the SDT has revised the definition as follows:

> Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.~~Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.~~

BES Reliability Operating Services

Several commenters commented that BES Reliability Operating Service needs more information for clarity as a defined term; that it is too broad, or that it uses language that many unintentionally result in overreach of the standards. Several commenters also asked for clarification of several components, whether the time horizons (which are in the NERC document "Time Horizons") or with particulars of several of the specifically listed services. Commenters also noted that

there needed to be clarity in the relationship to its use of terms with the functional model. In response, BES Reliability Operating Services is no longer a defined term, and has been moved to the Guidelines and Technical Basis section as guidance for Responsible Entities. The SDT has included in the definitions of BES Cyber Assets and BES Cyber Systems the concept that each BES Cyber Asset must be part of a BES Cyber System, and the relationship of the BES Cyber System with reliability functional tasks for functional entities. Situational analysis and decision making would be initially scoped as components necessary for the functional tasks and will be further scoped by the "Real-time" operations filter in the definition of BES Cyber Assets.

CIP Exceptional Circumstance

The SDT received a small number of comments regarding the definition of CIP Exceptional Circumstances. These comments consisted of requests for additional circumstances to be added to the definition. The SDT appreciates that it cannot be sure of all situations that may arise. As such, it has modified the definition to more closely tie it to safety and BES reliability. Additionally, it has added the case of "an imminent or existing hardware, software, or equipment failure" in consideration of the comments from industry that equipment may fail in ways that are not planned.

Based on these comments, the SDT has revised the definition as follows:

> A situation that involves one or more of the following, or similar, conditions~~:~~ that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

The SDT received a number of comments indicating that the definition of CIP Senior Manager should reference the specific standards for which it is applicable. The SDT notes that the term is only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which is currently planned for retirement.

Control Center

Commenters were concerned that the definition was too broad, either generally, with respect to location, or by the inclusion of "by System Operators," and that the drafting team should clarify if it is the intent to only include the Control Center with the primary responsibility for maintaining reliability of the BES and performing one or more of the functions that support Real-time operations by System Operations. Other commenters were concerned about whether it only applies to BA, TOP, GOP, or RC, and that without specifying, it could unintentionally include certain field assets. The SDT

has modified and clarified the definition in response to these concerns by specifying, ". . . operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations."

Some commenters also expressed concern about use of "facilities" in lowercase. The SDT uses facility in the generic sense (not the NERC Glossary term) of a location or site, and then specifies the capitalized term "Facilities" with respect to Transmission Facilities or generation Facilities (as noted in the preceding paragraph.)

Some commenters were concerned about generation Facilities that control small remote units at different footprints being part of the definition (that the units collectively may be significantly under the 300 MW threshold, as indicated in 2.13, and present no risk to the BES). The SDT notes that generation Control Centers are only categorized as medium if they control an aggregate of more than 300 MW.

Some commenters noted that Transmission Owners do not have Control Centers (and that TOPs-have Control Centers). The SDT has modified the definition of Control Center to address this comment. The new definition does not include Transmission Owner, but does specify that it includes Control Centers performing the reliability functional tasks of a Transmission Owner: Transmission Owner Control Centers may be delegated certain tasks through agreements with Transmission Operators. (See Guideline and Technical Basis section.)

Some commenters asked the SDT to include "situational awareness" in the fourth item. Instead of adopting that specific suggestion, note that the SDT has made other modifications to the definition of Control Center that address this comment. The new definition now refers to the reliability functional tasks of BAs, RCs, TOPs, and GOPs.

Some commenters questioned whether Control Center needs to be defined, and were concerned about confusion with use of lowercase "control center" in other standards (e.g., EOP-008-1). Control Centers is used throughout all CIP standards. These terms are capitalized in the standards to refer to the proposed NERC Glossary defined term. Other standards use the generic term "control center," which does not refer to the (proposed) NERC Glossary defined term. Other standards can use the current proposed term in their future versions, or may make modifications subject to stakeholder vetting. The SDT expects that the defined term will not apply to standards that already use "control center" (lowercase) without this stakeholder vetting.

Based on these comments, the SDT has revised the definition as follows:

> One or more facilities hosting ~~a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions~~operating personnel that ~~support~~monitor and control the Bulk Electric System (BES) in real-time ~~operations by System Operators~~to perform the reliability functional tasks of: 1) a Reliability

Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more ~~BES~~locations, or 4) a Generation Operator for generation ~~facilities or transmission facilities,~~Facilities at two or more locations~~:~~

~~• Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,~~

~~• Inter-utility exchange of BES reliability or operability data,~~

~~• Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,~~

~~• Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,~~

~~• Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES~~

~~• Coordination of BES restoration activities~~.

Cyber Assets

Some commenters requested the term be singular, but the SDT notes that the term is already in the Glossary of Term used in NERC Reliability Standards.

Some commenters asked about "programmable" with respect to electronic device. The SDT notes that it is an electronic device which can execute a sequence of instructions loaded to it through software or firmware, and configuration of an electronic device is included in "programmable." Depending on the scheme used, these instructions may include data, or data that must be processed to execute these instructions.

Some comments expressed concern that the removal of "communication networks" from the definition might cause some to not include communication devices, or that the removal eliminates a protection of data in motion. There is no exclusion of communication devices in the definition. As long as the electronic device meets the definition, they are Cyber Assets. Furthermore, there is no specific requirement to protect data in motion within the Electronic Security Perimeter, hence no expectation of compliance to a requirement that does not exist. A FERC-approved interpretation addressed the specific case of separate physical security perimeters within an Electronic Security Perimeter, and it addresses the alternate physical protection measures required in CIP-006-3. Physical access requirements now apply to BES Cyber Systems.

Other commenters asked to retain "and communication networks" because of concern that any programmable device at

a location (e.g., within a substation) is a Cyber Asset regardless of whether they communicate to it or is used for communications, and that Cyber Asset devices that are not programmable via communications should be excluded. The SDT notes that any device that meets the definition is a Cyber Asset. The intent of the SDT is to include all such devices: Communication and connectivity considerations are included in the Applicability column of requirements and their parts, not the definition. Communications is not a pre-requisite for compromise of a Cyber Asset. However, note that BES Cyber Systems that do not have External Routable Connectivity are excluded from certain requirements.

Some commenters indicated that "Cyber Asset" should not include any portable memory devices such as USB memory devices, CDs, etc. The SDT notes that those are not specifically included unless they meet the definition of "Cyber Asset," including that they are programmable (i.e., capable of executing a set of instructions). Furthermore, commenters asked about legacy Remote Terminal Units (RTU's) with eproms, and they are typically considered programmable devices (programs/data are typically loaded into memory for execution).

Based on these comments, the SDT has revised the definition as follows:

> Programmable electronic devices~~, and communication networks~~ including the hardware, software, and data in those devices.

Defined Physical Boundary ("DPB")

The preponderance of the comments received on the term Defined Physical Boundary (DPB), indicated a preference to return to the more familiar industry term of Physical Security Perimeter (PSP). Although the drafting team initially chose DPB to help entities recognize the changes from the original PSP definition, the standards have been modified to use the original PSP term with a revised definition, and the proposed definition of DPB has been deleted. Even with the reversion to PSP, the drafting team wants to address the challenges with the completely enclosed "six-wall" border, especially in field locations, and the definition no longer retains the "six-wall" border concept. The intent of this definition change is to focus on the controls put in place to restrict access, rather than solely focusing on the PSP and a boundary protection model for physical security.

Based on these comments, the SDT has revised the definition of Physical Security Perimeter as follows:

> **Physical Security Perimeter ("PSP")**
> The physical~~, completely enclosed ("six-wall")~~ border surrounding ~~computer rooms, telecommunications rooms, operations centers, and other~~ locations in which ~~Critical Cyber Assets are housed and~~ BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Electronic Access Control or Monitoring Systems

Some commenters asked the SDT to split the definition to define electronic access control and electronic monitoring systems separately. Others commented to drop the "or monitoring" from the term. The SDT considered that approach but disagrees, as these Systems are grouped together for the purpose of requirement applicability. There are no requirements that would apply to one but not the other, therefore the SDT maintains the definition as one for simplicity. In all previous versions of the standards, these systems were called "Cyber Assets used in access control and monitoring." The SDT is simply taking this otherwise 'on the fly' definition of a class of assets within a requirement in Versions 1 through Versions 4 and making it a defined term for Version 5.

Some commenters asked the SDT to delete or remove the "or BES Cyber Systems" from the definition, as it is broader than the usage of the term in the standards and could imply applicability to low impact BES Cyber Systems. The SDT disagrees because a definition is just that: It is defining what an EACMS is, not providing the scope of requirements applied to the defined object. The scope of applicability of requirements is handled in each standard itself, not in the definition of the object. As previous versions had monitoring requirements in CIP-007 at the Cyber Asset level that continue in this version, we cannot remove this from the definition without reducing the scope of today's standards.

A few commenters thought the definition was too vague as to its scope and that it needs a comprehensive list or bright-line criteria. The SDT has taken this definition out of the requirements that have been in CIP-005 since Version 1. The SDT agrees that the term is broad, but reflective of its overall approach in Version 5, it is opposed to creating comprehensive lists of current technology items, as they can quickly become outdated. The SDT prefers to stick with a definition based on the function of the technology. The SDT addressed vagueness by changing the word 'used' to 'that performs,' and it added clarification that it is 'electronic access control' and 'electronic access monitoring' to clearly denote that the scope does not include all types of monitoring.

Based on these comments, the SDT has revised the definition as follows:

> Cyber Assets ~~used in the~~that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.

Electronic Access Point ("EAP")

Commenters noted concern with EAPs being an interface that restricts communication, and several comments suggested that the definition become more focused on 'crossing an ESP.' Many rightly pointed out that an EAP could be required for communications even between systems within an ESP, which was not the SDT's intent. The SDT agreed and has

rewritten the definition to focus on the fact that EAPs are Cyber Assets that reside on an ESP and allow communications across the ESP.

The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.

Several comments pointed out that the definition did not require ALL external communication interfaces to be included. It would be inappropriate to add this to the definition, as requiring EAPs and ESPs and specifying what they must do is in CIP-005-5, not in the definition of each term.

Based on these comments, the SDT has revised the definition as follows:

> ~~An~~ A Cyber Asset interface on ~~a Cyber Asset~~ an Electronic Security Perimeter that ~~restricts~~allows routable ~~or dial-up data communications~~communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

Most comments concerned the change to a 'collection of points' based definition for a 'perimeter' and asked for additional clarity. The SDT agreed and has rewritten the definition based on the legacy definition of a logical border. Several comments pointed out that the definition did not require ALL external communication interfaces to be included. It would be inappropriate to add this to the definition, as requiring EAPs and ESPs and specifying what they must do is in CIP-005-5, not in the definition of each term.

Based on these comments, the SDT has revised the definition as follows:

> The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled.~~
>
> ~~A collection of Electronic Access Points that protect one or more BES Cyber Systems~~.

External Connectivity

The comments indicated that there was confusion about the scope and use of External Connectivity, uncertainty surrounding whether the term included serial communication, and commenters concerns about the relationship between

External Connectivity and External Routable Connectivity. All uses of this term have been eliminated within the standards, and the proposed glossary term has been deleted completely.

External Routable Connectivity

Commenters noted concern that the definition took an "outside-in" only view of communications. The SDT has added the term 'bi-directional' to the proposed definition to clarify that any bi-directional communications path is included, regardless of the initiating side.

Commenters suggested that the SDT define 'routable protocol' and maintain a list of non-routable protocols, as per some of the NERC Guidelines. The SDT disagrees, as a guideline outside of the standards development process is the proper place to maintain such types of ever-changing information.

Based on these comments, the SDT has revised the definition as follows:

> ~~The~~A BES Cyber System that is accessible from ~~any~~a Cyber Asset that is outside its associated ~~ESP~~Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

Commenters' primary concerns regarding Interactive Remote Access were: 1) clarification of "interactive" access; 2) read-only remote access; and 3) ownership of Cyber Assets performing remote access.

Commenters noted concerns with the concept of asset ownership being included in the definition of Interactive Remote Access. The concept of asset ownership was included in the definition to provide an understanding that remote access is to have the appropriate protections applied, regardless of who owns or uses the system initiating the Interactive Remote Access session. Changes were made to the definition to add "use" along with owned. This is to assist those entities that lease equipment.

Comments were provided requesting a definition of "interactive" access. The definition of Interactive Remote Access has been updated to clarify that access is user-initiated access by a person. Interactive Remote Access has been clarified that this does not include system-to-system process communications. Additionally, the SDT updated the definition to use the term "routable" in the place of "network-based" to be more consistent with other requirements and definitions.

Commenters requested that read-only access to BES Cyber Systems be excluded from Interactive Remote Access. Because of the open channels that are needed, read-only access cannot be excluded.

Based on these comments, the SDT has revised the definition as follows:

~~Any~~All user ~~interactive~~ initiated access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether ~~network based~~routable or dial-up access~~.~~, using a client or remote access technology. Remote access ~~can~~may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate Device

Commenters noted concern over the location of the device. To clarify, the definition has been modified to require that the device must not be located inside the Electronic Security Perimeter. This allows for the appropriate termination of the required encryption and authentication prior to allowing access into the Electronic Security Perimeter.

Commenters also noted concern with the required protections of the Intermediate Device. The definition has been updated to specify that the Intermediate Device performs access control.

Additionally, comments were provided regarding the use of the terms DMZ and proxy. These terms have been removed.

Based on these comments, the SDT has revised the definition as follows:

A Cyber Asset ~~that 1) may be used to provide the required multi-factor authentication for the interactive remote~~or collection of Cyber Assets performing access~~; 2) may be a termination point for required encrypted communication; and 3) may~~ control to restrict ~~the interactive remote access~~ Interactive Remote Access to only authorized users. The Intermediate ~~devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may~~Device must not be located ~~outside~~inside the Electronic Security Perimeter~~, as part of the Electronic Access Point, or in a DMZ network.~~.

Physical Access Control Systems

There were not many comments received on this definition. Of those received, several were actually related to the use of the term "Defined Physical Boundary" in the definition, and that term has been changed back to Physical Security Perimeter. One comment indicated the definition was acceptable as written. Another comment asked for the inclusion of cameras in locally mounted exclusion list, but the drafting team believes this is not necessary since the list is not all-inclusive. However, the drafting team has further clarified the exclusion of locally mounted devices to only those that do not contain or store access control information or independently perform access authentication.

Based on these comments, the SDT has revised the definition as follows:

> Cyber Assets that control, alert, or log access to the ~~Defined~~ Physical ~~Boundary~~Security Perimeter(s), exclusive of locally mounted hardware or devices at the ~~Defined~~ Physical ~~Boundary~~Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Protected Cyber Asset

In limiting the definition to routable protocol connectivity, commenters suggested that relays and other devices in a substation or generating plant that are serially connected would not fall under this definition. The SDT agrees they would not be PCAs under this definition; however, such devices would be part of a BES Cyber System in and of themselves and not out of scope.

Some comments requested that this be defined as 'non-critical cyber assets'. The SDT believes this term is not descriptive enough, as every other Cyber Asset in existence could be considered a non-critical cyber asset. The SDT has chosen the term Protected Cyber Asset as a more descriptive term, as these are the Cyber Assets within an ESP, and by their proximity and direct connectivity to BES Cyber Systems, they must be protected in much the same way as the BES Cyber System itself.

The definition was also changed in response to comments concerning how to handle a mixture of varying impact BES Cyber Systems within a single ESP. The definition now considers all Cyber Assets connected with a routable protocol within an ESP that are not a part of the highest impact BES Cyber System to be PCAs of that BES Cyber System.

Based on these comments, the SDT has revised the definition as follows:

> A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System~~. A Transient~~ within the same Electronic Security Perimeter (a Cyber Asset is not ~~considered~~ a Protected Cyber Asset~~.~~ if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes).

Reportable BES Cyber Security Incident

For Reportable BES Cyber Security Incidents, many commenters did not agree with the referenced BES Reliability Operating Services definition. In response, we have replaced the term with "reliability tasks of a functional entity."

Based on these comments, the SDT has revised the definition as follows:

Reportable ~~BES~~ Cyber Security Incident

Any ~~BES~~ Cyber Security Incident that has compromised or disrupted ~~a BES Reliability Operating Service.~~ one or more reliability tasks of a functional entity.

Transient Cyber Asset

The SDT has removed this definition as a standalone term from the proposed glossary terms, and has included it as an aspect of the definition of BES Cyber Asset.

The intent was to take Cyber Assets that are temporarily connected to BES Cyber Systems and exclude them from becoming part of the BES Cyber System. The SDT agrees that TCAs pose some level of risk. However, the SDT believes that considering them as BES Cyber Assets is not the solution. These are normally portable maintenance and diagnostic tools, which by their very nature cannot meet all the requirements mandated for BES Cyber Assets, such as a fulltime physical security perimeter, or wiping all information when it is 'redeployed' to another location when the purpose for its existence may be to bring back field data for analysis. The SDT does not intend for the CIP requirements to make impossible or impractical normal practices that increase reliability of the BES, such as being able to use Cyber Asset based tools for diagnostics and maintenance, especially among numerous field assets.

The SDT, in an attempt to define 'temporarily connected,' has replaced that concept with 'less than 30 days' to give some measurable boundary to the term. The SDT acknowledges that there is no perfect definition that will cover every conceivable circumstance, such as the "one minute disconnect."

The SDT agrees that the 30-day time frame should be clarified; that it is 30 'consecutive' days, and has made the change. The SDT has also incorporated suggestions that the connections could be made not only to another Cyber Asset, but also to the network within the ESP.

The SDT believes external (not directly connected) Cyber Assets are addressed through CIP-005-5' EAP and Interactive Remote Access requirements. The SDT is focusing on those primarily maintenance and diagnostics devices that are indeed 'directly' connected to the system within the ESP.

Some commenters wanted more examples within the definitions. The SDT disagrees, as confusion regarding examples within definitions or requirements tend to be interpreted as prescriptive lists.

QUESTION 2 – CIP-002 Attachment 1:

CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Attachment 1. The explanations below describe the responses the drafting team provided to commenters, along with the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. The last section of this question's summary provides general comments for Question 2 along with the drafting team responses.

Criteria 1.1 to 1.4 (Control Centers)

One comment was that the Impact Rating of a control center should be linked to the Impact Rating of the facilities that the control center controls. If a control center only controls Low Impact facilities, it makes no sense for the control center to be rated at a Medium Impact Rating. The drafting team responded that, by definition, the Control Center controls more than one facility. For Transmission Control Centers, if the Control Center performs the functional obligations of a Transmission Operator, then it does so for more than a single facility and its impact is therefore more than a single Low Impact facility. The SDT believes that these Control Centers should be subject to the requirements for Medium Impact systems.

One commenter stated that it would be good to include some reference or example that relates to a Registered Entity that does not own generation, but provides services to those who do. The drafting team agreed and modified the definition of the Control Center to refer to real-time reliability tasks for applicable functional entities from the functional model, which includes those necessary for situational awareness.

Another suggestion was to delete " ... that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services ..." in the introduction of High Impact Rating, since the phrase is included in the definition. The drafting team responded that it agreed and included this suggested change in the new draft.

Another comment was that there is no explanation why a BES Cyber Asset (BES Cyber System) located at the Control Center would have higher impact than another BES Cyber Asset (BES Cyber System) located outside the Control Center.

The drafting team responded that a Control Center controls assets at more than one location. A compromise of the Control Center has the potential to impact multiple assets simultaneously, which means they have a higher potential impact on the BES.

Another comment was that a Control Center for very small BAs being High Impact is inappropriate. The drafting team agreed and included this suggested change in the new draft.

Another comment was that Transmission Owners do not have Control Centers and should be struck from Criterion 1.3. The drafting team agreed and included this suggested change in the new draft.

Another suggestion was to substitute the word "criteria" with the word "section" in Criterion 1.3 and 1.4 for clarity purposes. The drafting team agreed that clarity was needed and changed the language to use “parts” instead of “criteria”.

Another suggestion was that in criteria 1.3 and 1.4, the phrase “that includes” should be changed to “is limited to” in order to not leave these criteria completely unbounded. The drafting team responded that it believes that the language correctly conveys that the “functional obligations” must include the items specified for the criterion to apply. The proposed language implies that the functional obligations are limited to the items specified.

Another commenter noted that there appeared to be an error in category 1.4 where it references 2.12 (UFLS and UVLS). To match version 4 the cross-reference should be to 2.11 (Special Protection Systems). The drafting team agreed and included this suggested change in the new draft.

Another comment was to change the phrase "...that includes control of one or more of the assets..." in criterion 1.4 to match the definition of Control Center, which requires the control of two or more assets. The drafting team responded that the definition of the Control Center requires control of 2 or more assets irrespective of their impact rating. An additional qualifying criterion for a MW threshold of 1500 has been included as well. Criterion 1.4 will result in the categorization of High if at least one of those assets meets the qualifications specified.

Another commenter stated that the definition of BES Cyber System that can impact BES Reliability Operating Services would force the inclusion of RTU’s, Governors, Power System Stabilizers and Protective Relaying. The drafting team responded that it agreed that it is intended that these types of devices (RTUs, relays, etc.) are included if they meet the definition of BES Cyber Assets.

Another commenter stated that the High Impact Rating criteria do not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. BES Cyber Assets and BES Cyber Systems that interconnect with similar systems in other Control Centers should be afforded a High Impact Rating regardless of the

"span of control" of other BES Cyber Assets and BES Cyber Systems supporting that Control Center. The drafting team responded that using inter-connections as an impact criterion ultimately scopes in all interconnected systems in a single impact level. The concept of mutual distrust and security zones and perimeters implements cyber security boundaries that allow the selection and implementation of cyber security controls commensurate with the level of impact within a security boundary.

Another commenter noted that Criterion 1.4 does not consider an aggregate span of control. A generation control system could theoretically control 15,000 MW of generation without a single asset meeting the thresholds defined in the referenced criteria. The overall span of control of the BES Cyber Assets and BES Cyber Systems need to be considered by aggregating the field assets being controlled. The drafting team responded that it agreed and included this suggested change in the new draft.

Another suggestion was that it would help if section 1.4 clearly defined what level of control of generation would require classification as a 'High' impact. In some case a control center may have limited 'base point' setting capability for assets under section 2.1. The drafting team responded that the criterion has been modified to address the concern.

Another commenter stated that for Attachment 1, Item 1.3 and 1.4, the criteria for determining which control centers should be under the high category, the 2.4 Black Start Resources should be under Transmission Operator Control Centers not under Generator Operators since, under the EOP standards during Restoration, such units are under the control of the TOP, not the GOP/BA. The drafting team responded that it has eliminated the Blackstart Resources from these criteria, which is explained under Criterion 2.4 and 2.5's response.

Criterion 2.1 (Generation Plant)

Some commenters stated that although it is not delineated as such, it is implied that BES systems that are shared and control more than 1500 MWs collectively would be in scope. This should be clearly stated. If the intent is to include all BES systems for a facility that collectively produces 1500 MWs, then this should be clearly stated as such. The drafting team responded that it changed the criterion to clarify the situation.

Another commenter stated that since Interconnection is a defined term that is not applicable to this discussion, please remove the capitalization of the term "Interconnection" in this context, and change "in a single Interconnection" to "at a single interconnection". The drafting team responded that the use of the glossary term is correct: the 1500 MW threshold applies to generation in a single Interconnection. A generation plant may service multiple Interconnections.

Another suggestion was that Criterion 2.1, with its historical nature, needs to account for decommissioned generating units by adding "commissioned" or "active" to the beginning of the criteria. The drafting team responded that it agreed

and included this suggested change in the new draft.

Another commenter suggested that the threshold in the Medium Impact category for generation should be 1,000 MW instead of 1500 MW. The drafting team responded that the determination of the thresholds are derived in large part from version 4, which has been vetted by the industry, and was drafted with assistance from subject matter experts in the relevant operating areas.

Another commenter stated that the value of 1500 MW should be defined as either the nameplate or the continuous "rated" capability (where the equipment has been de-rated by the Responsible Entity for age/reliability). The drafting team responded that the criterion's MW value is based on a required rating measurement that must be submitted to the Regional Entity.

Another commenter stated that Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e., wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. The drafting team responded that, while the unavailability of intermittent generation (vs. controllable generation) may not be considered an extreme event, the impact of misuse of the associated BES Cyber Systems due to a cyber security compromise can result in BES disturbances. The impact criteria provide a measure of this impact.

Criterion 2.2 (Reactive Resource)

One suggestion was that "Net Reactive Power" should be read as "Absolute value of Reactive Power" to consider Static VAR compensator and synchronous condenser. The drafting team responded that the word "net" has been removed, since the nameplate value is specified as the value to be used for aggregation.

Another commenter stated that the former version had BES in front of Reactive Resource. The term BES should be restored to make clear that this is transmission level as stated in the application notes. The drafting team responded that it agreed and included this suggested change in the new draft.

Criterion 2.3 (Adverse Reliability Impact)

One commenter asked: What is meant by this criterion? How will it apply? The drafting team responded that this criterion is intended to include generation facilities that are designated as "must run" for reliability reasons, not market reasons.

Section 2.3 in Attachment I, may be problematic as it potentially allows Planning Coordinators or Transmission Planners to "arbitrarily" move GO and GOP entities from Low to Medium should the unit be identified as reliability must-run unit. The drafting responded that is has clarified the language to "to avoid BES Adverse Reliability Impacts in the planning

horizon of more than one year." The drafting team believes that this change addresses the concern.

Another commenter recommended deleting "or Transmission Planner" to ensure that only one entity is responsible for designating appropriate generation. The drafting team responded that this standard does not determine who does the designation. Designations may be issued by either of these entities, depending on the region's practice.

Another commenter expressed concern that there is a need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? The drafting team responded that other NERC Reliability standards already define the obligations of these entities with respect to these criteria. Once identified, the Responsible Entity owning these Facilities, Systems and equipment is responsible for compliance to the CIP standards of the associated BES Cyber Systems.

Another expressed concern was that Criterion 2.3 uses the phrase "long-term planning horizon" which is later defined as one-year or longer. It would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. The drafting responded that is has clarified the language to "to avoid BES Adverse Reliability Impacts in the planning horizon of more than one year." The drafting team believes that this change addresses the concern.

Another commenter asked for the definition of BES Adverse Reliability Impact. The drafting team responded that Adverse Reliability Impact is a NERC Glossary defined term. The most recent BOT approved definition is "The impact of an event that results in Bulk Electric System instability or Cascading." The currently approved FERC definition is "The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection."

Another commenter stated that Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. The drafting team replied that there is no implied requirement for PCs or TPs to designate "must run" generation to avoid Adverse Reliability Impact. The criterion is merely stating that when such a TP or PC does designate such generation, the BES Cyber Systems for that generation is subject to the CIP requirements.

Another commenter stated that the use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. The drafting team responded that it agreed and included this suggested change in the new draft.

Another concern expressed was that Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. The drafting team responded that the designation of generation as "must run" for reliability purposes as a result of "long term planning" has nothing to do with

the "real-timeliness" nature of the impact of its BES Cyber Systems on the function of "must run" generation asset to mitigate Adverse Reliability Impact. These time parameters are applied in different contexts. The intent is to ensure that the generation assets under these criteria are not transient assets run to mitigate short term market or operational conditions, but rather as long term mitigations for infrastructure deficiencies, whether permanent or temporary until long term remediation is engineered and put in service. In any case, the drafting team made minor modifications to avoid confusion with new Transmission Planning Horizon definitions in the glossary.

Criteria 2.4 (Blackstart Resources) and 2.5 (Cranking Path)

Many commenters expressed concern with this criterion. The SDT notes that it has removed restoration facilities from CIP-002-5, Attachment 1's "Medium Impact Rating (M)" category. The SDT made this decision after receiving input from commenters, from industry, and following discussions about the issue as presented to NERC's Operating and Planning Committees. The SDT learned that Blackstart Resources face reduction because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool. Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed. The SDT explains this change in more detail in the Guidelines and Technical Basis section of the posted draft CIP-002-5.

Criterion 2.6 (500kV Transmission)

One commenter asked if this criterion address facilities that essentially are radial leads and no load flow through. The drafting team responded that if they meet the definition of the BES, they are in scope. The use of the glossary term Facilities implies BES assets.

Another commenter asked if an autotransformer of 500 kV to 230 kV included. The drafting team responded that an autotransformer of 500 kV to 230 kV may be included depending on how the Responsible Entity defines its group of Facilities.

Criterion 2.7 (Other Transmission Facilities)

One commenter asked how a weighted value of a line is related to reliability. The drafting team responded that the weights used are based on average MVA ratings. These weights are used to normalize impact to a value for sites operating with different or multiple voltage levels.

Another suggestion was to change the first sentence of 2.7 to read: "Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000." The drafting team responded that the intent was to include BES Cyber Systems that could impact the reliable operation of the BES for any Facility within the single station or substation, not just Transmission Lines.

Another concern expressed was that the "weight value per line" used to determine total weighted aggregate value does not allow for variations in various owners' systems. Provisions should be made to exclude facilities that can be shown to not lead to cascading or voltage collapse upon their loss. The drafting team responded that the MVA values used are those used from a NERC reliability report, as pointed out in the Guidelines and Technical Basis section. The drafting team believes that this is an objective way of determining the level of impact that is sufficient for categorizing BES Cyber Assets.

Another commenter stated that line count does not necessarily mean that issues at particular substation will have a significant impact on the BES. Such impact can only be determined by studies and risk-based analysis of an entity's assets. The drafting team responded that they identified some gaps in the previous Version 4 criterion. The SDT believes that the current approach provides a more comprehensive approach to the impact of Transmission Facilities.

Another commenter suggested returning to the industry balloted and approved language that is in CIP-002-4 regarding 345kV with 3 or more lines. The drafting team responded that they made modifications to the transmission voltage threshold to remediate coverage gaps uncovered from the FERC data request following the Version 4 filing and to account for impact in situations with mixed voltage levels.

Another commenter stated that Criterion 2.7 specifies a floor of 200 kV. In certain parts of the country, the 200 kV floor is too high. The drafting team responded that the purpose of Criterion 2.7 is not to require all transmission Facilities in the transmission backbone (Bulk Electric System) be protected, only those that are determined to be critical. Criterion 2.7 establishes thresholds that would qualify such Facilities as Medium impact. Other Facilities are protected under the requirements for Low impact.

Another commenter noted that Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. However, there is no guidance given for transformers. The drafting team responded that guidance has been added for transformers in the Guidelines and Technical Basis section.

Criterion 2.8 and 2.9 (IROL for generation and FACTS devices)

One commenter stated that the phrase "at a single station or substation location" does not seem to add any value and

can be a source of ambiguity. The drafting team responded that with the amended focus of the categorization criteria on Facilities, systems and equipment and their associated BES Cyber Systems, the drafting team believes that the phrase is now appropriate.

One commenter suggested adding an additional criterion that captures the fact that IROLs may be based on dynamic system phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. The drafting team agreed and included language to this effect in the IROL criterion in Section 2 (Medium Impact).

Another commenter noted that the standard is placing a burden upon the TO for actions of others, that the TO has no control over, with no allowance for coordination or negotiations for potential changes in the determination of IROLs. The drafting team responded that FAC-014 requires the communication of the SOLs and IROLs to the asset owners who operate the affected Facilities.

Another suggestion recommended changing "Transmission Facilities" to "BES Transmission Facilities" for consistency purposes. The drafting team responded that the use of the NERC Glossary term “Facilities” includes the BES qualification.

Another commenter asked the drafting team to provide a definition for the term "Flexible AC Transmission Systems FACTS". The drafting team responded that the criterion specific to FACTS has been removed since it is included in Transmission Facilities.

Another commenter recommended that the term ‘Planning Coordinator’ be used rather than ‘Planning Authority” to be consistent with the rest of the standard and current NERC practice. The drafting team responded that they agreed and have changed the term to conform to the functional entity in the functional model.

Another commenter suggested that the phrase ‘. . . as critical to the derivation of IROLs and their associated contingencies’ be changed to, ‘. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations’, like the wording using in Criterion 2.11. The drafting team responded that the current wording of this phrase is taken from the wording in FAC-014-2.

Another commenter expressed concern that there is a need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? The drafting team responded that other NERC Reliability standards already define the obligations of these entities with respect to these criteria. Once identified, the Responsible Entity owning these Facilities, Systems and equipment is responsible for compliance to the CIP standards of the associated BES Cyber Systems.

Another commenter stated that in sections 2.8, 2.9 and 2.11, the table titled “Major WECC Transfer Paths in the Bulk

Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. The drafting team responded that upon further consultation with WECC, the specific language in question has been removed.

Criterion 2.10 (Nuclear Plant Interface Requirements)

One commenter stated that Criterion 2.10 needs to be limited to the plant switchyard, otherwise the entire grid could be included. The drafting team responded that the current language is the language used in NUC-001.

Criterion 2.11 (SPS)

One comment was that Criteria 2.11 twice contains the phrase "...if destroyed, degraded, misused". This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the "15 minutes" qualification as defined at the top of the Medium Impact Rating section. The drafting team responded that the 15 minute term is meant to provide some boundaries to the term "real-time". It is intended to indicate the amount of time of when the effect of the triggered action resulting from the compromise of the BES Cyber Asset on the affected BES Asset (not BES), notwithstanding any other recovery mechanisms from contingency actions or redundancy. The drafting team has reviewed the definition of BES Cyber Assets and has removed the redundant terms from the Attachment 1 pre-ambles.

Another commenter observed that this criterion implies that all components of the SPS are designated as medium without regard to whether loss of those elements of the SPS system would lead to the referenced IROL violation. The SPS can be designed so that incorrect readings or misoperation of a given element of the system has either no impact or acts to run the SPS in the "safest" manner. If this is the case, the individual elements of the SPS should not require a medium designation, and should be allowed for in the standard. The drafting team responded that all the Elements of the SPS will inherit the "high water mark" of the SPS, and as a "system" that could cause excursions beyond the IROLs, should be categorized as Medium.

Another commenter questioned if this includes SPSs which are associated with Generation sites. The drafting team responded that these are included by referring the commenter to the Guideline and Technical Basis.

Another commenter stated that in sections 2.8, 2.9 and 2.11, the table titled "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. The drafting team responded that upon further consultation with WECC, the specific language in question has been removed.

Another commenter stated that Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. An SPS or RAS may be implemented for a specific contingency for example. As an example, when that contingency happens,

certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. The drafting team responded that the drafting team responded that they agreed and have changed the criterion to address the comment.

Criterion 2.12 (UFLS/UVLS)

One commenter asked for clarification as to whether a UFLS or UVLS program of less than 300 MW is a Low Impact Rated Cyber Asset or is not subject to the CIP standards at all. The drafting team responded that changes have been made to the DP and LSE sections of Section 4 of CIP-002-5. Sections 4.2.1 and 4.2.2 state that only UVLS or UFLS Facilities that are in a UVLS or UFLS program required by a NERC or Regional Reliability Standard and meet the qualifications for Medium Impact are in scope for registered LSEs and DPs. No other UVLS or UFLS Facility is in scope for these CIP standards. The BES Cyber Systems that impact those automated UVLS and UFLS Facilities for more than 300 MW are categorized as Medium. Other BES Cyber Systems that only impact other UVLS or UFLS are not in scope.

Another commenter observed that the 300 MW bright-line seemed arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with criterion 2.1 of 1500 MW. The focus should be on how a malicious user can cause an Adverse Reliability Impact. The drafting team responded that UVLS and UFLS systems are last ditch efforts to recover from a BES event, when all other contingencies have been exercised to address the reliability issue. In fact, it could probably be argued that any UVLS or UFLS system that is part of a regional load shedding program designed to provide last ditch relief should be considered Medium Impact. The drafting team carried over the 300 MW from the current effective version, and version 4, which was industry approved in December of 2010.

One commenter expressed concern that Criteria 2.12 refers to a “system” - as in “Each system or Facility...” - which implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. The SDT may want to consider removing “Each system or”. The drafting team responded that the term BES Cyber System” or BES Cyber Asset” was used when referring to those BES Cyber Systems or BES Cyber Assets subject to the CIP standards. The term “systems” when used stand-alone is used in its broader sense to include Facilities, cyber assets or a combination of both when they directly perform a BES reliability function.

Another observation was that the standard and the Application Guidelines do not indicate whether the 300 MW limit is a system limit or an entity limit. The drafting team responded that it added the phrase “Each System or group of Elements that performs automatic Load shedding under a common control system” to clarify the criterion.

Another commenter suggested that the SDT replace the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency. The drafting team responded that it added the phrase "Each System or group of Elements that performs automatic Load shedding under a common control system" to clarify the criterion.

Another commenter requested that "system" be capitalized as it appears to align properly with the NERC definition. The drafting team responded that it agreed and included this suggested change in the new draft.

Another commenter observed that a small entity may be required to own and maintain UFLS relay or relay system by the Transmission Provider. In the standard, the UFLS threshold is at 300MW. The small entity may not have 300 MW of load, but their relaying is part of the design of an UFLS system that is much greater than 300 MW. This small entity's relay is not critical to the BES and if degraded or destroyed would not compromise the capability of the Transmission Provider's UFLS system as the two systems are not integrated and do not communicate. The drafting team responded that changes were made in the applicability section of the standard and in this criterion to address the concern.

Criterion 2.13 (Other Control Centers)

One commenter stated that Criteria 2.13 in Attachment 1 is not acceptable because under 1) the functional obligations of TOP and TO is too vague and 2) 300MW of in many cases does not qualify as significant impact. Also 300 MW of generation should not be equated to 300 MW of UFLS/UVLS. The drafting team responded that the functional obligations of the Transmission Operator and the Transmission Owner are listed in the NERC Functional Model. In many cases, where the Transmission Operator and the Transmission Owner are separate entities, there are agreements between the TOP and the TO on which functions of the TOP have been delegated to the TO. Registered Transmission Operators may have some of their functions performed by another entity through agreements. In addition, the application of the 300-MW threshold in this case is for Generation Control Centers. By definition, this criterion is applicable only to generation Control Centers that control more than one generation facility in more than one location. Generation Control Rooms that control generation in a single generation facility fall under the 1500 MW threshold. The intent is discussed in the Guidance and Technical Basis section.

Another comment was that Transmission Owners do not have Control Centers and should be struck from this criterion. The drafting team agreed and included this suggested change in the new draft.

Another comment was that the term "control centers" should be capitalized in the phrase "generation control centers" to make it clear that it refers to the defined term "Control Center." The drafting team agreed and included this suggested change in the new draft.

Another commenter recommended that the proposed 2.13 language be deleted and replaced with the following: “TOP and GOP Control Centers not included in High Impact Rating and controlling 1500 MW or greater of load or generation.”

Add: “2.14. Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers.” Making this change will ensure that other appropriate Control centers will be categorized in either the Medium or Low level. The drafting team responded that for criterion 2.13, the proposed language would not adequately reflect the level of impact of generation and TOP Control Centers. The drafting team believes that all Control Centers not categorized as High Impact should be categorized at least as a Medium because of the functions they perform and their interaction with other Control Centers. The intent of the 300 MW threshold in the case of generation is an attempt to consider a specific type of configuration in generation Facilities, as explained in the Guideline and Technical Basis section. Regarding the addition of 2.14, criteria for Control Centers are precisely drafted so that adequate cyber security protections are applied. If these protections have been applied, then the Responsible Entity already complies. These ensure that all Control Centers have the protection implemented all the time. These protections implement a defense in depth posture represented by the requirements in these standards. Network connectivity is but one aspect of the total protection that is required for Medium Impact assets.

Another observation was that it is not clear if the term “generation control centers” is referring to: 1) control centers local to generation, 2) centralized control centers controlling multiple geographically disparate generation resources, 3) or both. The drafting team responded that the term Control Center is now capitalized: the assets covered under this criterion must meet the definition of Control Centers, not control rooms local to the generation location.

Another commenter asked for clarification on what is meant by the term "control" in (2) generation control centers that "control" 300 MW or more of generation. Does this mean physical control only or does it include verbal commands? Also, does the 300 MW refer to name plate rating or some other method AND is that 300 MW only for BES generation or all generation that generation controls? The drafting team responded that the term “control” means perform the functions of a Control Center. Verbal commands that have a real-time effect are included. The 300 MW is net Real Power for BES generation. The criterion has been amended to clarify these parameters.

Another commenter stated that Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e. wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. The drafting team responded that, while the unavailability of intermittent generation (vs. controllable generation) may not be considered an extreme event, the impact of misuse of

the associated BES Cyber Systems due to a cyber security compromise can result in BES disturbances. The impact criteria provide a measure of this impact.

Section 3 – Low Impact Rating

One commenter proposed to change the phrase "...or Section 2 Medium..." to "...Section 2 as having a Medium..." for consistency purposes. The drafting team agreed and included this suggested change in the new draft.

Another observation was that Section 3 does not provide a minimum site MWs or interconnection voltage and recommended a nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high side of the step-up transformer(s) connected at a voltage of 100 kV or above. This was proposed in line with the Bulk Electric System (BES) definition developed under NERC Project 2010-17 Definition of the Bulk Electric System. The drafting team responded that it specifically chose the defined term Facilities to limit the applicability to the BES. The SDT addressed the concern in Section 4 (Applicability) of the standard itself. Section 4 clearly stipulates under Facilities 4.2.3: "Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities." (Underline added). Only those Facilities that are deemed to be BES Facilities are in scope for the standard. If these Generation facilities are excepted from the BES definition, then they are also excepted from the applicability of these CIP Cyber Security standards.

General Comments

A general comment was that it is unclear if BES systems at a facility can have numerous levels of impact. The drafting team responded that at a given physical facility, there may be a BES Cyber System that may adversely impact a BES Facility classified as Medium and there may also be a BES Cyber System that may adversely impact a BES Facility classified as Low.

Another concern was that there is little justification provided for why the criteria for the various categories were selected and why three categories were selected. The drafting team responded that the Background, Rationale and Guidelines and Technical Basis sections of the posted CIP-002-5 provide the justification for both the criteria and the "bright lines" defined.

Several commenters wanted an impact level of "No Impact Rating". The drafting team responded that Cyber Assets that have "No Impact" are by definition not in scope.

Other commenters wanted a fourth category of risk impact, "De Minimis Impact", that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. The drafting team responded that the

electronic connectivity of the BES Cyber Systems does not have a bearing on the impact of the specific BES Cyber Systems or BES Cyber Assets on the reliable operation of the BES. The drafting team has included consideration of the connectivity in the applicability column of various requirements.

Another concern was that there is no appreciable difference between the requirements for High and Medium impact levels. The SDT may want to consider modifying items 1.1 through 2.13 on Attachment I to be "All these assets have a Critical Impact Rating". The drafting team responded that there are significant differences in the functional impact of the High Impact assets and those in the Medium Impact. The Facilities, systems and equipment in the High Impact category typically provide reliability functions for a wide area and have control and therefore impact for a large number of Facilities with significant impact, especially with the additional qualifications in the revised draft. While the actual number of additional controls may not be significant in number, these few additional controls (or differences in controls) are significantly stronger in these environments. They are also more practically implementable in these environments.

Another commenter proposed that Low Impact assets and their requirements be moved to another standard separate from High and Medium Impact assets and requirements. In addition, it was felt that the scope for Low Impact generation would bring a considerable number of new assets into the CIP standards. The drafting team responded that they moved all the requirements for Low impact systems to CIP-003 as management controls, further indicating the programmatic nature of the requirements as well as substantive changes in the requirement language.

Another concern was that generation facilities that require notification from the Planning Coordinator or Transmission Planner (e.g. Criteria 2.3 and 2.6) must be placed on a transition plan that would allow those facilities that are notified of change in status adequate time for remediation. The drafting team responded that the implementation plan for newly identified BES Cyber Systems or BES Cyber Assets provides adequate time for the Responsible Entities to come into compliance.

Another concern was that the 15 minute criterion does not apply to the vast majority of systems covered by the standard because power system apparatus and computer systems generally operate in the time frame of five seconds or less. The drafting team responded that the combination of impact on reliable operation of BES Assets and the 15 minute "real-time" impact was used to limit the scope to those Cyber Assets that would impact the reliable operation of BES Assets within a 15 minute window, and excludes those Cyber Assets that do not have an impact within 15 minutes.

Another comment was that the term "adversely impact" should be defined. The drafting team responded that the term adequately conveys the meaning of an impact that has a negative effect on the reliable operation of the BES and therefore does not need to be added to the NERC Glossary of Terms.

Another comment was the suggestion to change the phrase "would, within 15 minutes, adversely impact" to "could

adversely impact." There is a significant difference between would and could. The drafting team debated the use of both terms and decided that the use of the term "would" provides a more accurate direction on the evaluation of the impact of the BES Cyber System or BES Cyber Asset on the BES Facilities, systems and equipment, and that the term "could" was too open- ended.

Another comment suggested an additional criterion (similar to CIP-002-3 R1.2.7) in the Medium category to capture these self-identified impacts: 'Any additional facilities that support BES Reliability Operating Services that the Responsible Entity deems appropriate.' The drafting team responded that they considered inclusion of such a criterion in Version 4 but withdrew it in consideration of the complexities for the Responsible Entities demonstrating compliance to such an open ended criterion.

Other comments were that study based exceptions should be allowed. The drafting team responded that the bright-line criteria ensure that these standards are uniformly applied across regions and entities. The use of exceptions based on engineering studies is contrary to that objective and reintroduces the non-uniformity and inconsistencies that bright-lines address.

Another concern was that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS may extend into the substation and field RTU and devices. The drafting team responded that the proposed definition of Control Center provides adequate scoping qualifications. The definition has been amended to refer to reliability tasks defined in the functional model for real-time operations for applicable functional entities. The scope of included BES Cyber Systems will depend on many factors, including how Responsible Entities define their systems and ESPs.

Another commenter stated that the Attachment 1 "bright line" criterion regarding load shedding systems ("300 MW") should be included in the Section 4.1.2 Distribution Provider Applicability section. Otherwise, all distribution providers may be obligated to demonstrate that their UFLS / UVLS / SPS / RAS equipment was not responsible for IROL violation / 300 MW - where they may not even be aware of the full scope. The drafting team changed the Applicability section in the updated draft to address this comment.

Another commenter observed that Criterion 1.10 in CIP-002-4 was removed and recommended that it be reinstated in Attachment 1. The drafting team agreed and included this suggested change in the new draft.

Another comment stated that the opening paragraph of the definition of Medium Impact Rating should be revised to correspond with the wording for High Impact Rating. The drafting team modified the heading as suggested.

Another concern expressed was that application of the "bright line" criteria proposed, some of which require identification of Critical Assets based on determinations made by Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners, will create significant new burdens on Reliability Coordinators,

Planning Authorities/Coordinators, and Transmission Planners. The drafting team responded that the criteria in Attachment 1 provides no new requirement that the RC, TOP, PC, or TP are not already doing or being required to do by other NERC reliability standards.

QUESTION 3 – CIP-002 R1:

Requirement R1 of draft CIP-002-5 states, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R1 and Parts 1.1 through 1.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Most of the comments submitted in response to this question centered around the following themes:

- Confusion about the order of categorization
- Disagreement with the use of the word, “intended” in Part 1.1
- Concerns about having 30 days to update categorizations in Part 1.1
- Concerns about the scope of change prompting the need to update asset categorizations
- Questions about identification of low impact assets
- Questions about responsibility for the requirement
- Minor wording recommendations
- Comments about the Informational sections of the standard
- Comments on Attachment 1
- Other comments

Each of these themes is discussed in more detail below.

Confusion about the Order of Categorization

Several stakeholders noted that the sequence of actions associated with complying with Requirement R1 was confusing and the process of classifying and categorizing cyber assets and then identifying other assets which must be protected (CIP-005 and CIP-007) is excessively complicated.

One commenter recommended the following three-step process for identification and categorization, and indicated that this process would result in only needing to identify high and medium impact facilities:

> 1. For each BES facility that has cyber assets associated with it, go to CIP-002-5 Attachment 1 to find out if the facility is low-, medium-, or high-impact.
>
> 2. Determine the BES Reliability Operating Services that the BES facility supports.
>
> 3. Just as was the case in CIP Versions 1-4, the last step is to identify the cyber assets associated with the facility that are in scope for the remaining CIP standards

Other commenters suggested starting by first identifying high, medium , and low assets and then proceed with identifying Critical Cyber Assets at those facilities. Still other commenters proposed identification of low impact BES Cyber System at a Facility level, rather than by listing all the Cyber Assets associated, as this would add administrative burden and not provide additional BES security or reliability.

Other commenters recommended creating two Requirements - one for identification of BES Cyber Assets and another for categorization of BES Cyber Assets to eliminate multiple repeat violations of the same requirement, noting that

multiple violations of this requirement may stem from different causes and may unintentionally lead to mischaracterize an entity's compliance record and have consequences that impact the scope of subsequent audits and compliance investigations. Another stakeholder recommended an identification process that starts with identifying any applicable BES Reliability Operating Services relative to the entity's Registered Function(s), then identifying and classifying BES Cyber Assets and/or BES Cyber Systems associated with that BES Reliability Operating Service according to the criteria in Attachment I.

As noted above, and in response to the above, the SDT offers that there are many different ways of approaching the organization of the actions in this requirement. After much deliberation, the SDT modified the Requirement R1 so that the order of activities in identifying and classifying assets is clearer. Requirement R1 now includes several "Parts" to step entities through the process of categorizing their BES Cyber Systems:

- Part 1.1 addresses the first step of identifying which of the entity's Facilities, Systems, and equipment meet the bright-line criteria in Attachment 1
- Part 1.2 uses the output of Part 1.1 and for each Facility, System and equipment with a high impact rating, requires the responsible entity to identify the BES Cyber Systems and associated BES Cyber Assets used for that Facility, System or equipment
- Part 1.3 uses the output of Part 1.1 and for each Facility, System and equipment with a medium impact rating, requires the responsible entity to identify the BES Cyber Systems and associated BES Cyber Assets used for that Facility, System or equipment
- The entity's Facilities, Systems and equipment not identified as high or medium impact is, by default, categorized as low impact

Some commenters expressed concern about the grouping of BES Cyber Assets into a BES Cyber System without any consideration criteria. One commenter asked if each cyber asset is categorized EITHER alone OR as part of a BES system. The SDT made significant changes to the Criteria in Attachment 1 in an attempt to make the criteria as objective as possible to eliminate questions about groupings. These changes clarify that a BES Cyber System is one or more BES Cyber Assets, and that all BES Cyber Assets are part of a BES Cyber System.

Disagreement with the Use of the Word, "Intended" In Part 1.1

Several commenters noted that Requirement R1.1 (Requirement R1.4 in draft 2) refers to the "intention" for the BES Element or Facility to be in service for more than six calendar months and observed that the word "intended" is not auditable. The SDT agrees and has changed "intended" to "planned". One stakeholder proposed that entities be

required to document the intent in that instance to allow the auditor the latitude to accept intent over actuality in the case where the BES Element or Facility was in service for more than six months due to unforeseen circumstances. With the change in wording from "intended" to "planned", the SDT believes that the dated electronic or physical lists showing changes to the BES (with a date for each change) accomplish the documentation of evidence required to demonstrate the planned nature of changes to the BES.

Concerns about Having 30 Days to Update Categorizations In Part 1.1

Several commenters had questions about the 30 days proposed for updating categorizations following a change to the BES in what was Requirement R1, Part 1.1 (now Part 1.4 in the revised standard). Some questions arose around the number of days, with some commenters proposing a longer period (60 days or 90 days or annual update). One commenter asked the SDT to provide its justification for the selection of the day time period, and implied that an annual review would be preferable to the 30 days. CIP-002 is the foundational standard for the entire set of CIP standards. If an entity adds a new piece of equipment to the BES and it is not accounted for under CIP-002, then that piece of equipment could be unprotected for an extended period of time (a year or more if the proposal to change the 30 days to "annual" were adopted.)

Some commenters questioned whether updates should be required for all changes to the BES and the SDT does not believe this is necessary. Under the revised standard, Responsible Entities are not required to implement protections to assets that have changed only in response to a temporary emergency situation and where the protective controls will not be implemented before the asset is returned to its original configuration.

Some commenters noted that updating this categorization, especially for low impact Elements and Facilities is burdensome as every configuration change of the BES would need to be tracked, dated, and evidence of the process to identify or categorize the BES Cyber Assets or BES Cyber Systems documented. An alternative method should be considered - for example, when planning studies reveal that the configuration change of the BES is material, this could trigger the process of identifying or categorizing the associated BES Cyber Assets or BES Cyber Systems.

One commenter proposed requiring the update before the equipment was placed into service cautioning that deployment or reconfiguration of a BES Cyber Asset may pose a significant risk to the BES. A thirty day gap would delay identification of a BES Cyber Asset, and also delay implementation of Cyber Security measures prescribed under CIP-003 through CIP-010, thus also disagreeing with the provision limiting "updates" to include only those Cyber Assets "that are intended to be in service for 6 months."

The SDT considered the different proposals provided and changed the 30 days to 60 days to provide entities more time to make needed updates – however the SDT cannot justify extending the period for longer than 60 days. Annual updates

would allow some Facilities, Systems, or equipment to go unprotected for longer than justified given the high or medium risk to the BES of leaving that Facility, System, or equipment unprotected. The SDT did not adopt the suggestion that changes to categorization be completed before deploying or reconfiguring a BES Cyber Asset. The SDT recognizes the risk to the BES that may occur if some equipment is not protected, however the SDT tried to maintain a balance of reasonable security awareness while also moderating audit impact and the impact to real-time operations. There may be many scenarios in which an entity is faced with the need to change a piece of equipment in 'real-time,' and waiting to do so while the asset is categorized may jeopardize reliability.

Concerns about the Scope of Changes Prompting the Need to Update Asset Categorizations

Some commenters asked if Part 1.1 refers to inclusion of the element or facility on the BES Cyber Assets and BES Cyber System list, or inclusion in the entire scope of CIP-002 actions including the signature of the CIP senior officer. As specified in Requirement R1, the requirement only requires an update to the identification of the Facilities, Systems, or equipment and the high and medium impact BES Cyber Systems and their associated BES Cyber Assets. Approval by the Senior Manager or delegate is specified in R2.

Several commenters expressed concern with the open-ended use of the word, "change" in reference to a change to the BES that prompts the responsible entity to update its categorization and indicated that leaving this open-ended leaves the requirement subject to varying interpretations and challenging to audit. One stakeholder suggested making the impact change determination dependent upon BES Cyber Asset changes; returning to an annual review; or alternatively adding a very specific list of BES changes for which the analysis must occur. Another commenter proposed that a change to a relay setting could be could be considered, using the strict definitions of Elements and Facilities, as a change to a BES Element and proposed that such a change is too granular for inclusion in the scope of changes warranting a revision to the categorizations required under Part 1.1 (now Part 1.4). The commenter proposed establishing boundaries for changes that would warrant updating the categorization including topological changes, generator interconnections and generator uprates and equipment retirements but not for derates since derates may lower the categorization of BES Cyber Systems and/or BES Cyber Assets and the reduction in compliance burden will cause them to do this.

One set of commenters recommended changing to, "when a change to BES Elements is completed and / or the facility is placed into operation".

Another set of commenters recommended adding a word between "calendar days of" and "a change to BES…"

In response to the concerns and suggestions offered above, the SDT notes that it elected to leave this open-ended as any list the SDT might develop would likely not meet all reasonable circumstances. The revised sentence says: "Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change

to BES Elements or Facilities is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category."

One commenter expressed a concern that the requirement doesn't explicitly address "Transient Cyber Assets," noting that a transient cyber asset could fall "under the radar" and result in a major threat to the BES. The SDT deleted the proposed definition of "Transient Cyber Asset." These transient assets are normally portable maintenance and diagnostic tools, which by their very nature cannot meet all the requirements mandated for BES Cyber Assets, such as a fulltime physical security perimeter, or wiping all information when it is 'redeployed' to another location when the purpose for its existence may be to bring back field data for analysis. The SDT does not intend for the CIP requirements to make impossible or impractical normal practices that increase reliability of the BES, such as being able to use Cyber Asset based tools for diagnostics and maintenance, especially among numerous field assets. As such, the SDT does not believe it is necessary to include these in the scope of R1.

Another commenter recommended adding a companion requirement to address updating categorization when Facilities are "out-of-service." Regarding "out-of-service" cyber assets, these cease to be BES Cyber Assets by definition the moment their impact cease on the BES (i.e. within the 15 minute). The SDT offers that it is the Responsible Entity's option to ensure they do remain compliant if and when they are brought back in service.

One commenter noted that Part 1.1 doesn't provide a timetable for the phase-in for the entity to meet the potential additional Standard(s) Requirements caused by this change. The SDT notes that phase in of requirements is addressed in the Implementation Plan for the set of CIP standards.

One commenter asked for more clarity when categorization of the BES Cyber Assets or BES Cyber Systems shifts from a higher to a lower impact category. The SDT responds that if the change is from a higher to a lower category, the Responsible Entity is not required to update the lists, but if not doing so, it will be required to be compliant to the requirements for BES Cyber Systems at that level.

Questions about Identification of low impact Assets

One commenter asked the team to provide its justification for the criteria for the various categories selected, and specifically why three categories were selected, and expressed concern about the inclusion of "low impact" assets, proposing that the low impact assets be excluded from the standards. The SDT tried to provide its justification for the criteria and the categories in the Background section of the standard and the Application Guidelines at the end of the standard. Together these explain how the drafting team developed its justification for the criteria selected with this risk-based approach to cyber security.

Several commenters proposed revisions to the following sentence: "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be low impact and do not require discrete identification" and identified that entities will still need to maintain this list when the listing of BES Cyber Systems is created and each system is classified. Several stakeholders indicated a concern that auditors will demand the list even if it is not explicitly required. The SDT believes that an explicit statement to the effect that no list is required is required to provide the required clarity in compliance requirements.

Several stakeholders proposed elimination of all requirements associated with low impact BES Cyber Systems from CIP-002 and proposed moving all the low impact requirements into a separate standard with a longer implementation plan. The SDT adopted the suggestion to move all the requirements associated with protection of low impact Systems into a single standard – and moved those requirements into CIP-003. The SDT did not remove the low impact language from CIP-002, as this is the standard where low impact systems are identified by default. Note that the SDT also adopted the suggestion to give entities more time to become compliant with protection for low impact assets in support of this suggestion. The Implementation Plan now specifies an implementation timeline of at least three years for the low impact requirement. This should allow entities more time to focus on protection of the more critical assets.

One stakeholder asked how entities could comply with CIP-005-5 R1.1 and CIP-006-5 R.1.1, (defining operational or procedural controls to restrict unauthorized electronic access or physical access) without previously identifying those assets either globally or specifically in CIP-002-5 R1? The SDT agrees that each responsible entity will need to identify and categorize its assets in CIP-002 as a prerequisite for meeting compliance with other CIP standards. Please see the revisions the SDT made to CIP-002 to clarify the process for identifying and categorizing assets.

Some commenters had questions about the low impact category and indicated that this resulted in having all BES Cyber Assets in the CIP standard scope, which was not directed by FERC Order 706. The SDT notes that FERC order 706 includes a directive to consider the National Institute of Standards and Technology (NIST) approach, which includes baseline protection for all applicable systems.

Several commenters indicated that the Measure M1 appeared to require documentation of the low impact assets even though the associated requirement included the phrase, "…and do not require discrete identification." In response, the SDT removed the following sentence from M1: "Evidence of categorization of low impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls."

Questions about Responsibility for the Requirement

Several commenters made suggestions about what functional entity should be required to comply with Requirement R1. Stakeholders raised issues about joint ownership, about responsibility for protection of facilities that are leased.

Regarding ownership, the SDT believes that the responsibility for compliance should rely on the owner of the asset, and that it is the responsibility of the owner, through contractual arrangements or otherwise, to ensure compliance by the operator if such operators are different from the asset owner.

One commenter noted that the word 'owns' is used in two places in R1 and recommended changing the word "owns" to 'operates' or 'utilizes' and cautioned that ownership may not be the determining factor based on outstanding operating agreements over time – and also noting that a single asset may be used by more than one entity. The SDT notes that the standard was revised so the word, "owns" is no longer used in Requirement R1, but removal of the word "owns" does not mean that the "Responsible Entity" is no longer the owner.

Some stakeholders asked the SDT to modify the standard to clearly state that those entities with no Bulk Electric System (BES) assets per the definition included in the NERC Project 2010-17, Definition of Bulk Electric System, are not required to comply with this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no BES Cyber Assets/Systems or to create a fourth category of "No Impact", thus no further action required which can be certified annually by the Senior Manager. In response, the SDT notes that if an asset has "no impact" this is not a cyber asset and is outside the scope of this standard by definition.

Some stakeholders asked for confirmation that entities without any BES will not have any Critical Cyber Assets or Systems and therefore, R1 will not apply to them. In response the SDT notes that registered entities that own assets necessary for the reliable operation of the BES must be included. That is the reason these entities are required to register as NERC Registered Entities.

Other Minor Wording Changes for Clarity

One stakeholder recommended changing "of" to "when" in the statement, "…when a change to BES Elements…" and the SDT adopted the intent of this suggestion by adding the word, "when" so that the revised phrase now reads, "…of when a change to BES Elements…"

One stakeholder indicated the term "would" adversely impact one or more BES Reliability Operating Services is used in the background discussion and recommended using the word, "could" instead. The commenter's concern was that without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. The SDT believes the word, "would" is more definitive and more clearly conveys the intended meaning, thus the SDT did not adopt this suggestion.

One commenter noted that the Rationale for R1 used the terms, "Cyber Assets and Cyber Systems.." and recommend the language be changed to "BES Cyber Assets and BES Cyber Systems.." and this change was adopted and is reflected in the

revised standard.

One commenter noted that the Rationale for R1 refers to "impact" and proposed that this should be changed to "potential impact." In response, the SDT modified Attachment 1 so that it no longer includes the phrase, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services…" and instead relies solely on defining Impact categorization based on bright line criteria. Thus the SDT believes the word, "impact" is the correct word.

One commenter noted that the "Rationale - R1" box uses the term "Cyber Systems," which is not a formal term and suggested changing the case to avoid confusion. The commenter was correct that "Cyber System" is not a defined term – however the SDT did propose a definition of "BES Cyber Systems" – and in the revised standard the SDT was careful to use the defined term, "BES Cyber Systems" in its updated rationale for Requirement R1.

One commenter suggested expanding the language when referring to several levels of impact or assets and systems and indicated that as originally drafted, "high and medium impact" could be interpreted as meaning an asset or system which is both high and medium . The SDT revised the standard so it does not include the phrase, "high and medium impact."

One commenter proposed changing the wording in Part 1.1 (now Part 1.4 in the revised standard) from "…and change to BES Elements and Facilities is placed…" to "…and change to BES Elements and Facilities being placed…" The phrase was changed based on several suggestions from different commenters to: "… of when a change to BES Elements or Facilities is placed…"

One commenter recommended changing "security plan" to "Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes and plans in place to comply with security requirements. Should the last paragraph on page 7 say "cyber security plan"? In response, the drafting team notes that, in the context of these standards, the term "security plan" includes any plan required by the standards (e.g. physical security plan, incident response plan, and recovery plan).

The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." The SDT changed this to "BES Elements or Facilities" in R1.4 to clarify the SDT's intent. (Underlining added).

Another stakeholder proposed modifying M1 to change the language, "…as required in R1 and list of changes to the BES…" to "…(as required in R1 and list of changes to the BES Elements and Facilities)…". Measure M1 was not modified in response to the proposed language modification. The requirement doesn't tie the update to changes in "Elements and Facilities" – the requirement ties the update to changes to the "BES."

Comments about the Informational Sections of the Standard

Some stakeholders asked about the enforceability of the Background and Application Guidelines sections of the standard. The SDT clarifies that the Background and Application Guidelines and Technical Basis are provided for guidance but is not enforceable - compliance monitoring is to requirements, not to any of the background, rationale or other contextual information presented in the posted standards. NERC has adopted the results-based format and process for standards and all results-based standards will include these sections.

Several commenters noted that in the background section of the standard, there is a statement that malware protection applies to a system as a whole and may not be necessary for every individual device to comply. These commenters noted that network-based anti-malware is only one aspect of malware protection and expressed the view that it is completely ineffective for malware not introduced over the network or introduced within a protected network where the configuration of the network allows traffic to pass between Cyber Assets without inspection. In response the SDT notes that there is a requirement in CIP-007-5 to protect the "BES Cyber System" not the asset. The entity has to be able to demonstrate compliance with protection of the BES Cyber System. See CIP-007 Requirement R3 and the associated information in the Rationale for R3 which includes the following: "The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection."

Other comments noted the phrase one "of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems." The "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" defines the term BES Cyber System as "[o]ne or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services." The SDT goes on to state that the use of the term BES Cyber System is intended "to provide a higher level for referencing the object of a requirement." The commenter suggested that neither the definition of BES Cyber System nor the malware requirements in CIP-007-5 indicate, on their own, that compliance with the requirement does not require every BES Cyber Asset that comprises a BES Cyber System to have malware protection. The commenter is therefore concerned that the Regional Entities will continue to enforce the CIP standards on an individual BES Cyber Asset basis, per a literal interpretation of the text of the Version 5 Standards. As such, the commenter requests more explicit confirmation of the holistic approach of the Version 5 Standards as indicated by the "Background" section of CIP-002-5 and additional examples similar to the malware example already provided.

In response, the SDT notes that it has made several significant changes to all of the standards and to the definitions of BES Cyber System and BES Cyber Asset to more clearly explain the BES Cyber System-level approach. The standards

themselves are applicable on a BES Cyber System-level (and certain associated Cyber Assets). The SDT also clarified the background section of each standard to more clearly explain the applicability section in the tables. Additionally, since the BES Cyber System definition was modified to strengthen the SDT's intent that they are one or more BES Cyber Assets logically grouped by the responsible entity, it underscores the holistic approach of the Version 5 standards. The SDT has also expanded the guidelines and technical basis section of CIP-007.

Some stakeholders questioned the Responsible Entity's ability to "determine the level of granularity at which to identify a BES Cyber System[,]" as stated in the "Background" section of CIP-002-5 and asked for clarification that the Regional Entities would **not** play a role in the definition of boundaries of BES Cyber Systems. The SDT cannot make promises for what a Regional Entity will and will not do. However, in addition to the changes made in the definitions and standards themselves, the SDT notes that the flexibility remains with the responsible entity. These are results-based standards, and the requirements indicate the required result aimed at the applicable BES Cyber System. By stating that "defining the boundary too broadly could make the secure operation of the BES difficult to monitor and assess," the SDT is cautioning that a determination to classify a system too broadly may introduce unnecessary challenges in meeting the requirements. In general, the SDT has attempted to explain that Version 5 is responsive to lessons learned from implementing previous versions by recognizing that Cyber Assets function together as a complex system. Entities now have an opportunity to identify those collective BES Cyber Assets as BES Cyber Systems and apply requirements to them on a system level.

In the Guidelines and Technical Basis section of the standard, commenters recommended that the team consider omitting the reference to "Substation automation" as it may have different meanings in the industry and is not defined in the NERC Glossary. Another comment identified a difference in the description of BES Reliability Operating Services in this part of the standard and in the proposed definition. The SDT has retained the reference to "Substation automation" since this is a term that may not be familiar to all, is likely to be familiar to substation owners – and those are the entities we are trying to reach. The SDT removed the proposed definition of "BES Reliability Operating Services" from the list of proposed definitions – so there is no conflict.

Comments on Attachment 1

One commenter indicated that Versions 1 and 3 of the CIP standards only required protection of the Blackstart initial or primary cranking paths and proposed retention of this approach.

The SDT modified the criteria in Attachment 1 so that Blackstart Resources and associated Cranking Paths are no longer included in the Attachment.

A commenter requested that the drafting team clarify whether the SDT contemplates that scheduling systems would adversely impact one or more BES Reliability Operating Services within fifteen minutes if rendered unavailable, degraded,

or misused (for example, does the potential for cyber attack on e-tagging systems before tags are loaded into EMS prior to the ramp suggest that scheduling systems should have a high or medium impact Rating?). In response, the drafting team has made changes to the approach that no longer uses the BES Reliability Operating Services. Rather, the approach is based on BES Cyber Systems that affect real-time functional tasks of the asset (in this case the Control Center). Scheduling and e-tagging is not generally considered a "real-time" operation.

Some commenters proposed that BES Reliability Operating Services encompass everything a utility does and use of this definition, by itself, would encompass all assets and expressed concern that the term, "BES" is under refinement, leaving entities in a position where they could potentially become instantly non-compliant in the event that the definition of BES changes. The SDT notes that the reliability functions provide the first step in a multi-layered filter intended to focus the most protection on those BES Cyber Systems that are most critical to reliability. The term, "Bulk Electric System" is a defined term today – and when the BES Definition team proposes revisions to this term those proposed revisions must be posted for stakeholder comment.

Other Comments

For consistency with the format of the other CIP standards being proposed, one stakeholder suggested putting the requirements into a table format and the SDT declined. The table format was developed for other standards where the requirements were subject to varying applicability. CIP-002 doesn't have the same variation with respect to applicability – Requirement R1 applies to all Responsible Entities.

Some commenters asked for confirmation of the distinction between lists that are bulleted and lists that are numbered. When a list in a requirement is bulleted, that is an indication that the responsible entity is required to meet the performance in at least one, but not all of the listed items. When a list in a requirement is numbered, that is an indication that under the specified condition, the responsible entity is required to meet the performance in each numbered item.

The SDT believes that the wording in each of the requirements clearly identifies the distinction between these cases.

One commenter proposed that the SDT revise the standard to align with the NISTIR 7628 SG.CA-3, Continuous Improvement High-level requirements by adding the concepts of "continuous improvement" and best practices. It is not the intent of the standards' requirements to specify best practices, but to clearly specify minimum requirements that must be made to provide the protection commensurate with the impact level. Certain requirements will include processes to ensure a specific action in response to changes, the concept of "continuous improvement" is hard to implement as an enforceable requirement sanctioned by penalties other than through clear and specific process actions.

Some commenters expressed a desire to include exemptions for smaller entities and proposed that the following be included: "Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have

no BES Cyber Systems" noting that the similar language was found in other CIP standards. The commenters noted that use of this exemption would require the identification of "no cyber systems" rather than "low impact assets" and proposed modifying the standards for greater consistency. In response the SDT notes that the exemption is for entities that have no BES Cyber Systems – the CIP standards apply to BES Cyber Systems, not cyber assets.

One stakeholder asked the team to define BES Elements and Facilities, however these terms are already defined in the NERC Glossary of Terms Used in Reliability Standards.

One stakeholder noted the use of the terms, "Associated Protected Cyber Asset" and "Associated Electronic and Physical Control and Monitoring Systems in the diagram used to explain "BES Cyber Systems" and questioned the use of these terms. On page 7 the diagram uses the term "Associated Protected Cyber Assets." The SDT has added more information on these terms in the revised standard's Background section and these terms are used in other CIP standards to help narrow the applicability for specific requirements.

Several entities asked for more clarity on the use of the phrase, "application of the required controls (last sentence of M1). Here the SDT uses the word, "controls" in reference to the procedures, processes, etc that are required for protection of the BES Cyber Systems in the other CIP standards.

One commenter asked what VSL would be associated with an update that was less than 30 days late. The SDT notes that VSLs are only referenced after a finding of noncompliance. If the actual performance of the responsible entity meets or exceeds the required performance there is no associated VSL. Another commenter noted that the VSLs for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified and identified that in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a low impact to determine the correct VSL; thus, requiring ALL low BES Cyber Assets being identified. The SDT revised the VSLs to remove this conflict. The revised VSLs in R1 are linked more specifically to failure to assign a Facility to the high or medium impact categories.

One commenter recommended modifying the "BES Reliability Operating Services" paragraph, by removing "BES" prefix to Cyber Assets and by eliminating a phrase that seemed redundant in the paragraph and the SDT did not accept these suggestions. Based on other comments and SDT discussions, the SDT revised the informational sections of the standard (as well as R1) to better distinguish between BES Cyber Assets and BES Cyber Systems.

Some commenters noted that the "Evidence Retention" section of the standard used the phrase "until found compliant" in the following: "If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer." The SDT has updated this sentence to reflect the latest language from the enforcement program "until mitigation is complete and approved".

One commenter indicated support for the approach of categorizing systems based on their impact on the Bulk Electric System and proposed having FERC or NERC define which Country Assets are critical for defense and stability of the nation and to define better that for which we are trying to stabilize and provide reliability, thus defining those "BES" components that should be high, medium, or low impact. The SDT applauds this idea, but it is beyond the scope of work assigned to the SDT. The work of the BES Definition team and the work of the Adequate Level of Reliability Task Force may provide more clarity on the issues associated with classifying "Country Assets" in the future.

One commenter asked for a specific implementation timeline for the compliance of the newly identified and categorized BES Cyber Asset(s) and/or BES Cyber System(s) and the SDT notes that this information is contained in the Implementation Plan.

A commenter asked about Section 4.1.2 in relation to smart grid devices being operated by Distribution Providers, or for smart grid assets 100 KV+. The SDT notes that there is no special consideration of "smart grid" devices. The CIP standards specify certain types of Facilities, Systems, and equipment that are included as in scope for applicability of the CIP standards. If the BES Cyber Systems for these Distribution Providers perform that function for the BES, they are in scope. Similarly, for assets at 100KV+, if the BES Cyber Systems for those assets perform the function for the BES, they are also in scope (e.g. PMUs when they affect real-time operations).

A commenter also suggested that battery storage is is not addressed by the standards. The SDT notes that the omission is intentional, since these may include other types of Cyber Assets (e.g., Electronic Access Control and Monitoring Systems).

QUESTION 4 – CIP-002 R2:

Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the rationale, requirement, measure, and VSLs associated with Requirement R2 of CIP-002-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Please see the redlined version of the standard for a complete set of revisions.

R2 should be modified to read “The Responsible Entity shall have its CIP Senior Manager or delegates approve the identification and categorization required by R1 initially upon an Annual basis, even if it has not identified High or Medium BES Cyber Assets or BES Cyber Systems.”

Response: The SDT has defined the specific time requirement.

For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months...”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year..." Similarly for “every 39 months...”.

To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc.

This wording precludes attempts to extend the word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z".

The SDT may want to consider that this requirement and all others that use the words “...initially upon the effective date of the standard...” have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It’s not reasonable to assume that every entity is capable of executing all procedures “upon the effective date”.

Minor point, but this is the first time “CIP Senior Manager” is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5.

In section “B. Compliance”, under sub-section “1.2 Evidence Retention”, there is a typo in the second to last line. Please change “complaint” to “compliant”.

Response: Changes were made to CIP-002-5 requirement R2 and Attachment 1 to address your comments.

Rationale R2 - Propose a content change:

a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized.

b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been

properly identified and categorized.

R2 - Proposed Change

a. Original Text - The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.

b. Proposed Change - The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1.

c. Rationale – We note instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.

M2 - Proposed Change

a. Original Text - Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2)

b. Proposed Change - Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2)

c. Rationale - The requirement only asks for Senior Manager (or delegate) approval. We note instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.

Response: Changes were made to CIP-002-5 requirement R1 and Attachment 1 to address your comments. Regarding R2 and the replacement of the language with the CAN-010 definition of annual, the suggestion was considered and rejected since the CAN is not meant to be a standard, but simply guidance for compliance enforcement authorities. The SDT has defined exactly what the requirement is.

Requirement 2 and Measure 2 contain the phrase "...initially upon the effective date..." We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.

If the Guidelines and Technical Basis section will remain in the final published version of the standard, the table on page 18 should be updated to include the Entity Registration of Load Serving Entities with consideration of an "X" in the functional rows of "Dynamic Response", "Balancing Load and Generation" and "Controlling Voltage".

Response: The drafting team agrees with your comment and will remove the “upon the effective date of the standard” from the text.

We do not disagree with the requirement for the CIP Senior Manager or delegate approval. There are clear definitions of the necessary bookends. However, we are concerned that given the recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry.

Response: Regarding R2 and the replacement of the language with the CAN-010 definition of annual, the suggestion was considered and rejected since the CAN is not meant to be a standard, but simply guidance for compliance enforcement authorities.

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won’t accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories.

Response: Approval of the lists of Critical Assets and Critical Cyber Assets has been a requirement of CIP-002 in all versions. The SDT believes that an explicit approval of the lists by the Senior Manager or delegate is important as these lists are the foundation for the scope of applicability of the rest of the CIP standards.

The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. The requirement should direct an entity to develop their Cyber Asset lists. Furthermore, the entity is directed to perform a review and approval process. The level of review and approval should be determined by the entities governance model, organizational structure, compliance culture, etc. It is inappropriate for

the CIP Standards to dictate how the organization manages cyber security requirements or compliance with regulations.

Response: Version 5 is scoped to complete changes responsive to FERC Order 706.

This should be stated clearly that this initial and annual review applies to all BES Cyber assets impact levels, regardless if the entity has not identified High or Medium BES Cyber Assets or BES Cyber Systems.

Response: The requirement for review and approval applies to list required in R1.

a. To add clarity to CIP-002-5 R2, any change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems in between the "once each calendar year" review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval.

b. It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.

Response: There is no requirement to have the CIP Senior Manager or delegate approval of the identification and categorization other than that specified in R2, which is once every year. The requirement language "at least once each calendar year, not to exceed 15 calendar months between approvals" allows sufficient flexibility for the Responsible Entity to manage this periodic compliance.

AZPS recommends changing the language "initially upon" to "prior to". In M2 of R2, the phrase "review and update, where applicable" should be replaced with "review and approve".

Response: Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

We recommend that the Senior Manager could approve "prior to or initially upon".

In general, with regard to the proposed CIP Version 5 Standards, it is unclear whether all the requirements have to have been completed at least once prior to the effective date? In some cases, the standard requires that the entity perform some function initially upon the effective date and then have a follow-up requirement (e.g. update cyber security incident plan within 30 days). NERC should provide further guidance in regards to implementation of CIP Version 5 in this regard.

Response: The SDT will take the proposal into consideration. The drafting team agrees with your comment and will remove the "upon the effective date of the standard" from the text.

In M2. Reference to CIP Senior Manager should include "and delegate".

Response: Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

We would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to effective date of the standard.”

Response: The drafting team agrees with your comment has removed the “upon the effective date of the standard” from the text. Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

For clarity in R2 and M2, request 1) using the term “annual” instead of all these extra words and 2) making “annual” a Glossary term

Response: The term “annual” is used in many other NERC standards. The SDT opted to include the specific periodic language in the requirement itself to avoid repercussions in other NERC standards.

The assumption is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R2 will not apply to those utilities.

Response: Responsible Entities that own assets qualified under the registration criteria are included in section 4.

”Upon the effective date” should be restated to read “on or (within 30 days) prior to. A list of Low impact BES facilities is not required to be maintained, however, certain standards require controls to be enforced at these facilities. At the very minimum, the standard should require that the RE’s approval of High and Medium lists should include a list of facilities and systems considered as potential candidates for the evaluation.

Response: The SDT will take the proposal into consideration. The drafting team agrees with your comment and will remove the “upon the effective date of the standard” from the text.

Should it not read delegate(s) instead of just delegate? There could be more than one delegate.

The measure makes no mention of the delegate(s) approval? Need consistency between the Requirement and the measure.

1.2 Evidence Retention: Please explain what “Other evidence” would be required.

Response: As an example, if the requirement is to keep 90 days of event log entries, the Responsible Entity is not required to keep the event logs for the full compliance period between audits, but to be able to produce evidence that these logs have been retained for 90 days on a rolling basis during that period. Evidence could be logs of the process that

ran to implement the 90 day rolling event log.

We believe R2 should say “initially prior to or upon the effective date of the standard...” Without that, it would seem the CIP Senior Manager or delegate(s) would need to approve the lists precisely on the effective date.

Response: The drafting team agrees with your comment and has removed the “upon the effective date of the standard” from the text. Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

CIP-002 R2: a. The following wording should be added to the Measure in CAPs,"

BES Cyber Assets and BES Cyber Systems initially upon....." should become "High and Medium Impact BES Cyber Assets and BES Cyber Systems initially upon....."

Evidence Retention comment:

1.2 We recommend the deletion of the following sentence "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." as it contradicts the requirement to retain the data for three calendar years.

Response: The SDT will take the proposal into consideration.

R2 Rationale CHANGE: “Manager’s approval” TO: Manager’s responsibility in approval”

RATIONALE: the Senior Manager or delegate performs an approval, but the responsibility remains with the Senior Manager.

Response: The SDT will take the proposal into consideration.

Why does this need to be a recurring requirement? Upon identification and categorization, there are typically no changes and those that do change are typically addends. All I am saying is that this requirement asks for every Responsible Entity to do an exercise even if a large majority of the entities will have a similar or identical result as the previous year. I don't see the point.

Suggest: "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and upon Cyber Asset or Cyber System changes."

Response: The SDT will take the proposal into consideration.

General - For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.

Response: The SDT will take the proposal into consideration.

CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be changed in one of the following:

1) plainly state those entities with no BES assets per the definition are not required to adhere to this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no Cyber Assets; or,

2) create a fourth category stating No Impact, thus no further action required which can be certified annually by the Senior Manager.

Response: The SDT is aware of the DP and LSE issues and will consider your response.

QUESTION 5 – CIP-002 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

All comments not directly related to VRFs/VSLs for CIP-002-5 are addressed in Question 2.
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.

Response: The drafting team debated and developed the Table of Compliance Elements along with VRFs and VSLs to simplify and account for risk and severity measures with respect to the reliability of the BES.

Issue - We believe that the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.

Response: Violation Severity Levels are a measure of performance towards a standard independent of the size of the registered entity, and the drafting team developed the VSLs for the cyber security standards to account for the wide range of entity configurations and systems. The drafting team included both percentages and fix numbers of BES Cyber Systems and BES Cyber Assets in the VSLs to account for the wide range of entities with an objective toward reaching a

more equitable effect of the requirements on all entities.

The VSL table should refer to BES Cyber Assets and BES Cyber Systems (not just BES Cyber Assets) as does Requirement R1 for consistency with terminologies used in R.1 & R.2.

Response: The language of the VSLs will be revised.

Percentages of non-compliance are difficult to determine; using discrete numbers of non-compliant assets would be preferable in determining the R1 VSL. This is particularly true where random sampling of the entity's assets is performed and the number of failures is derived by extrapolation.

Response: The VSLs were developed to account for the wide range of entity configurations and systems. The drafting team included both percentages and fixed numbers of BES Assets in the VSLs to account for the larger and smaller entities with an objective toward reaching a more equitable effect of the requirements on all entities.

Additionally, the R1 VSLs refer to entities with more than 100 High and Medium Impact BES Cyber Assets (or 100 or fewer such assets). Is this count determined by the entity's determinations prior to the audit or is the count determined by the auditor, adjusting the entity's initial determination upon finding a possible violation?

Response: The methods and processes used to determine compliance with the requirements is a compliance process question and should be addressed to NERC's Compliance Department to achieve a consistent approach and determination.

The standard refers to BES Cyber Systems as well as BES Cyber Assets. It appears that the VSL requires the compliance monitoring and enforcement staff determining the VSL to break down each BES Cyber System into its BES Cyber Asset components in order to achieve the correct determination. As the bright line criteria remove any subjectivity from the categorization process, the R1 VSL should be binary. Either the entity got it right or the entity did not. There should be only one VSL, that being "Severe." Similarly, the R2 requirement is very straightforward and a binary VSL is appropriate in that instance.

Response: The language of the VSLs will be revised to include both BES Cyber Systems and BES Cyber Assets. The methodology and process used to determine compliance with the requirement is a compliance process question and should be addressed to NERC's Compliance Department to achieve a consistent approach and determination.

The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. EEI would like a more risk based approach in which the compliance assessment considers risk in any non-compliance finding.

Response: The drafting team debated and developed the Table of Compliance Elements along with VRFs and VSLs to simplify and account for risk and severity measures with respect to the reliability of the BES. Violation Severity Levels are a measure of performance towards a standard independent of the size of the registered entity, and the drafting team developed the VSLs for the cyber security standards to account for the wide range of entity configurations and systems. The drafting team included both percentages and fix numbers of BES Cyber Systems and BES Cyber Assets in the VSLs to account for the wide range of entities with an objective toward reaching a more equitable effect of the requirements on all entities. The Violation Risk Factors are designed to assess the impact to reliability of violating a specific requirement, and to determine an appropriate sanction when the associated requirement is violated (refer to the ERO Sanctions Guidelines document). When a single requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, following the FERC Order of May 18, 2007, the VRF assignment must not be watered down to reflect the lesser risk level. The drafting team defined the VRFs for the cyber security standards in accordance with these guidelines.

For the Last Paragraph VSL's within R1 (failed to update its documentation), we propose the following time periods:

Lower - More than 30, but less than or equal to 60 calendar days

Moderate - More than 60, but less than or equal to 70 calendar days

High - More than 70, but less than or equal to 80 calendar days

Response: The portion of the VSL for R1 that refers to the number of calendar days taken to update its documentation following the completion of a change to the BES Asset or BES System categorization will be revised by the Drafting Team.

We propose that documentation errors should rarely if ever be deemed high/severe. Only violations that could have an immediate impact on the reliability of the BES should be considered high/severe.

Response: The omission of a BES Cyber Asset in the documentation required in CIP 002 may not always be a documentation error. The omission could be a result an incorrect application CIP-002 resulting in a BES Cyber Asset being incorrectly classified and protected under the requirements stated in CIP-003 to CIP-011. While the drafting team agrees that the updating of documentation as an isolated incident is not severe, the updating of documentation associated with the identification and categorization of its BES Cyber Systems and BES Cyber Assets is critical to the reliability of the BES, since it could lead to inadequate security measures or erroneous operations.

The severity levels are determined by, among other things, the number of low impact cyber assets that are categorized improperly. The entity is not required to keep records of low impact cyber assets. This approach will not work.

Response: The severity levels are determined by the impact of the BES Cyber System or BES Cyber Asset on the reliable operation of the BES if the BES Cyber System or BES Cyber Asset is destroyed, degraded, or otherwise rendered

unavailable. The Low Impact BES Cyber Systems or BES Cyber Assets are not required to have discrete identification.

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES Cyber Assets or BES Cyber Systems. The VSLs drop the "or delegate" language which implies the CIP Senior Manager has to approve the categorization and identification. The "or delegate" language should be added back.

Response: The drafting team agrees with your comment and will insert the "or delegate" language as indicated in the VSLs for R2.

R2 VSL - We do not believe that being late by 30 to 40 days is adequate since this a mere review of the list each year. We suggest changing the LOWER to "30 to 60 days", then have 10 day increments for the rest of the VSL such as "60 to 70 days" for MEDIUM, "70 to 80 days" for High, and "80 to 90 days" for SEVERE.

Response: The drafting team believes that the current range of days for review and approval of the required categorization of BES Cyber Systems and BES Cyber Assets is appropriate and commensurate with the due diligence that is required by CIP 002.

The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.

Response: CIP 002, which is the scoping standard, is the foundation for CIP Version 5 Cyber Security standards. The CIP-002 standard is designed to identify and categorize the BES Cyber Systems and BES Cyber Assets that if destroyed, degraded, or otherwise rendered unavailable can potentially impact the reliable operation of the BES. An error in addressing the requirements of this CIP standard could result in the incorrect or inappropriate application of controls listed in standards CIP 003 to CIP011. Hence, the drafting team believes that the VSL severity levels for this standard are appropriate.

In general, regarding VRFs in each of the CIP standards, it is our understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement. For instance, the VRF should be used to differentiate between violating the Disturbance Control Standard (BAL-002), and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRF's should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF's are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on

VRF determination, or the SDT should split the requirements so that appropriate VRF's can be applied.

Response: The Violation Risk Factors are designed to assess the impact to reliability of violating a specific requirement, and to determine an appropriate sanction when the associated requirement is violated (refer to the ERO Sanctions Guidelines document). The VRF is not meant to compare the severity of the reliability impact of one requirement with another. When a single requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, following the FERC Order of May 18, 2007, the VRF assignment must not be watered down to reflect the lesser risk level. The drafting team defined the VRFs for the cyber security standards in accordance with these guidelines. The drafting team recognizes the possible extraordinary level of effort required to protect the numerous Low Impact BES Cyber Systems and BES Cyber Assets, and therefore strived to minimize the potential workload of protecting the Low Impact BES Cyber Assets and BES Cyber Systems by limiting the specific requirements that are applicable to those BES Assets. The drafting team believes that the VRFs for this requirement are appropriate.

Under the Table of Compliance Elements is included the phrase "Operations Planning" under the "time horizon" column. The industry cannot predict with certainty future upgrades and additions to the system, yet the standard appears to state that VSL apply to the planning time horizon under the "time horizon" column. It may be that the standard intends to apply to operations only, but this is not clear in the text since both "Operations" and "Planning" are capitalized. Please clarify.

Response: The meaning of the entries in the "time horizon" column in the Table of Compliance Elements is defined by NERC. The "Operations Planning" timeframe is defined as "operating and resource plans from day-ahead up to and including seasonal", and "Real-time Operations" is defined as "actions required within one hour or less to preserve the reliability of the bulk electric system". Please refer to the NERC Time Horizons document at http://www.nerc.com/files/Time_Horizons.pdf.

While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies.

Recommend Low, Medium, High and Severe VSL's for all requirements.

Response: The VSLs were developed to account for the wide range of entity configurations and systems, as well as the specific requirements. Some of the requirements are "binary" in nature (either the entity meets it or it doesn't), and a partial compliance is not possible. Following FERC's June 19, 2008 Order on Violation Severity Levels, these binary VSLs are by definition Severe.

This standard has a high VRF that applies to requirements for both high and medium impact asset categories. We

recommend a medium VRF for the medium impact assets to recognize the difference between asset impact categories.

Response: CIP 002 R1 includes the classification of all BES Cyber Assets into appropriate impact categories. An error or omission on the part of an entity in the performance of the tasks required by the standard or in the upkeep of documentation that is proof of performance of these tasks could result in an asset being incorrectly classified or completely omitted from classification. The result of such an error would cascade to the application of the controls stated in CIP 003-CIP011 and hence jeopardizing the reliability of the BES due to the incorrect application of cyber security controls. The Higher VRF associated with this requirement is due to these reasons. The VRF does not apply just to the classification of assets as Low Impact but rather to the entire process by which such a determination is made. Requirement R2 carries a lower VRF since the task associated with this requirement is a demonstration of senior management involvement and approval of the entity's BES Cyber System and BES Cyber Asset identification and categorization. The drafting team believes that the VRFs for this requirement are appropriate.

"And" needs to be struck from moderate and high VSL in the phrase "High and Medium Impact and BES Cyber Assets".

The drafting team agrees with your comment and will remove the extra "and" from the Moderate and High VSL language for R1.

We are concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. This overall proposal is not substantive enough to objectively assess VSRs and VSLs. We recommend that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.

Response: The drafting team is keenly aware of the possibility to inadvertently require entities to produce a list of Low Impact BES Cyber Assets, and included language in the standard to avoid the generation of the list of Low Impact BES Assets. The wording states that "discrete identification" of Low Impact Assets is not required.

We recommend that the high VRFs and VSLs are extreme and the definition of what is high, medium, or low violations are unclear and need to be clearly defined in order to show how entities can fully comply.

-No mention of BES Cyber Systems throughout the VRF/VSL, only mentions BES Cyber Assets.

-R2: There is no mention of the delegate(s) completing the annual review. Delegate is called out in the requirement.

Response: The VSLs were developed to account for the wide range of entity configurations and systems, as well as the specific requirements. Some of the requirements are "binary" in nature (either the entity meets it or it doesn't), and a partial compliance is not possible. Following FERC's June 19, 2008 Order on Violation Severity Levels, these binary VSLs are by definition Severe. The Violation Risk Factors are designed to assess the impact to reliability of violating a specific

requirement, and to determine an appropriate sanction when the associated requirement is violated (refer to the ERO Sanctions Guidelines document). When a single requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, following the FERC Order of May 18, 2007, the VRF assignment must not be watered down to reflect the lesser risk level. The drafting team defined the VRFs for the cyber security standards in accordance with these guidelines.

The language of the VSL requirements will be revised to include "BES Cyber Systems" in R1 and "or delegate" in R2.

Seems like if you incorrectly categorized or missed 5% or fewer of your assets, by default you are automatically put into the Severe VSL range as it most likely will have been more than 60 days since the BES Cyber System was identified or categorized. If it only covers major changes to facilities and elements and not cyber systems, it would not be a concern - but this would need to be spelled out.

Response: Please note that there are multiple parts to the VSL definition for R1. One part requires an entity to correctly identify and categorize its BES Cyber Assets and BES Systems, and the second part refers to the number of calendar days taken by the entity to update its documentation following the completion of a change to its BES Cyber Systems or BES Cyber Assets. The first part of the VSL is in relation to the identification and categorization of BES Cyber Systems and BES Cyber Assets that have a High or Medium Impact on the reliable operation of the BES. If an entity incorrectly identifies or categorizes 5% or fewer of these assets at a lower category, then the entity will be in violation of the CIP-002-5 standard.

If an entity implements a change to the BES that is planned to be in service for more than 6 calendar months and it causes a change in the identification or categorization of its BES Cyber Assets or BES Cyber Systems from a lower to higher impact category, then the change needs to be documented within 30 calendar days of its implementation.

The type of change (major, minor, or other) is not addressed since the drafting team is concerned about the reliability of the BES and the impact of any change to the BES Elements that results in a change to the identification and categorization of the BES Cyber Systems or BES Cyber Assets.

VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.

Response: The comment requires changes to the compliance methodology and processes that must be addressed by the NERC Compliance Department and is out of scope of the drafting team for this standard.

In general, the VSL should relate to reliability and not administrative errors.

Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation

management VSL model may offer an alternative model to follow.

Response: An "administrative error" resulting in the failure to identify a High or Medium Impact BES Cyber Asset or BES Cyber System could potentially result in the BES Asset not being afforded the protections mandated by the NERC CIP Standards. The drafting team strived to define VSLs that are related to the reliable operation of the BES and to limit the effect due to administrative errors. However, administrative errors also need to be recognized and corrected in a timely manner. The SDT will examine the VSLs for FAC-003 for consideration.

QUESTION 6 – CIP-003 R1:

CIP-003-5 R1 states "Each Responsible Entity shall identify, by name, a CIP Senior Manager." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R1 and Part 1.1 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Industry comments raised a number of valid issues with CIP-003-5 R1. Many commenters were concerned with the reordering of the requirements. The opinion of the SDT in developing the first draft of version 5 was that the designation of the CIP Senior Manager should come prior to the requirement for Cyber Security Policy. However, the SDT was persuaded by industry comments and restored R1 as the Cyber Security Policy and moved the requirement to identify a CIP Senior Manager to Requirement R3. Other requirement ordering in CIP-003-5 may still impact existing compliance

documentation, however.

For instance, some commenters requested that requirements for low impact assets be collected and presented in a single location. The SDT agreed with this approach and modified the standards to include a single policy requirement for low impact BES Cyber Systems and included it as R2. This will displace the existing numbering for CIP-003-4, but compliance documentation impacts were unavoidable as several requirements from CIP-003-4 were either removed entirely or relocated to other standards.

Several entities raised concerns about the requirement to have a single senior manager. This was a key point of FERC Order 706 and as such is still included in the requirement. However, it should be noted that it is not the intent of the SDT or this requirement to dictate a particular organizational structure. Some comments were raised concerning repeating the phrase which defines the CIP Senior Manager in the language of the requirement itself. In drafting the CIP Standards, the SDT attempted to remove all cases which required an explicit cross reference to a requirement in another standard. As such, the SDT proposed a definition of CIP Senior Manager to be included in the NERC Glossary. This definition adequately clarifies the authority and responsibility of the CIP Senior Manager.

Additionally, commenters raised concerns, in this requirement and others, about specific examples included in the measures. To be clear, the measures are not mandatory or enforceable. In some cases, it is true that in the measures the SDT mentions items not specifically included in the language of the requirement. The SDT is attempting to use the measures as a tool to provide guidance about what may be considered high quality evidence, not to indicate any particular required performance, and encourages the industry to read them in the context in which they were intended.

QUESTION 7 – CIP-003 R2:

CIP-003-5 R2 states "Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R2 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address

the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Many comments raised valid concerns that some topics that were required to be included in the policy for low impact BES Cyber Systems were not addressed elsewhere in the CIP Standards. The SDT appreciates this concern and in response has drafted a separate policy requirement specific to BES Cyber Systems not identified as high impact or medium impact - see Requirement R2 in the revised standard. (Policies for high and medium impact BES Cyber Systems were moved to Requirement R1 in the revised standard.)

Some commenters requested additional specificity to be included as to the nature of the cyber security policy. The SDT believes that in order to have effective policies, organizations need the flexibility to write policy in a manner in which is compatible with their corporate culture. As such, the SDT has allowed for flexibility to have higher level policies as well as very detailed policies.

A number of commenters raised concerns that the requirement to “implement” the cyber security policy may raise double jeopardy concerns with other CIP Standards. The SDT is very concerned about possibilities of double jeopardy, but disagrees that there is a double jeopardy issue here. The policy does not have the same level of granularity as the other requirements and the SDT does not believe that a violation of another CIP requirement would constitute a violation of the policy requirement. The “implement” language was added to the policy requirement as a result of FERC Order 706 paragraph 75 and the intent is for the Responsible Entity to demonstrate that it has not written a policy and put it on a shelf somewhere but is actively using it and abiding by its statements.

> Order 706, Paragraph 75: Consistent with that proposal, the Commission concludes that, where the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, there should be a corresponding obligation to implement the plan, policy or procedure. However, while the CIP NOPR proposed to interpret the CIP Reliability

Standards as including an implicit obligation to implement plans, policies and procedures, we are persuaded by the commenters that a better approach is for the ERO to develop modifications to the CIP Reliability Standards that contain appropriate implementation language. Accordingly, we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards.

Also, of concern to the SDT were comments that suggested that the policy requirement was administrative in nature or simply a documentation burden. The SDT disagrees that security policies are administrative in nature because they require documentation. The SDT believes that security policies are essential for an organization to ensure an effective security posture. Security policies were a concern identified in both the FERC Order No. 706 as well as the 2003 Blackout Report.

In addition, a number of commenters expressed a preference for all modifications to the language to return to the previously vetted and approved language of version 4. The SDT appreciates the concern about the use of previously approved and vetted language and has attempted to retain this language wherever possible. Some of the changes in language are a result of directives from FERC Order 706 while others are made based upon industry feedback.

Additionally, the SDT has attempted to bring the CIP standards in line with the NERC Results Based Standards format. As such, there were a number of language changes made based upon the requirements structure identified in the NERC Results Based Standards format. While the drafting team agrees that there is value in utilizing previously vetted language where possible, it believes that the migration to the NERC Results Based Standards format is the best approach for the future evolution and maturation of the standards.

QUESTION 8 – CIP-003 R3:

CIP-003-5 R3 states "Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address

the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Several commenters noted that the language of the proposed CIP-003-5 R3 was unclear. The SDT has attempted to reword the requirement to provide clarity as to the intent. The SDT removed the phrase, "initially upon the effective date of the standard," and rearranged the sequence of information in the requirement but did not otherwise change the scope or intent.

Additional comments questioned the need for annual approval of the policy, particularly in situations where updates to the policy are not needed. The SDT believes that the periodic approval reaffirms management's commitment to the protection of its BES Cyber Systems. A few commenters also suggested an allowance for the policy to be approved by a delegate of the CIP Senior Manager. While the SDT appreciates this desire, the SDT believes that this is one area that must be approved by the CIP Senior Manager and not a delegate. This is consistent with previous versions of the CIP Standards.

QUESTION 9 – CIP-003 R4:

CIP-003-5 R4 states "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R4 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address

the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Industry highlighted a number of concerns around the clarity of the proposed language of CIP-003-5 R4 and the potential overlap with the existing training and awareness program in CIP-004-5. The SDT was persuaded by these comments and has proposed the deletion of R4 with a corresponding addition in CIP-004-5 to explicitly require annual training on the cyber security policy (see CIP-004-5, Requirement R2, Part 2.2 and Requirement R3, Part 3.2).

Several commenters also requested that the list of acceptable types of evidence to support compliance in Measure M4 be either removed or clarified. The Standard Drafting Team responded that it did not intend the measure to be an exhaustive list of acceptable forms of evidence, but rather a list of possible examples.

Commenters also argued that this requirement should apply to onto those entities that have High Impact or Medium Impact BES Cyber Security Systems. The SDT responded that to ensure the overall culture of security for the industry, these are minimum areas that should be implemented by all owners of BES Cyber Security Systems.

QUESTION 10 – CIP-003 R5:

CIP-003-5 R5 states "The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated." Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R5 and its associated rationale and

measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Many commenters raised concerns about the significant overhead that may be required to track multiple levels of delegations. The SDT is persuaded that the documentation required to maintain documentation of multiple levels of delegations may be burdensome to some organizations. As such, the SDT has proposed language closer to the existing approved language of version 4 which did not explicitly allow for sub-delegations.

Additionally, the SDT believes that the additional flexibility allowed with the ability to delegate by title will make this proposed standard less burdensome, without any decrease in effectiveness, over previously approved versions of the standard.

A number of commenters noted the discrepancy between the written R5 Requirement and the measure that according to the requirement, delegates can be documented "by position or name of the delegate" yet the measure states that the document must include an actual name. The requirement and measure have both been rewritten to clarify that the document may include either the name or the title of the designee.

A number of commenters also raised questions about the consistency of the use of the term position vs. title. The SDT has revised the standard with consistent language using "title".

QUESTION 11 – CIP-003 R6:

CIP-003-5 R6 states "Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R6 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

There were 3 primary issues raised by commenters concerning CIP-003-5 R6. First, commenters rightfully pointed out that the reference to the footnote was not properly superscripted. The SDT determined that the footnote should instead be included in the language of the requirement itself and the superscript "2" was deleted.

Several commenters made reference to revert the language back to the previously approved language of version 4. The SDT interpreted this to mean that the commenters preferred that the requirements to update the CIP Senior Manager and delegate should be included as separate sub-requirements. The SDT appreciates the desire to use the previously vetted and approved language. However, the change to explicitly call out updates to the CIP Senior Manager and the delegation in a single requirement (instead of sub-requirements of other requirements) allows for consistency with respect to the VRF and VSL for the requirement to have up-to-date documentation. As it exists in the version 3 standards, an update to a delegation outside of the 30 day window would constitute a violation of CIP-003-3 R2.3 instead

of CIP-003-3 R2.2 where the proper VSL is aligned with the activity.

Additionally, a few commenters requested that the SDT allow additional time to update documentation beyond 30 days. The SDT has chosen to keep the currently approved time window of 30 days in an effort against creating a situation where we are lessening the current level of compliance, which is not allowable without significant justification to the Commission and other governmental authorities.

QUESTION 12 – CIP-003 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for R1, R3, and R4, and only minor or no changes to the VSLs for R2, R5 and R6. The SDT also changed the VRF for M3 from "Lower" to "Medium".

Please see the redlined version of the standard for the complete set of revisions.

A number of good concerns were raised by commenters regarding the VSLs and VRFs. Overall, commenters expressed a desire for additional granularity and reduction of severity with regards to VSLs. The SDT agrees with many of the comments that additional justification for VSLs and VRFs is needed. The VRFs and VSLs are based upon guidelines developed by NERC and FERC, and the SDT has provided an analysis of the VSLs and VRFs based upon these guidelines. One item of note was concern that the VSL for R4 was inconsistent with the stated SDT intent that awareness of the policy did not imply that this awareness should be investigated on an individual by individual basis. This issue has been resolved by the deletion of R4 and the introduction of cyber security policy as an explicitly required element of the training program in CIP-004-5.

Additionally, the core of several comments for additional granularity appeared to center around the severity as it may relate to multiple violations. The NERC and FERC guidelines make clear that VSLs should be written to account for single violations and not cumulative violations. As such, in many cases, additional granularity is not warranted.

Several commenters also expressed concern about the VRF level for the identification of the CIP Senior Manager. The SDT notes that this VRF is based on the VRF in previously approved version of the CIP-003.

QUESTION 13 – CIP-004 R1:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to Requirement R1 but did make significant changes to Part 1.1 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has reassessed the overall scope and applicability during the comment review period, and has concluded that CIP-004-5, R1 represents an approach which is a reasonable effort to advance the cyber security of the Bulk Electric System and critical infrastructure overall.

After review of the comments, the SDT updated the requirements with a goal toward improved clarity, while trying to maintain a balance of reasonable security awareness and to moderate audit impact. The changes to Requirement R1 include the following:

• Table R1: In response to several commenters asking for clarification as to who at the Responsible Entity should receive

security awareness information, the SDT has added the term “personnel” to the requirement.

• In response to comments that quarterly awareness is too frequent, the SDT made no changes because the team believes the current requirement of quarterly security awareness is appropriate for Version 5. Note that the measure for this requirement provides several ways an entity may demonstrate that it has implemented a security awareness program. In addition, the SDT narrowed the scope of entities that must comply to just the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to High and Medium Impact BES Cyber Systems.

• In response to concerns that R1 indicates that each of the applicable items in Table 1 are to be implemented, the SDT notes that even though there is only one Part, using “applicable items” is consistent with the rest of the standard, and the “applicable items” references the required elements of the requirement part language that a security awareness program must convey ongoing cyber security awareness of both authorized electronic and authorized unescorted physical access.
• In response to comments that the requirement in the table uses unmeasureable terms; such as a program that "conveys" security awareness, and the term "on-going" reinforcement, the team made no changes. The intent of R1 is to require all Responsible Entities who have High and Medium Impact BES Cyber Systems to have a security awareness program that communicates (“conveys”) information to personnel that supports and informs effective security practices. The use of the term “access” covers both authorized unescorted physical access and authorized electronic access. The term “on-going” is used in the current standards and repeated in Version 5 to help with consistency.

• In response to comments that the capitalized term “Facilities” needs to be clarified in the Applicability section of the standard, the team has reviewed the Applicability sections of each standard to address the consistency issue. The capitalized term “Facilities” refers to the definition in the NERC Glossary of Terms.

• In response to comments that clarity and consistency is needed between the requirement and the Implementation Plan, the team has revised the Implementation Plan to clarify compliance on the Effective Date.

•In response to concerns to be “compliant” with requirements that simply rely on documentation, the drafting team believes documentation is appropriate for demonstrating compliance with the standards.

In addition, several commenters provided comments specific to Requirements other than Requirement R1, and those comments are addressed in the summary responses for the appropriate questions.

QUESTION 14 – CIP-004 R2:

CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program for personnel who need 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R10 and to each of its Parts (2.1 through 2.10) and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has reassessed the overall scope and applicability during the comment review period.

After review of the comments, the SDT updated the requirements with a goal toward improved clarity. The changes to Requirement R2 include the following:

•In response to comments that Requirement R2 precludes an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems, it is not the intent of the team to preclude a single, comprehensive cyber security awareness and training program; however, all requirements of Requirement 1 and

Requirement 2 must be met.

•In response to comments that Requirement R2 should be reworded from "...contains the proper policies..." the SDT agrees, and has made the proposed change in the Rationale for Requirement R2 by adopting the phrase, "…covers the proper policies…".

•In response to comments as to whether the role-based training approach adequately addresses Order 706, Paragraph 435, the team believes the awareness and training programs adequately address FERC Order 706, Paragraph 435.

> Order 706, Paragraph 435: Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.

• In response to comments that FERC Order 706, Paragraph 435, calls for identifying what "…role and steps should be taken by the ERO to ensure quality and consistency of trainers," that Requirement R2 should identify what areas of the standards that the training program must include, the SDT discussed the issue of adequate training for the trainer and agreed that trainers do not need any special certification beyond the CIP training provided to personnel. The SDT believes the awareness and training programs adequately address FERC Order 706, Paragraph 435.

•In response to several comments suggesting Requirement R2 Part 2.2 should be eliminated, the SDT has removed Part 2.2 from Table R2. Requirements R2 Part 2.3 2.4 adequately capture the requirement.

•In response to several comments suggesting Requirement R2 Part 2.6 word change from "Original - Training on handling of BES Cyber System Information and storage media." The SDT agrees that the result of the requirement should provide training and handling on BES Cyber System Information and its storage (without specifying "media" and has modified the language to remove the word "media."

•In response to clarify wording in the requirement to make explicit Parts 2.7 and 2.9, the SDT believes Parts 2.7 and 2.9 in Table Requirement R2 should remain separate entries. The training requirement on connectivity has been modified to clarify the content should focus on the risks of a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets. The SDT has clarified the Applicability for the training on the visitor control program to include both physical and electronic access.

•In response to comments that the statement, "Define the roles that require training," implies that some roles do not require training, the SDT agrees and has modified the language in Requirement R2 Part 2.1 of Table R2 to use "identification" instead of "define".

•In response to concerns that CIP-004-5 R2 and CIP-004-5 R3 need to be consistent, the SDT has modified the

Applicability column in Table R2 to be consistent with Table R3.

•In response for clarification as to whether training on the visitor control program includes both electronic and physical access, the SDT has clarified the Applicability for the training on the visitor control program to include both physical and electronic access. The training for a visitor control program should focus on the responsibilities for each role designated by the entity that participates in the program; e.g., it is important to train individuals who serve as escorts on their roles.

•Requirement R2 Part 2.10: In response to comments concerning role-based training on the BES Cyber System's interconnectivity and interoperability with other cyber systems, the team has modified the requirement for clarification that the content should focus on the risks of a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets. The team has modified Requirement R2 Parts 2.3 through 2.10 to require "training content," and added examples in the Measures.

•In response to requests for clarification on role-based training, comments that Parts 2.3 and 2.5 be combined, and that Part 2.7 should also be deleted and its concepts combined with Part 2.9, the team has added "and training required for each role" to Part 2.1 of Table R2. However, the SDT disagrees with the combination of Parts 2.7 and 2.9, as these address different activities.

•Requirement R2 Part 2.3: In response to comments that the phrase "proper use" of physical access controls is not consistent, the SDT agrees and has removed "proper use" from Part 2.3 of Table R2.

•In response to comments that the requirement should include Cyber Assets as well as Cyber Systems, the SDT has modified the Applicability section to include associated Physical Access Control Systems and associated Electronic Access Control or Monitoring Systems for High and Medium Impact BES Cyber Systems.

•In response to comment that the "Delivery of cyber security training to vendor support staff on site at a Registered Entity's facility can be difficult to document," the SDT would request specificity regarding the challenge of documenting training to vendor support staff. The Responsible Entity may allow vendor attestations in accordance with its policies, practices, and procedures.

•In response to concerns that the requirement has the potential to be highly violated and that may or may not prevent a physical or cyber event, the SDT disagrees. The team believes that this requirement is necessary, it provides the requirements to be met for an entity's training program.

•Measure M2: In response to comments to change the word "must" in M2, the team was attempting to make a distinction by using the word, "must" for instances where the Responsible Entity "must" have something as evidence. Since there are many ways of demonstrating "how" an entity has implemented a procedure, the word, "may" has been

used ahead of samples of performance that may be acceptable.

•Requirement R2 Part 2.1: In response to suggestions that Part 2.1 require the role definitions to be reviewed on an annual basis, the SDT notes that Requirement R2 specifies what must be included in the training, and Requirement R3 requires when and how frequently the training required in Requirement R2 must be conducted.

•In response to suggestion that the term "Storage Media" be defined, the drafting team has removed the term "media" from Requirement R2 Part 2.6 and the associated measure.

QUESTION 15 – CIP-004 R3:

CIP-004-5 R3 states "Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3 and Parts 3.1 and 3.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

After review of the comments, the SDT updated the requirements with a goal toward improved clarity. The changes to

Requirement R3 include the following:

•In response to suggestions of changing “each individual needing authorized electronic” to “each individual with authorized electronic,” the SDT modified the language to “to attain and retain” authorized electronic or unescorted physical access.

•In response to suggestion of changing the phrase “associated with,” the SDT has revised the Applicability sections to help clarify the meaning of the term “Associated” as it is used with Physical Access Control Systems, Electronic Access Control or Monitoring Systems, or Protected Cyber Assets.

•In response to several comments that Tables in Requirement R3 apply to only High and Medium impact assets, the SDT notes that it has moved the requirements for Low Impact BES Cyber Assets into CIP-003-5 to emphasize the programmatic nature of these controls, which further clarifies that the requirements do not apply to “Low Impact”

•In response to suggestions that Requirement R3 Parts 3.1 and 3.2 should clarify the required training is role-based, the SDT agrees and has modified Requirement R3 to include a reference to “role-based.”

•In response to requests for clarification of Requirement R3 Part 3.2, "annual" training as being completed within 15 months, the team reviewed the requirement, and believes inclusion of 15 months to complete training in Part 3.2, Table R3, does not preclude an entity from using only the once every calendar year timeframe. When an individual is assigned a new role, the training should be completed prior to granting new access, not within 30 days.

•In response to request to clarification of Requirement 3.1 on whether all personnel who access the systems during a CIP Exceptional Circumstance require training after the fact, the team notes that the requirement requires training before access is granted, and the CIP Exceptional Circumstance exception clarifies that such training is indeed not required before granting access in those instances (e.g., in emergency situation that is a CIP Exceptional Circumstance, such training is not required of responding emergency personnel before they are granted access).

•In response to the suggestion to eliminate Requirement R3, the SDT made no changes. The requirement is necessary, as it requires completion of the training in R2 before access is granted.

•In response to the suggestion to modify the requirement to read, “Require completion and documentation of the training specified . . ..” the SDT agrees and has made the suggested addition to Part 3.2.

•Measure M3.1: In response to comment to delete the phrase, “the date access was first granted,” the team made no changes, as although the requirement does not include documenting the date access was first granted, the entity must demonstrate that it provided the training before access was granted – and this is hard to do without the dates involved.

The Measure uses "may" so that date is not required to be tracked.

•In response to comments that a potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for "transient" workers, the SDT reviewed the requirement and transient workers still need the applicable training before authorized electronic or unescorted physical access is granted. Additional training would not be needed if access was removed and then reinstituted for the same individual, with the same role, within the same calendar year as the training occurred.

•In response to comments that "Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems" be removed from the Applicability, the team believes protection of the Physical Access Control Systems and Electronic Access Control or Monitoring Systems Associated with High and Medium Impact BES Cyber Systems is a security enhancement that is appropriately included in these requirements.

•Requirement R3 Part 3.1: In response to comments that Part 3.1 may be onerous because training will be required for every new hire in the Applicability section, the SDT reviewed the requirement and believes the training must occur before authorized electronic or unescorted physical access is granted, except during CIP Exceptional Circumstances. In response to the comments that Applicability includes other associated Systems, but R4 does not have these in the Applicability, the SDT agrees there needs to be consistency between the Applicability section in R3 and R4, and has made those changes.

•In response to the comment that Table R3 doesn't contain any "applicable items," the SDT responds that the reference to applicable items in the Table is standard language to indicate that the Responsible Entity should implement the applicable requirements listed in the Table.

QUESTION 16 – CIP-004 R4:

CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made clarifying changes to Requirement R4, Part 4.1 and Part 4.4 but made significant changes to Part 4.2 and Part 4.3 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for

improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

•After review of the comments, the SDT updated the requirements with a goal toward improved clarity, while trying to maintain a balance of reasonable security awareness and to moderate audit impact. The changes to Requirement R4 include the following:

•In response to comments to add the phrase, “to BES Cyber Systems,” to clarify what this requirement applies to, the SDT added the language “to BES Cyber Systems, as suggested.

•Requirement R4 Part 4.2: In response to requested clarification to understand the phrase “six months or more,” the team has modified the language in Requirement R4 Part 4.2 to clarify that “six months or more” applies to resided, employed, and attended school.

•In response to concern for consistency in CIP-004-05, Table R4, the team has edited the language in Requirement R4 to clarify the purpose of the risk assessment programs are to attain and retain authorized electronic or authorized unescorted physical access.

•Requirement R4 Parts 4.1 and 4.2: In response to comment**s** asking whether either of these requirements is retroactive, the SDT states that the revised requirements for the criminal history check could necessitate a new assessment if the entity’s previous program does not meet the new requirements.

•In response to several comments that it will be difficult to be 100% sure of a “full seven year criminal check,” the team recognizes there may be challenges conducting a full seven-year criminal history check, and has included language in Part

4.2 to cover that possibility.

•In response to comments regarding online schools and how an entity determines location, after review of the comments, the SDT believes the expectation is that the student's physical location is considered when taking on-line classes.

•In response to several comments of being difficult to have "fails" defined for each role within the organization, the team agrees that all the criteria for determining what causes an individual to "fail" the PRA are difficult to document, and has modified the order of words in Part 4.3 to ensure Entities are clear that a assessment "process" is acceptable.

•In response to comments of difficulty in setting a hard line of when an employee "fails" a PRA is difficult, as it may be determined based on what role the individual is performing, after review of the comments, the SDT agrees that all the criteria for determining what causes an individual to "fail" the PRA are difficult to document, and has changed the order of the words in Requirement 4.3 to ensure entities are clear that a assessment "process" is acceptable. Information requested during an audit or investigation is covered under the NERC Rules of Procedure.

•Requirement R4.1: In response to comments regarding the word "initial" could indicate that this requirement must be done for existing individuals who already have access prior to V5 becoming enforceable, the team believes the word "initial" is needed to clarify that identity verification is only performed once, with the first PRA.

•Requirement R4 Part 4.2: In response to requests for clarification of the language, "resided and been employed," the SDT modified the language in Part 4.2 to clarify that "six months or more" applies to resided, employed, and attended school. The location of employment is where the individual actually worked, not necessarily the location of the corporate headquarters. The team recognizes there may be gaps if there are locations where an individual resided, been employed, or attended school for less than six months, but it does not preclude an entity from including those locations in its program.

•Requirement R4 Part 4.4: In response to requests for clarification as to why contractors must be separated out, rather than just having R4 be applicable to all individuals needing the access, the SDT reviewed Part 4.4, and the language is intended to verify that if an Entity is relying on the vendor's program, then the vendor's program must meet the specified criteria.

•Requirement R4 Part 4.4.: In response to comments to add "Parts 4.1 through 4.3" at the end of Part 4.4, that the measure should be consistent with the Requirement R5, Part 5.1 measure, which allows the use of attestations from vendors and contractors, the SDT has modified the requirement to include the reference to Requirement 4 Parts 4.1 through 4.3. The Responsible Entity may allow vendor attestations in accordance with its policies, practices, and

procedures.

•In response to comments that the Applicability stated in CIP-004-5, Table R4 - Personnel Risk Assessment Program, and CIP-004-5, Table R5 - Personnel Risk Assessment are inconsistent, the SDT agrees there needs to be consistency between the Applicability sections in R4 and R5, and has made the necessary changes.

•In response to comments to change "identify" to "identity," the SDT has changed Part 4.1 Rationale section to correct the typographical error.

•In response to comments that two defined terms be added to the glossary: Escorted Electronic Access and Unescorted Electronic Access, the SDT notes that the standards do not allow "escorted electronic access," and modifying the requirements to include the suggested language or adding the glossary terms. The SDT further clarified language relating to both electronic and physical access by stating "authorized electronic" and "authorized unescorted physical" to denote that all electronic access, whether "escorted" or not, must be authorized, and such authorization must meet the requirements of the standards.

•In response to comments that PRAs completed prior to V5 should be acceptable until the next time a PRA is required in the seven-year cycle, the SDT agrees and the Implementation Plan has been revised to allow the existing PRA to be "grandfathered" until it is time for its renewal. If the criminal history/background check for other compliance programs meets the new requirements in CIP-004-5, these would be acceptable.

•Requirement R4 Part 4.2: In response to comments that Requirement R4.2 lessens the requirements for international individuals, the SDT believes that it has not lessened the requirements for international individuals, but recognizes the need for vendor attestations, if an entity chooses to accept them.

•Requirement R4: In response to comments that the Measures require that the personnel risk assessment include a seven-year criminal history check, the requirement does not, the SDT has rewritten the requirement to clarify that a personnel risk assessment is needed to attain and retain authorized electronic or authorized unescorted physical access.

•In response to comments of FBI background checks qualifying as acceptable, the SDT believes FBI background checks would be acceptable if they meet the requirements of CIP-004-5.

•In response to comment to eliminate the requirement, the SDT thanks you for your comment, but believes the requirement is necessary.

•In response to comments to require why a seven-year background could not be performed will add additional costs, contributing little or no value to the personnel risk assessment program, the SDT believes documenting why a complete

seven-year criminal history check could not be performed demonstrates due diligence in meeting the requirement.

•In response to comments that there are no other FERC directives for the personnel risk assessment program requirement, the SDT believes the changes in CIP-004-5 increase the security posture of the entity over previous versions of the standard.

•In response to comments that the combination of requirements has the effect of discouraging entities from subjecting contractors to internal programs for entity employees because the burden of collecting, validating, and protecting information for non-employees is so overwhelming, the SDT believes Requirement 4.4 provides the flexibility to use the same process for contractors as employees.

•In response to comments that residency and educational history is not relevant to a criminal history, the SDT reviewed the requirement, Part 4.2 does not require an assessment of residency or educational history. It is intended to identify locations where the criminal history check should be performed.

•In response to a recommendation to modify this requirement to include the use of a National Criminal Research Database, which is believed to cover all of these requirements and show reasonable due diligence, the SDT disagrees with the assertion that the National Criminal Research Database covers all the requirements in CIP-004-5.

•In response to comments that the requirement only states criminal record checks and not other checks, such as random drug and alcohol testing, the SDT believes the addition of random drug and alcohol testing would be an expansion of the scope and is not under consideration at this time.

•In response to comments to leverage the Transportation Worker Identification Credential (TWIC) program, or to create a similar program specific to the electric sector, the SDT appreciates your comment, but it is not within our purview.

•In response to comments to align with the National Institute of Standards and Technology Interagency Report 7628 (NISTIR 7628) High-level requirements, the requirement should be elaborated, the SDT has reviewed the Personnel Screening requirements in NISTIR 7628, SG.PS-3, but believes Requirement 4 is appropriate.

•In response to comments of Table R4, Part 4.2 on Page 17, delete the phrase "regardless of duration," commenting that it does not add to the meaning since there is a six-month exception for certain addresses, the SDT believes the term “regardless of duration” means that the location of current residence must be included in the criminal history check, even if the individual has lived there less than six months. The concern with using the term “county of residence” is that it may not be applicable throughout the US and Canada.

•In response to comments that dormant accounts with privileges could be misused, the SDT believes revocation of access requirements in Requirement R7 provide for removal of such privileges.

QUESTION 17 – CIP-004 R5:

CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made clarifying changes to Requirement R5 and Part 5.1 and significant changes to Part 5.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

• Requirement R5 – Added "to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems" for added clarity per comments received.

• Part 5.1 –Updated language per comment received to "Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted…".

• Part 5.2 – The language has been modified to clarify that the current personnel risk assessment should be no older than seven years.

• Low Impact BES Cyber Assets have been moved into CIP-003-5 to emphasize the programmatic nature of the controls.

• Applicability has been revised to High Impact and Medium Impact BES Cyber Assets as in Requirement R4.

• Personnel risk assessments are addressed in two requirements with the requirement to have a "program" in Requirement R4 and "implementation" of that program in Requirement R5.

• The SDT believes that Requirement R5 is necessary because it required completion of the personnel risk assessment in Requirement R4 before access is granted.

• In regards to providing evidence of the personnel risk assessments during an audit, the SDT reminds commenters that information requested during an audit or investigation is covered under the NERC Rules of Procedures.

• The SDT disagrees with the assertion that the National Criminal Research Database covers all the requirements in CIP-004-5.

• The Implementation Plan has been revised to allow existing personnel risk assessments to be grandfathered until renewal time.

• The SDT recognizes the need to rely on information provided by the individual in identifying residence locations. The SDT has created requirements for a records check, not requirements that an individuals' fraud on one of those checks would necessitate a self-report, and the SDT respectfully disagrees that an individual's fraud would constitute noncompliance with the requirement so long as the responsible entity conducted the records check as required.

QUESTION 18 – CIP-004 R6:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to Requirement R6 but made significant changes to each of its Parts (Parts 6.1 through 6.6) and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The majority of comments on for CIP-004-5 R6 centered on the authorization language in requirement parts 6.1 through 6.3. In particular, commenters expressed disapproval of the CIP Senior Manager or delegate(s) authorizing access and the difficulty in auditing “the minimum necessary for performing assigned work functions.”

Regarding the inclusion of “CIP Senior Manager or delegate(s)”, we are reverting to previous language found in CIP-003-4 where the Responsible Entity maintains a list of authorizers. To avoid cross-referencing among Standards, which allows for independent revisions to Standards on a going-forward basis, the SDT combined parts from CIP-003-4, CIP-004-4 and CIP-007-4 in this requirement. CIP-004-4 R4 requires entities to maintain a list of personnel with authorized access. CIP-007-4 R5 Part 5.1.1 requires entities to ensure user accounts are implemented by approved designated personnel with a reference to CIP-003-4 R5. It’s in CIP-003-4 R5, nested through 2 references, where entities are required to designate authorizers by name and annually review the list of authorizers in CIP-003-4 R5 (nested through 2 references).

To address comments on the audit ability of “the minimum necessary” language in what was included in Parts 6.1, 6.2, 6.3, 6.5, and 6.6, (now 6.2, 6.3, 6.4, 6.6 and 6.7 in the revised draft of the standard) the SDT substituted the following language: “those that the Responsible Entity determines are necessary for performing assigned work functions.” This replaces what previous approved versions of CIP Cyber Security Standards had as “need to know” and makes clear that is the Responsible Entity who makes the determination of what is considered necessary. The compliance evidence necessary to demonstrate this would be showing that consideration was given to the required work functions as part of the provisioning process. When role-based access is configured, the necessary evidence would be documenting the type of access each role has and determining the level of access an individual needs to perform their assigned work functions. Demonstrating compliance can be much easier for simple access control systems such as generation control systems and relay where only one level of access exists. If access is only used occasionally or in emergencies, then it would still be considered necessary for the assigned work function.

Several commenters also expressed the view that the quarterly review (Part 6.5 in the revised standard) should be

extended to be performed annually. In response, the quarterly verification process comes from the previously approved CIP-004-3. The purpose of having a quarterly review is not for assuming the process is broken, but rather, for preventing unauthorized access as quickly as possible. In order to implement an effective access management program, this control is necessary to ensure the unauthorized access is revoked in a timely manner. There were also a few commenters who expressed the opinion that the review language significantly increases the scope of work for a quarterly review. In response, the changes made to this draft are in response to past industry comments and general feedback that the following phrase, "review the list of its personnel who have such access…" is not well understood or consistently implemented.

In addition, several comments expressed concern over the use of the words "calendar quarter." To clarify, performing the obligations in 6.4 (Part 6.5 in the revised standard) at the beginning of one calendar quarter and the end of the subsequent calendar quarter is an acceptable method for satisfying this requirement. The use of "calendar quarter" in this case will be easier for entities to maintain compliance deadlines.

Other modifications include specifying the authorization of access for BES Cyber System Information was limited to repositories instead of the BES Cyber System Information itself, which can be very extensive. The measures have also been modified to remove references to evidence sampling.

QUESTION 19 – CIP-004 R7:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to Requirement R7 but made significant changes to Parts 7.1 though 7.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

There were a number of comments submitted on CIP-004-5, Requirement R7 that express concerns of the majority of respondents. These are:

1. Removal of access "at the time of resignation or termination."
2. Various comments on the use of "next calendar day" for an access removal timeframe.
3. The requirements around reassignments or transfers.
4. Removal of access to BES Cyber System information.
5. The use of the term "extenuating circumstances" as it applies to compliance with Part 7.5 (changing passwords).

6. The inclusion of medium impact assets for removing shared accounts and changing passwords following a termination action.
7. Retroactive terminations or resignations
8. Application Guideline – No action required to revoke access in the case of a death of an employee.

We believe that the responses to these comments strike a well-orchestrated balance between industry concerns and addressing FERC Order No. 706 directives. The Standards Drafting Team provides the following summary responses:

1. Removal of access "at the time of resignation or termination"

First, the term "termination actions" was added to respond to numerous industry comments. The drafting team decided to consolidate both terminations and resignations since both of those actions are required to be addressed by FERC Order No. 706 to be completed "immediately." Immediately is definitively clear but realistically and from an audit perspective, subject to interpretation. Accordingly, the drafting team adjusted the requirement (see Part 7.1 in the revised standard) to read "initiate the process to revoke" unescorted physical and electronic access to BES Cyber Systems "upon the effective date and time of the termination and complete the revocation within 24 hours after the effective date of the termination action." Because various entities have diverse processes in place for initiating termination actions, the revised requirement considers those differences and establishes a 24-hour metric for audits based on the established date and time of the process start time.

2. "Next calendar day" for access removal time frame

The use of "next calendar day" is consistent throughout the Version 5 standards. While the drafting team is sensitive to the difficulties inherent to revoking access outside of normal working hours, the time lags, particularly in the case of terminations, could expose the entity to malicious activity. The time frame remains in effect for all termination actions.

3. Reassignments and Transfers

To address reassignments and transfers, the drafting team revised the requirement to specify that one must "revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. The requirement allows retention of access that the entity considers necessary as long as a review of all accesses is completed by the next calendar day following the transfer or reassignment and that any unnecessary accesses are removed at that time.

4. Removal of access to BES Cyber System Information. (Part 7.3 in the revised standard)

There were many comments highlighting the difficulties associated with ensuring that all access to BES Cyber System Information was removed. Some entities suggested the use of the term "repositories" to identify those areas where such information is stored. The drafting team chose not to integrate the term "repositories" because in an audit situation, use of a repository could become an incidental piece of evidence. Because BES Cyber System Information may be housed in numerous locations throughout an organization, the drafting team chose to revise the requirement to revoke an individual's "access to the physical and electronic locations" to locations where the Responsible Entity stores BES Cyber System information. This alleviates the issue of trying to track each individual hard copy of such information. It also prompts entities to try to consolidate BES Cyber System Information and limit its storage to as few locations as possible.

5. Use of the term "extenuating circumstances" as it applies to changing passwords in the event of a termination action. (Part 7.5)

"Extenuating circumstances" has been removed from the requirement. The requirement now states that a responsible entity may determine and document that "operating circumstances" require a longer time period to effect necessary password changes. Once the operating circumstances end, passwords must be changed within ten days.

6. The inclusion of medium impact assets for removing shared accounts and changing passwords following a termination action.

In both Parts 7.4 and 7.5, medium impact assets were inadvertently included in the applicability section. The medium impact assets have been removed from the revocation of individual user account and shared password requirements.

7. "Retroactive" terminations or resignations.

A number of respondents cited retroactive terminations or resignations as complicating the access removal process and time frame requirements. The drafting team attempted to clarify that though there may be retroactive resignations, retroactive terminations are an unfamiliar concept. The drafting team believes that an individual cannot effectively be terminated on a prior date and continue working. If a business unit "intends" to terminate an individual at some future date, the termination is not effective until the actual action is taken. By the same reasoning, an individual can decide to resign effective on some future date. The resignation is not effective until the actual projected date. In the case of

retroactive resignations, an individual may "resign" by leaving a voicemail on a manager's phone over the weekend. Realistically, the resignation cannot be processed until the manager is aware of the employee's action. Once there is awareness, the process initiation and 24-hour requirement begins.

8. Revocation of access in the event of an employee's death

There have been a number of comments discussing the Application Guideline not listing revocation requirements in the event of an employee's death. The drafting team agrees that there is a security risk if no action is taken. We have adjusted the Application Guideline to reflect expeditious removal of access.

QUESTION 20 – CIP-004 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to all the VSLs except for the VSLs for R4 which had only a minor change.

Please see the redlined version of the standard for the complete set of revisions.

One commenter suggested the VRF for revoking access should be medium. In response, we note that the currently approved VRF for access revocation is lower and we have no compelling justification for modification at this time.

For R1, several commenters suggested a more granular break out for missing a single quarter. One entity suggested that failure to document the program be a lower VSL than failing to implement the program. Several commenters noted the Severe VSL failure to document or implement the program negated the High VSL failure to perform on a quarterly basis. In response and regarding the granular break-out, a single violation of this requirement would be on a per quarter basis. So, instead, we provided more levels of severity according to the time of an entity performance beyond missing a calendar quarter. Regarding the documentation and implementation of the program in the Severe VSL, we modified this to include documentation only.

For R2, several commenters suggested a more granular break out than what was proposed. In response, we provided additional granularity based on the amount of training content an entity failed to document.

For R3, several commenters suggested a more granular break out on percentages of missed training. One entity commented that this requirement should be written as a find, fix, repeat process, and the VSL should be based on the

amount of time to fix the error. Another entity indicated the Severe VSL negated the High VSL. In response, we have provided additional granularity based on the number of individuals missing training in a calendar year. Regarding the find, fix, repeat process, if the VSLs were gradated on the amount of time to fix the error, that would indicate that the requirement allows individuals to access without training as long as the entity caught the error in a specified amount of time. Such a requirement would not achieve the reliability objective to provide ongoing training. In essence, an entity would never violate the requirement so long as the violation was caught within an acceptable period of time. Regarding the Severe VSL, we have modified this to make clear that it applies when the Responsible Entity does not implement the training program at all.

For R4, one entity noted the High VSL refers to "required documented results" and to Part 4.5. The documented results are a requirement of R5 and there is no Part 4.5. Another entitysuggested a lower VSL for lack of documentation. In response, we have removed references to "required documented results." Regarding a lower VSL for lack of documentation, the FERC makes clear in its March 18, 2010, Order on CIP VSLs that a VSL cannot be lower for failure to document because documentation indicates and provides evidence of a consistent practice.

For R5, one entity suggested breaking out the VSL so that one individual not having a complete update every seven years is a moderate, and two or more becomes a high VSL. Other commenters suggested simplifying the language in the High VSL to "Personnel risk assessments are not updated at least once every seven years." They also suggested the failure to document should not be a Severe VSL. In response, we have gradated much of the VSL based on the number of individuals not having a PRA and have simplified the language similar to what was suggested.

For R6, one entity noted the Severe VSL refers to a nonexistent Part 6.7. Another entity commented that administrative errors found during quarterly and annual assessments should not be considered a violation. Another entity suggested breaking out the quarterly and annual assessment VSLs based on percentages. Another entity commented that for VSLs gradating on counts, there should be a timeframe identified. Another entity suggested making separate VSLs for requirement parts instead of having long or clauses. In response, we note that administrative errors not leading to unauthorized access are not violations of the Standard. We have also gradated the VSLs, both on the number of individuals not having authorization and on the time beyond performing required assessments. We have also identified timeframes for the aforementioned counts.

For R7, several commenters suggested VSLs be broken out by percentages. Some commenters suggested breaking out the violations by specific numbers of individuals who did not have their access revoked. In response, we have provided further gradation on the number of individuals. We chose not to use percentages because it becomes less meaningful with a smaller sample size and the risk for a large company for one failed access revocation is the same as for a smaller

company.

QUESTION 21 – CIP-005 R1:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to R! but did make significant changes to Parts 1.1 through 1.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

There were numerous comments concerning the Requirement R1 Part 1.1 requirement on Low Impact systems. The SDT has moved all requirements concerning Low Impact systems from the entire suite of CIP standards to CIP-003 and rewrote the Requirement R1 Part 1.1 at a higher level. The SDT has also re-invoked the ESP definition from previous versions in order to use it to handle the 'high watermark' comments and clarify what entities are to do when systems of mixed impact classifications are within one ESP. The applicability of R1 has been clarified and changed in order to match previous versions and not create recursion in the requirement (ESPs around ESP devices). The SDT has clarified in the responses that the malicious communications requirement has been intentionally written at a level that does not require

specific technologies (such as IDS, although IDS is used as an example in the measures). The SDT also clarifies that the requirements that were noted as deleted (R1.1-R1.3) were from previous versions as they were definitional in nature. New requirements with those numbers have been added. The SDT also clarified that outbound permissions on Electronic Access Points (EAPs) are now required as a first level of defense against compromised systems in the ESP. Guidance has been added to the standard with further explanation.

The term "non-interactive" in the applicability column of Requirement R1.4 was removed. Commenters found this term confusing. "Non-interactive" was originally included to distinguish it from the Interactive Remote Access covered in Requirement R2. The term "explicit" in Requirement R1.3 was removed because of commenter suggestions that the term is superfluous. In Requirement R1.5, many commenters expressed confusion around detecting malicious communication "at each EAP". The SDT recognizes the confusion and potential for multiple interpretations, and in response, it has made the requirement less specific to focus on the objective of detecting malicious communications. One commenter suggested that R1.5 was overly prescriptive and should be written to allow entities to choose how to address Order No. 706, paragraphs 486-503. In response, the SDT believes that would cause numerous comments from industry as to its audit ability. To address the full intent of the Order's language, nearly 6 paragraphs would need to be included to clarify what is and is not acceptable. The SDT has chosen instead to narrow the requirement to something that does meet FERC's intention, while wording it in such a way that it remains quite flexible and not tied to a particular technology such as IDS. IDS is only mentioned in the Measures as an example of evidence.

QUESTION 22 – CIP-005 R2:

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 – Remote Access Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made a clarifying change to Requirement R2 and made significant changes to Parts 2.1 through 2.3 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The majority of comments for CIP-005-5, Requirement R2 were aligned to a few areas. The three most commented on issues for CIP-005-5 R2 were: (1) the starting and the ending point for encryption, (2) clarification of multi-factor authentication, and (3) the prescriptive nature of the requirements for Intermediate Device.

The majority of comments regarding CIP-005-5, Requirement R2 requested clarification on the initiating and the terminating point for required encryption. In response to comments, Part 2.2 has been modified to state that encryption must terminate at the Intermediate Device. Encryption initiates at the Cyber Asset performing Interactive Remote Access.

The second most noted comment was requesting clarification on where multi-factor authentication is required. To address the comments submitted, the definition of Intermediate Device has been updated to require that access control is performed by the Intermediate Device. This would include multi-factor authentication.

Many commenters also raised concerns with the note regarding UserID not being an authentication factor included in Measure 2.3. The note in the Measure regarding User ID has been removed in response to those concerns. Clarification of multi-factor authentication has been added to Requirement Part 2.3, and further information regarding multi-factor authentication is included in Guidance for Secure Interactive Remote Access published by NERC in July 2011.

Regarding the third area of comments, the SDT considers Requirement R2 Part 2.1 to be broad in implementation, and the requirement allows for appropriate flexibility in the design of remote access architecture. Intermediate Device is not defined to be technology specific. The requirement has been drafted to allow a Responsible Entity to define the infrastructure that meets the needs and capabilities of its organization, while also specifying a set of parameters. Varying examples of remote access system design are included in Guidance for Secure Interactive Remote Access published by NERC in July 2011.

Additionally, many commenters noted concerns regarding the need for Technical Feasibility Exceptions. To address these

comments, the SDT notes that all parts of Requirement R2 are eligible for a Technical Feasibility Exception.

Commenters requested segregation of dialup from network based remote access. Dial-up is addressed in other requirements. However, the securing of remote access using dial-up is only addressed in this requirement. As such, the content is relevant to this requirement and the SDT did not segregate this requirement.

QUESTION 23 – CIP-005 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for R1 and R2 but did not change the VRFs.

Please see the redlined version of the standard for the complete set of revisions.

Commenters recommended segregating the VSLs by the percentage of number of failures to protect the Interactive Remote Access sessions. Due to the protective measures generally being enterprise-level solutions, this sort of gradation of the violation severity is not appropriate and would be onerous in retaining evidence of compliance.

Comments were submitted requesting VSLs identified by the criticality of the asset. The applicability of the requirement addresses the impact of the asset. The requirements are written to address the protection of the assets already identified. The VSLs have been modified to address the implementation of the appropriate protective measures.

Comments were made to propose estimation of the monetary penalties associated with a potential violation of the requirements. This information is available in Appendix 4B of the NERC Rules of Procedure.

Overall, the primary issue for the comments related to the CIP-005-5 R2 Violation Severity Levels (VSLs) were that all violations would be deemed as severe rather than the VSLs being graduated based on risk. In response to the comments, the VSLs have been modified to address not implementing the required procedural or technical controls.

QUESTION 24 – CIP-006 R1:

CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans that include each 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R1 and all of its Parts 1.1 through 1.6 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The entire contents of CIP-006-5 are intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

In addition to several comments that assisted the drafting team in making positive revisions to correct for consistency, eliminate ambiguity, or provide clarity, the SDT considered several constructive comments and made substantive changes to CIP-006-5.

Other modifications were added to address FERC Order No. 706, Paragraphs 572 and 575, which were directives for physical security (defense in depth), and to address industry comments. These modifications include, but are not

limited to, the following general concepts:

- The language of R1 has been modified to clarify the scope as applicable to BES Cyber Assets, BES Cyber Systems, Electronic Control Monitoring systems and Physical Access Controls Systems.
- The phrase “real- time alerts” has been removed, and the requirement expanded to clarify the intent.
- The measures have been modified to agree with the requirements to track access (i.e., ingress only).
- The phrase “access point” has been removed, and the language has been clarified to reflect the SDT’s intent.
- Information on access openings has been provided in the Guidelines and Technical Basis section of the standard.
- The requirement around physically protecting Physical Access Control Systems is limited to restricting access using operational or procedural controls, and the language has been clarified to reflect this intent.
- “Where technically feasible” language has been added in cases where it may not be possible to implement two or more different physical access controls due to physical restrictions, with an expectation that this language will not be abused to deviate from the intent of this standard. The language has been modified to clarify the intent that two different physical access control mechanisms are required, not two completely independent physical access control systems
- The requirements in this standard have been reworded such that an entity must utilize one (or more) physical access control(s) to allow physical access into a PSP to only those individuals that are authorized. There is no explicit requirement for a completely enclosed ("six-wall") border.
- The SDT attempted to stay away from detailed “how” questions posed in an attempt to all different implementation methods that obtained the same minimal risk level.
- Recommendations on the management of CANs were viewed as outside the scope of the SDT.

More specifically, commenters raised several issues, which are discussed in greater detail in the paragraphs that follow.

As described in the summary response to “Defined Physical Boundary,” the SDT has changed this term back to “Physical Security Perimeter” in response to comments. Note, however, that the definition of the term, “Physical Security Perimeter” has changed significantly from the currently-used definition.

Commenters requested greater clarity with respect to the phrase “Issue real-time alerts” in Requirement R1, parts R1.4 and R1.5, and the drafting team agrees and has modified the requirement to remove “Issue real-time alerts.” Instead, the requirement language requires issuing “an alarm or alert in response to detected unauthorized . . . to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes . . .” (These parts are R1.5 and R1.7 in draft

2). That also ties in better with the requirements on incident response, which addresses commenters concern that there are requirements to alert, but not to respond. The requirement to detect unauthorized circumvention and alerting has also been separated into two requirements, with additional clarification provided in the new wording.

Commenters noted concern with R1.4's (now R1.5) used of "access point" and the phrase has been removed to clarify the SDT's intent. The requirement now references "unauthorized circumvention of a physical access control into a Physical Security Perimeter".

Commenters also suggested that "sufficient" in R1.6 was subjective. The use of "sufficient information to uniquely individual" is intended to provide flexibility to the entities. It is expected that the responsible entity's plan will define what set of information is adequate by demonstrating the ability to uniquely identify individuals from the logged records.

Commenters also suggested that Parts R1.2 and R1.3's measures implied a requirement to track egress. The measures have been modified so that they better align with the requirement to track access (i.e., ingress only).

In response to concerns that Part R1.3's TFE language may lead to increased TFEs, the SDT notes that in some cases it may not be possible to implement two or more different physical access controls due to physical restrictions and equipment locations. Because of this, the language "Where technically feasible" has been included. As is the case with any technical feasibility language within the standard, meeting the requirement language is the goal.

In response to concern that CIP-006 raises a conflict with the BES Exception criteria, for certain generation facilities, particularly those under 75 MVA, the SDT addressed the concern in Section 4 (Applicability) of the standard itself. Section 4 clearly stipulates under Facilities 4.2.3: "Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities." (Underline added). Only those Facilities that are deemed to be BES Facilities are in scope for the standard. If these Generation facilities are excepted from the BES definition, then they are also excepted from the applicability of these CIP Cyber Security standards.

Commenters recommended including the wording from CAN-0031, "That any opening that does not have physical preventative measures in place is less than 96 square inches. That any opening greater than 96 square inches, with its shortest side greater than 6 inches in length, is protected against entry by the use of bars, wire mesh or other permanently installed barrier that leaves no opening greater than 6 inches on its shortest side." In response, the SDT notes that Information on openings has been provided in the guidance. Importantly, the requirement is to restrict entry into a Physical Security Perimeter. The revised standard does not identify any specific size requirements and does not reference the term "access point". The SDT expects that if such an opening exists and cannot be eliminated, then it will have to be considered an "access point in a Defined Physical Boundary" with the appropriate controls applied. In Version 5's CIP-006 proposal, there is no requirement to ensure a completely enclosed ("six-wall") border. The requirements

have been reworded such that an entity must utilize one (or more) physical access control(s) to allow physical access into a PSP to only those individuals that are authorized.

This provides entities the option to implement alternatives to restrict access that may be more practicable or economical than a completely enclosed border without requiring the submission of a TFE. As noted, the guidance document states that in many instances a completely enclosed border this will remain a primary control for controlling access. In terms of controlling access, the CAN's information on the size of an opening that constitutes an access point would still apply insofar as a larger opening would need controls in place to allow access to only those individuals authorized, and a smaller opening (that an individual cannot pass though) would not require those additional controls.

Some commenters suggested that the CAN should be required, but the issue of retiring CANs is outside the scope of the drafting team. However, with the greater specificity of the requirements surrounding this issue in Version 5, the SDT understands that contrary language and instruction through requirement language may result in the withdrawal of the CAN.

In response to concerns surrounding the testing requirements of every two years (and a preference for every three years), the SDT notes that the modification to every 2 years is in direct response to FERC Order No. 706, paragraph 581's directive to test more frequently than every three years. Furthermore, if the active monitoring can be demonstrated to meet the requirements of the semi-annual testing (including validation of correct operation for all locally mounted hardware or devices at the Defined Physical Boundary) then this would most likely meet the two year testing requirement.

In response to commenters' suggestion that associated Physical Access Control Systems be added to applicability of R1.2 and R1.3, there is no explicit requirement to have Physical Access Control Systems protected by a Physical Access Control System (PACS). This is consistent with CIP-006 versions 1-4. The requirement around physically protecting PACSs is limited to restricting access using operational or procedural controls, and the language has been clarified to convey this intent.

Commenters questioned what was meant by two or more "different and complementary" controls under Requirement R1.3. This comes from a directive in FERC Order No. 706, Paragraph 572, but the SDT has made significant clarification to the language (and removing "complementary," while supporting the concept). The SDT addressed this in CIP-006-5, Requirement R1 (Part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to "utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access." This clarifies the intent that two different physical access controls are required, not two completely independent physical access control systems.

In response to questions surrounding the meaning of “associated with” in the applicability tables, it means “associated with” the High, Medium, or Low classification BES Cyber Systems (with or without additional conditionals) identified in that applicability section. The SDT has made significant revisions to the background and “applicability columns in tables” section of the standards to better explain this concept.

In response to suggestions to clarify the entry and exit logging requirements in R2.2, the SDT added clarifying language allowing for logging “first entry” and “last exit” from the Physical Security Perimeter.

In response to comments that suggested very specific artifacts for compliance, the SDT’s intent is to identify “what” is necessary for protection without adding the specificity on “how” to achieve that performance.

Commenters suggested that for R1 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances because there may be circumstances that require providing physical access control to individuals not on the authorized list, but this is not appropriate in CIP-006; the SDT notes that the CIP Exceptional Circumstances are addressed under CIP-004 – Authorization.

For logging access under R1.6 (now R1.8), some commenters questioned whether it included just the date, or also the time. The SDT has clarified the language by specifying that it includes both the date “and time.”

Commenters asked whether cabling must be protected between Defined Physical Boundaries (now Physical Security Perimeters), and the SDT notes that the requirements apply to Cyber Systems and Cyber Assets. With the changes to glossary term, “Cyber Asset,” along with the determination in Project 2008-10’s interpretation of CIP-006 (approved by NERC BOT, but not yet approved by FERC) that “wire” is not a Cyber Asset, the requirements in CIP-006 do not apply to wiring or cabling.

Some commenters questioned what was meant by “locally mounted hardware devices.” The SDT has clarified the language in the background and applicability explanations, which clarifies that “locally mounted hardware devices” is intended to refer to “dumb” devices that do not perform any authentication functions independently.

In response to suggestions to allow for CIP Exceptional Circumstances to except one from logging, the SDT did not see a reliability related reason to suspend logging just because of a CIP Exceptional Circumstance.

QUESTION 25 – CIP-006 R2:

CIP-006-5 R2 states "Each Responsible Entity shall implement its documented visitor control program that includes 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made minor changes to Requirement R2 and significant changes to Parts 2.1 and 2.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 2.1 and Part 2.2 - Applicability – revised Medium Impact to include only routable or dial-up access in order to limit the need for visitor controls.

(2) Part 2.2 – Changed "…of the entry and exit…" to "…of the initial entry and last exit…" for clarification.

(3) Part 2.2 – Changed "… individual point of contact." to "…name of an individual point of contact responsible for the visitor." in order to clarify "point of contact" and that it may be a different person than the escort.

Several commenters requested clarification as to whether physical access logs are required for physical access to Physical Access Control Systems. The SDT confirms that physical access logs for authorized users and visitors are **not required** for

physical access to Physical Access Control Systems.

Several commenters recommended the removal of "continuous" from "Require continuous escorted access…..". The SDT believes "continuous" should remain and notes that "continuous" is in version 3 and 4 requirement wording.

Additional requirements were proposed that the SDT believes go beyond what should be required as minimum level of visitor controls needed.

Measure for Part 2.2 – Comments were received to remove "and" from this measure. The SDT does not agree with removing "and" since the measure also states "not limited to" and for the examples provided both items would be needed to demonstrate compliance. The responsible entity must have the required language in its visitor control program AND must have evidence that it has implemented this program.

• •The SDT agreed with other comments and added the ability to deviate from Requirement R2, Part 2.1 and Part 2.1 during CIP Exceptional Circumstances, and added a new Part 2.3 to clarify that visitor logs only need to be retained for 90 calendar days. The SDT also updated change descriptions to reflect current requirement wording.

QUESTION 26 – CIP-006 R3:

CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made minor changes to Requirement R3 and significant changes to Parts 3.1 and 3.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"

- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 3.1 – Removed “prior to commissioning” per commenters suggestion.

(2) Part 3.1 – Changed ”…to ensure the required functionality is being provided.“ to “… to ensure they function properly.”

(3) Parts 3.1, 3.2,– Applicability – specified High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable in order to clarify which “locally mounted hardware or devices” are applicable.

(4) Part 3.2 – Expanded on Part 3.2 to require retention of outage records for 12 months.

(5) Applicability – Changed from “Associated Physica Access Control Systems” to “Physical Access Control Systems associated with” to standardize across the CIP standards.

Part 3.1 - Comments were split where maintenance and testing was concerned. Some commenters felt that maintenance and testing should be done more often while others wanted to revert to the current three years. Based on SDT discussions and the FERC directive in Order No. 706, paragraph 581, the SDT continues to believe that 24 months is appropriate.

Some commenters indicated that tracking of outages should only include Physical Access Control Systems. The SDT believes that tracking of outages should include more than just outages to the Physical Access Control Systems because other outages may be relevant for forensics purposes.

QUESTION 27 – CIP-006 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all three of the requirements in this standard but did not make any changes to the VRFs.

The drafting team appreciates the numerous comments pointing out the incorrect references to items in the requirements shown in the Table of Compliance Elements. These references have been corrected. These reference

corrections also addressed several comments on the High VSL for R1 stating the standard did not mention a 15 minute requirement. The correct reference is to Part 1.5, which does include this time requirement.

On the comments to reduce the VRF for R2 to Lower, the drafting team points out that the current VRF level for visitor control is Medium and believes this is the right level based on the definition of a Lower and a Medium VRF. A lower VRF is associated with a requirement that is administrative and, if violated, would never lead to cascading, uncontrolled separation, or instability. Requirement R2 includes "implementation" of the visitor control program, thus this requirement is not administrative and doesn't qualify for the "Lower" VRF.

Similarly, the use of the term "continuous" is in the current version of the standard and is intended to mean the escort should always be in close proximity to the visitor and aware of the visitor's actions.

The drafting team corrected the confusion over the term "each" in the Moderate VSL for R2 as pointed out by one commenter by specifying that it applies to the initial entry and final exit, not each entry and each exit.

As to the comments that there should be a Lower VSL for processes that are implemented but not documented, the drafting team does not agree. It is not clear how an entity consistently implements processes that are not documented. There was one comment that failure to adequately document information to uniquely identify an individual is more severe than failure to implement two or more controls to restrict access for High Impact BES Cyber Systems. If the individual is unknown and accessing an unknown area as described in the comments, this would be a potential Cyber Security Incident and handled as such. The Lower VSL is intended to capture an instance where an authorized individual appropriately accesses a Physical Security Perimeter, but for some reason, uniquely identifying information is not captured.

Finally, the drafting team believes the differentiation between High and Medium Impact BES Cyber Systems is done with the controls, if necessary, so it does not warrant separate entries in the Table of Compliance Elements.

QUESTION 28 – CIP-007 R1:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R1 but did make significant changes to Parts 1.1 and 1.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

In response to numerous comments the SDT has rewritten Requirement R1, Part 1.1 to:

(1) specify the requirement applies to applicable Cyber Assets

(2) to provide the ability to specify port ranges, as well as service names for those with truly dynamic port ranges, and

(3) enabling of only necessary ports – revised Part 1.1 now reads: "For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services where needed to handle dynamic ports."

The SDT notes that those ports and services that are allowed to cross an ESP are explicitly documented at that level in CIP-005. The SDT has left the term 'ports and services' in recognition that ports are actually just the listening 'channel' for a service, and we've added that services can be designated as needed to handle such things as remote procedure call (RPC) which use random, dynamic ports.

Numerous commenters noted the amount of work involved in creating screenshots. Based on these comments, the SDT removed "screenshots" as an example in measure 1.1.

Based on comments received concerning the clarity of the phrase, "Disable or restrict the use of . . ." in Requirement R1,

Part 1.2, the SDT has changed Part 1.2 to read "Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media." and has removed screen shots or pictures from the example measures. This requirement is in response to FERC's interpretation order that required the ERO to address the issue.

A commenter proposed a more graded approach to the level of security required in the standards. The SDT believes it does have a graded approach to the standards where higher impact systems have stricter requirements. The current requirements in V3-V4 of the CIP standards are carried forward as practical to the same types of cyber assets in V5 (medium impact), with a few more stringent requirements being applied to the high impact systems, especially where needed to meet the outstanding directives from Order 706.

A minority view held the guidelines provided additional requirements. The SDT notes that guidelines are not enforceable and are not requirements. Only the actual requirements are mandatory and enforceable. The SDT's intent in providing guidelines is to provide examples of how something could be met, and it is not intended to enhance the requirement language itself in any way.

QUESTION 29 – CIP-007 R2:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R2 but did make significant changes to the Parts 2.1 through 2.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"

- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Several commenters stated that the last sentence on sorting (“The list could be sorted by BES Cyber System or source.”) in Measure 2.1 was not needed. The SDT agrees and has deleted the last sentence of the measure.

Commenters raised issues with the language that suggested that ‘updates’ (old Part 2.2, now Part 2.3 in the updated standard) might be interpreted to include all updates, not just security-related updates. The SDT agrees and has incorporated the existing language from Version 4 to clarify that only security related updates are in scope.

Commenters raised issues with using the term ‘remediation plan’ (old Part 2.2, now Part 2.3 in the updated standard) and many suggested changing to ‘mitigation plan’. The SDT agrees; however, the term ‘mitigation plan’ has numerous meanings as it pertains to NERC standards, compliance, and enforcement and could cause further confusion. The SDT has changed the language to call for a ‘plan’. Further, many commenters questioned whether the plan is specific to the patch or the overall process. The SDT clarifies that a plan is needed per patch. The plan is simply the way the entity chooses to mitigate the vulnerability exposed by the security patch, either by installing the patch or taking other measures. The plan can consist of a simple notation that the patch will be applied in the Responsible Entity’s normal patch management process.

Numerous comments were made as to the clarity and order of the requirement Parts in the table, in particular Parts 2.2 and 2.3. There were also comments stating that the measures did not match the requirements. The SDT agrees and has reworked the requirements in the table to more closely model Version 4’s language, and the SDT made revisions to the requirements and measures in the standard for additional clarity.

There were a few commenters who called for patching requirements on low impact systems. The SDT believes that although low impact systems should be patched, the compliance burden of tracking every patch for every low impact asset is an onerous burden and thus has not required it in this mandatory, enforceable, and auditable standard.

Several comments concerned devices that can not be patched or for which no patch sources are available. The SDT has modified the requirement to better account for that possibility and to handle devices that are not updateable or have no patching source. Part 2.1 in the revised standard includes the following language: “…shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets

that are updateable and for which a patching source exists."

Many comments concerned the fact that no maximum timeframe for patching is required. The SDT is allowing flexibility in the patching implementation timeframe. The desired behavior from this requirement is that entities are tracking and are aware of vulnerabilities in their systems that patches expose and create a plan to mitigate those vulnerabilities. The SDT is not mandating the installation of all patches, but rather focusing on the entity's response to the vulnerability. The SDT has taken into consideration that control system patching itself is a risk to reliability and that there are entire seasons in our business where the risk of making changes to control systems that could affect availability outweighs the risk of compromise. The SDT believes that if entities are required to be aware of vulnerabilities in their systems, they can then make informed risk decisions that are in the best interest of overall reliability.

Some commenters requested clarification regarding who is responsible for identifying the sources of the patches and what level of patching requirements were required. The SDT clarifies that the Responsible Entity identifies the sources as part of its overall patch management process and it is up to the Responsible Entity to choose the source of the patch based on its maintenance contracts, etc. While the SDT has changed the requirement to incorporate V1-V4 language, it cannot prescriptively describe every piece of software/firmware that should/should not be patched. The SDT notes that the software/firmware should include those that affect the Responsible Entity's system's capability to perform its function in support of BES reliability.

One commenter stated that Project 2009-06 is an interpretation which was not adequately addressed in this standard and suggested that the SDT revise the requirement to either require Responsible Entities to have documented procedures for supervised electronic access or specifically state that no supervised electronic access is allowed. The SDT notes that the notion of "supervised" or "supervision" relates to physical access, not electronic access. All electronic access must be authorized, regardless of whether "supervised" or "escorted" and all authorization must occur pursuant to the requirement language.

Many commenters were concerned about the time allotted for completing the assessment and creating a plan. The SDT has revised the requirement and added a two step process with 30 days for completing the assessment and 30 days for creating/revising the plan.

Many commenters raised concerns regarding the intent of "CIP Exceptional Circumstances." The SDT has removed "CIP Exceptional Circumstances" from the requirement.

A few commenters stated that Part 2.2 went beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availability can be determined. The commenters also felt that requiring a plan and an assessment was beyond the rationale and that a "plan" should not be required as it

implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process. The SDT clarifies that the plan is the result of the assessment, if the assessment by the entity determines the patch to be applicable to their BES Cyber Assets. The SDT agrees and has reworked the requirements in the table to more closely model V4 language and added steps for additional clarity. The 'plan' is simply the entity's own plan for how to handle the vulnerability, which can include the installation of the patch using normal patch routines, or the implementation of new measures, or documentation of already existing measures. The requirement also now calls for a separate 'assessment', which is an assessment for applicability to the entity's systems and environment. The 'plan' for handling the vulnerability is then only needed for patches that are applicable. The timeframe can be a date certain or an event-based date.

A few commenters stated that firmware should not be included in the requirement as very few vendors post when firmware updates become available. A concern was also raised regarding the fact that firmware was mentioned in Part 2.1, but CIP-010 did not require the documentation of firmware levels. The SDT appreciates the comment, but has left firmware in scope, as entities do need to watch for any future firmware updates that address security issues, even if there are very few. The SDT has revised CIP-010 to require firmware level for cyber assets that don't have software versions.

Some commenters requested clarification on the definition of "defined timeframe." The SDT has removed "defined" and specifies instead that "the plan shall include the Responsible Entity's planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations."

A couple commenters suggested that the bulleted list in the measures for Part 2.3 (now Part 2.4 in the revised standard) should be separated by "or." The STD notes that the NERC standards convention is that bulleted lists mean "or" and numbered lists mean "and". Each bullet is separated by semi-colons and "or" has been added after the second to last bullet.

Some commenters raised concerns regarding applicability. The SDT has modified the applicability sections of all of the CIP Version 5 standards to be consistent.

One commenter was concerned that allowing entities to rely on a vendor to "certify" a patch before it is considered available would be an unnecessary delay and would increase the risk to the reliability of the BES. The SDT agrees with the points the commenter made, but in a mandatory and enforceable standard the SDT believes it is fraught with issues to require Responsible Entities to know and track the ultimate original source of all vulnerabilities in all software components of all BES Cyber Assets. As this standard expands in scope to include all types of field devices, the SDT believes it is problematic to measure and enforce such a requirement on all of an entity's purpose-built devices (i.e.,

substation IED's) that may have a vulnerability due to something found in some commercial real-time operating system kernel or embedded Linux kernel or Windows CE version in the device's firmware. The SDT believes it is reasonable and measurable for the entity to track the manufacturer of the device for firmware patches rather than the ultimate sources of vulnerabilities in embedded subcomponents. The SDT agrees that some poor vendor practices exist, but believes a CIP standard enforced on the Responsible Entities is not the place to deal with poor vendor practices. While the requirement is not a perfect control, we believe it is a large step in the right direction.

One commenter suggested that a more proactive mitigation, such as an upgrade plan, should be required for systems that do not require patches, but are still vulnerable to malicious exploitation. Further, the commenter was concerned that the requirement did not properly address increasing malicious attacks, mostly exploiting zero-day vulnerabilities. The SDT realizes that no single control is perfect at eliminating all risk and therefore the collection of standards accomplishes defense in depth with multiple levels of security concepts. The SDT does not believe that in a mandatory and enforceable standard that upgrades of functioning equipment should be required due solely to cyber security issues. The SDT also notes that patches do not address zero-day vulnerabilities, as they are 'zero day' because the vulnerability was previously unknown and thus no patches exist.

QUESTION 30 – CIP-007 R3:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any changes to Requirement R3 or Part 3.1 but did make significant changes to the Parts 3.2 through 3.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the standard for a complete set of revisions.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity

- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT received comments on the inclusion of the term “‘Maintenance Cyber Assets.”’ The SDT agreed with those comments as that occurrence of the term was missed as we changed “‘Maintenance Cyber Assets”’ to “‘Transient Cyber Assets’.” It has been removed from the standard (and so has the concept of “‘Transient Cyber Assets”’).

Numerous comments were received on the Transient Cyber Asset (“TCA”) requirements. The SDT agrees with many of the comments and has deleted those requirements. Part 3.4 required malware prevention tools on TCA’s. The point of the requirement is the protection of BES Cyber Systems from the introduction of malware, and that is included in Part 3.1. Part 3.5 covered logging of TCA connections, which provided no clear reliability benefit. Both have been struck. The SDT removed the term Transient Cyber Asset as a proposed glossary term, and the SDT added the concept of the previous definition to BES Cyber Asset as an exclusion. The SDT also considered the numerous auditing and evidence issues these two requirements posed and agreed to delete them.

The SDT received comments on the absence of ‘where technically feasible’ to allow for Technical Feasibility Exception (“TFE”)E requests. The SDT has not included this in R3, but R3 does not require specific external or locally installed controls as in previous versions. Parts 3.1 and 3.2 speak to “deploy methods. . .” and “mitigate the threat of . . .” Neither of those parts require particular external or dedicated controls, and it is expected that such requirements can be accomplished without a TFE. Furthermore, Part 3.3 is clear in its language that it only applies to devices that use signatures or patterns, and the SDT has added clarifying language to account for cases where a signature or pattern is only available infrequently. If a method doesn’t use signatures or patterns, Part 3.3 imposes no obligation upon it. For that reason, the SDT expects a TFE is not necessary. Overall, the SDT has crafted R3 in such a manner to clarify the desired results-based outcome without specifying technology-restrictive controls that would necessitate a TFE. In addition, the included guidance on R3 lists numerous methods an entity can use to meet the requirement.

The SDT received comments that the applicability of R3 should specifically exclude Low Impact BES Cyber Systems. The SDT disagrees with the comment, as the Applicability column throughout the standards specify what is in scope, not what is out of scope. An entity cannot be held to a requirement on a system if that system is not specifically noted in the

applicability column. In addition, with the now clarified "'high water marking"' concept of ESPs and "'Associated Protected Cyber Assets"' it is possible that if Low Impact Cyber Assets are within the same Electronic Security Perimeter ("ESP") with Medium or High impact systems, then they will be in scope of this requirement.

The SDT received comments suggesting limiting the malware requirement to only those medium impact BES Cyber Systems that have External Routable Connectivity. The SDT disagrees as the malware threat is not introduced solely through external network access. The SDT believes that most malware threats in a control system environment enter through portable media or locally connected devices. Stuxnet is one high profile example. For these reasons, tThe SDT has not made the suggested change.

The SDT received comments that the malware requirement should apply to Low Impact BES Cyber Systems. The SDT agrees that this is a good practice, however, in a mandatory and enforceable standard the evidence burden for all cyber assets would divert resources from higher impact systems and tasks. The SDT has purposefully decided to require only programmatic requirements for Low Impact assets and not require inventories or lists (which would be required for any device or system level requirement compliance measurement). This is due primarily to the large order of magnitude of cyber assets that would be in this category and the desire to have the industry not focusing the majority of its efforts on the lowest impact systems. For these reasons, tThe SDT has not made the suggested change.

The SDT received numerous comments on the "wheres" and "hows" of applying this requirement. The SDT has taken the approach of making this a competency based requirement and has stated a high level "what" with no "how.". The issue with previous versions of the standard is that it required a particular technology on all cyber assets, many of which could not meet the requirement. MAs malware prevention is a technical field in which technology is constantly changing and improving and new paradigms are constantly emerging in how to handle the issues, therefore, the SDT has made this a very high level requirement so as to allow entities to keep up- to- date with state of the art tools in this area and to do what makes sense adapt to for the specific systems and situations. There are no prescriptive "silver bullets" that can be specified without recreating the current state of generating more TFE's than incidents of compliance.

The SDT received comments around the terms "disarm or remove" concerning malware threats. Commentoers suggested that in some instances, removing or disarming is not the correct behavior. The SDT agreed and has changed to the following suggested language: to "mitigate the threat of."

The SDT received comments that Part 3.1 should include "based on the Cyber Assets susceptibility to malware" and that "Methods do not have to be used on every single Cyber Asset." The SDT disagrees as adding 'susceptibility' to the requirement is another element that could require some form of evidence from every entity for every Cyber Asset. For these reasons, tThe SDT has not made the change. The SDT has also made the requirement applicable at the systems

level, so that every Cyber Asset is not included. The included guidance discusses this issue and allows for the expressed concern.

The SDT received comments on the signature or pattern update requirement. The SDT agreed with these comments and has made numerous changes to add clarity to handle several special circumstances, as well as allow 35 days so that normal monthly update cycles have a chance to execute (35 days to account for 31 day months, or months that may start or end on a weekend or holiday, while generally supporting "once-a-month" frequency).

The SDT received comments on adding testing of signatures to the requirement. The SDT does not agree that this needs to be a prescriptive requirement. Some cyber assets may need testing because the impact of any false positive on reliability may be great, but other cyber assets within the system may benefit from the more timely and automated deployment of signatures where the impact of a false positive may be negligible. For these reasons, the SDT has not made the suggested change.

The SDT received comments that the signature update process should change from monthly to weekly. The SDT disagrees in that too frequent of a prescriptive requirement may preclude some entities from fully testing updates for those systems where the impact of a false positive is great. The point of the requirement is to state how stale signatures can be; it is not the prescription of ideal state. Other commenters suggested that monthly updates were too short for those who need to do manual updates of signatures. The SDT disagreed, in that if the situation calls for signature updates to be less timely than monthly, then other malware prevention solutions may need to be pursued.

Several other comments concerned the signature update requirement (R3.3), but the SDT stresses the conditional nature of the requirement's wording. It only applies in situations where the entity has chosen malware prevention techniques that are dependent on signature or pattern updates. There are numerous other solutions that are not dependent on signature or pattern updates and this requirement does not apply in those instances.

The SDT received comments that Part 3.2 should be part of an incident response in CIP-008-5. The SDT disagrees and does not believe the two are mutually exclusive. Simply invoking an incident response plan would not be sufficient as the malware would not be required to ever be mitigated. Part 3.2 ensures that the threat from the malware is mitigated. Some commenters requested a definite timeframe for the mitigation, but the SDT disagrees, as that will be situation specific. At times it may be the best course of action on a particular Cyber Asset to leave the malware in place for a time for forensic purposes (to discover what it is doing and who it is communicating with without alerting potential attackers).

Commenters raised issues with proving the 30 day timeframe for updates and suggested adding "from an identified source" for the signature or pattern updates. The SDT agrees and has made the suggested change.

QUESTION 31 – CIP-007 R4:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT not make any changes to Requirement R4 or Part 4.4 but did make significant changes to Parts 4.1, 4.2, 4.3 and 4.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

General Measures concern: The SDT can not determine what an auditor will or will not request as evidence of compliance. The measures as written provide examples of strong supporting evidence of requirement compliance but do not preclude an entity from providing actual logs as evidence if the entity feels this represents appropriate evidence of compliance …. Actual alerts

In response: To the breadth of expressed industry concerns throughout the course of the 706 SDT effort, the SDT has gone to great effort in an attempt to create balanced standards which provide reasonable critical infrastructure cyber security, the latitude to address current and future technical conditions and moderate audit impact.

The SDT has reassessed the overall scope and applicability during the comment review period, and has concluded that CIP-007-5, R4 represents an approach which is a reasonable effort to advance the cyber security of the Bulk Electric System and critical infrastructure overall.

CIP-007-5 M4: With respect to the use of the word "must" rather than "may,", measure is stated in the context of the overall Standard, CIP-007-5, R4, which specifies a requirement for one or more documented processes and the implementation of those processes. M4 specifies evidence must include each of those documented processes, and further includes the evidence recommended in the Measures section of the table of Requirements as appropriate proof of the implementation of the standard, ; though such evidence may exist in many forms.

The SDT thanks you for your comments and consideration in review of CIP-007-5, R4. The responses were varied, decidedly insightful, and, in many cases provided much appreciated suggestions for change. After review of the submitted comments, the SDT updated the requirements with a goal toward improvement and enhancement, while trying to maintain a balance of reasonable critical infrastructure cyber security, latitude to address current and future technical conditions, and to moderate audit impact.

R4.1 received several comments expressing the need to include stronger TFE exclusion language. The SDT determined this is not necessary; but, following lengthy discussion, did determine to modify the language in an attempt to strengthen the basis for not requiring TFE exclusion language. In the context of R4.1, the requirement is to log (in a central repository) the specified event types only if a systemSystem or asset has previously detected and logged such events. Essentially, if event detection and logging at the asset does not occur, there is nothing subject to the R4.1 requirement of logging.

Another common concern with R4.1 was the use of the word "any" being too broad to scope the body of required event types. The SDT feels the use of the word "any" in this context is appropriate and provides an essential scope of security practice for the applicable systemSystems and assets for the purposes stated by the requirement.

R4.1.4: "Any detected potential malicious activity" raised two common themes;

1) The use of the word "potential" was far too broad in scope, a concern with which the SDT agreed and consequently removed the word "potential; and

2) Define "malicious activity," which the SDT determined was not necessary, as the standard English dictionary definitions of the words "malicious" and "activity" provide sufficient definition for behaviors to detect and log, and there is no real benefit to establishing a NERC glossary definition for "Malicious Activity".

Though some comments were received suggesting the removal of the enumerated listed of event types, and removal of

the “at a minimum” language, the SDT persists in the assertion that the enumerated list provides a minimum consistent with previous versions of CIP-005 and CIP-007, and retaining the use of “at a minimum” avoids interpretations that the event types can only be the types enumerated and provides latitude for entities to apply stronger cyber security controls to mitigate risks as warranted.

For R4.2, several comments noted concerns regarding the use of the term ”Real-time” in the requirement and related requests for removal or definition. The SDT offers that “Real-time,” in the context of R4.2 alerting, is appropriate. The intent is to establish that an entity alert on events with an aspect of urgency and immediate concern and respond in a manner of urgency and immediate concern, at least within the context of “Real-time,” as established within the CIP-002 Standard for determination of BES impact.

This is not a requirement that the systems Systems or assets themselves perform an alert, but rather a requirement that the entity implement a method to produce a real-timeReal-time alert upon detection of the stated conditions. The requirement has been updated in an effort to clarify this intent and to further specify the minimum set of events which necessitate a Real-time alert. The method of detection and alerting is not specified, leaving it to the Responsible Entity to develop such methodologies as would be determined appropriate to the level of risk.

The most significant changes were implemented across R4.2, R4.3, and R4.5 in an effort to better focus the intent and action of each and eliminate the conflicts noted in and across R4.3 and R4.5. The action to detect and alert logging errors has been moved from R4.3 and R4.5 to R4.2; leaving R4.3 focused on responding to logging failures, and R4.5 focused on summary review of logs. This largely addresses the confusion within R4.3 and R4.5 regarding dealing with the timing imposition of multiple interdependent actions for logging failures. To address concerns with the lack of specificity, R4.2 was modified to specify a minimum set of security events to alert on, including logging failures.

In addition to the inherent conflicts noted above, R4.3 received several comments and requests to extend the logging failure detection and response activation time frame to “next business day,” rather than “next calendar day” on the basis of potential increase in staffing burden to meet the requirement. Here the SDT continues with the belief that the activity response time threshold of “next calendar day” is reasonable for the applicable systems and assets. These system have sufficient import to warrant consistent detection and logging of at least the minimum behaviors noted. However, the requirement was updated to separate the detection requirement and to more clearly establish the “next calendar day” response activity applies after detection has occurred. It should be noted that this is not specifically a requirement to resolve the issue within that time frame. The action is to activate the response which leaves the Responsible Entity with discretion to assess the risk conditions and alleviate the condition accordingly.

It should also be noted that, wherein some comments were concerned with clarity in understanding what constitutes a

logging failure, the SDT offers that in the context of R4.3, “event logging failures” is intended to direct a Responsible Entity to address logging failures which otherwise prevent a Responsible Entity from performing the activities required by R4 on the whole.

R4.4, in turn, carried several comments to the effect that 90 days of log data was of limited or no benefit, and potentially onerous; or the requirement is actually a compliance data retention function and did not belong in a standard requirement . The SDT offers that this is not considered a data retention requirement. This is a standard requirement to ensure sufficient log data is kept by the Responsible Entity to achieve the intent of requirement 4.1; “for identification of, and after-the-fact investigations of, BES Cyber Security Incidents,” and the activities of 4.5, “Review a summarization or sampling of logged events at a minimum every two weeks to identify undetected BES Cyber Security Incidents.”.

Several other comments for R4.4 raised concern with the phrase “records-of-disposition” in the measures. The SDT recognizes the concerns with the phrase “records of disposition” in the measures, and has updated them to indicate that this is one of a list of potential documentation and has expanded the list of potential evidence to include log data retention configuration reports.

With respect to increasing applicability of 4.4 (90 day log retention) to a broader set of medium, the SDT considered increasing the scope, and concluded that the benefit of increasing the applicable systems or asset scope to include more Medium Impact installations would be less than the potential compliance burden of implementation. The SDT would like to note, however, that any Responsible Entity may go beyond the requirements in the interest of advancing security.

For R4.5, beyond the issues of conflict with 4.3, comments for R4.5 focused on the opinion that a two-week cycle of log summary review was too frequent, once a month was sufficient, and a perceived lack of benefit of such activity. The SDT believes that reviewing logged events at least every two weeks is a reasonable security practice for risks associated with the applicable systems and assets, and reasonably addresses the concerns raised by FERC Order 706, Paragraphs 525 and 628. An intent of this requirement is to supplement the alerting process and ensure entities are regularly reviewing logs for conditions which may not be already be identified for alerting, or indicate changing conditions which warrant an update to the conditions for alerting.

The requirement specifies a timeframe and scope of review, but not the manner of review. The SDT believes by not specifying the manner of review, Responsible Entities may engage in automated or manual review in accordance with their current or future capabilities.

QUESTION 32 – CIP-007 R5:

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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any changes to Requirement R5 but did made significant changes to Parts 5.1 through 5.7 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

For Requirement CIP-007-5 R5 Part 5.1, many commenters did not believe the language was clear on the intent and felt extending this requirement to all components and accounts was not operationally feasible. In response, we have modified Requirement Part 5.1 according to commenters' suggestions. Part 5.1 is now limited to user access authentication and substitutes the word "enforce" for "validate" to provide clarity on the expectation. The reference to internal and remote access paths in the measures has also been removed.

In addition, the increase to 8 character passwords (see Part 5.5 in the revised standard) is part of an overall approach to making password requirements more flexible and appropriate to the risk reduction provided.

For Requirement CIP-007-5 R5 Part 5.2, (now Part 5.5 in the revised standard) commenters generally had 2 issues: (1) it

was unclear whether this requirement applied to individual accounts or types of accounts and (2) the CIP Senior Manager should not be required to authorize these accounts. In response, we have modified the requirement to make clear it applies to specific account types and have removed the requirement that the CIP Senior Manager or delegate authorize the account types.

Requirement CIP-007-5 R5 Part 5.3 refers to documenting personnel with access to shared accounts, which provides additional control to shared account and carries forward from the previous versions of CIP-007 Part 5.2.2.

For Requirement CIP-007-5 R5 Part 5.4, commenters overwhelmingly disagreed with application to all Responsible Entities. In response, we have moved all requirements applying to Low Impact BES Cyber Systems or all Responsible Entities to CIP-003-5 and made clear the requirements were programmatic and did not require a full inventory of BES Cyber Assets.

For Requirement CIP-007-5 R5 Part 5.5, most commenters expressed concern that the password change periodicity left too much open for interpretation. In response, we have moved the password change limitation to Part 5.5.4, reverted to an annual password change requirement and applied it to Medium Impact BES Cyber Systems with Routable External Connectivity.

Modifications were also made to the applicability section to address commenter concerns and to clarify that TFE requests may be submitted for this requirement.

QUESTION 33 – CIP-007 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all of the Requirements (R1 through R5) but did not make any changes to any of the VRFs.

A number of commenters suggested that the VSLs for CIP-007 should be revised so that each requirement has a complete set of four VSLs rather than only a 'High' and 'Severe.' For Requirements R2 and R3, the SDT adopted these suggestions by providing gradations based on how substantially the Responsible Entity missed the timeframe for compliance. For other Requirements, the drafting team did not adopt these suggestions because this approach is inconsistent with the FERC guideline for VSLs that requires each VSL to be based on a single instance of non-compliance (as opposed to cumulative instances). In the case of disabling ports, each port that is not disabled is a single instance of non-compliance,

and it is not possible to be partially compliant.

Several other clarifications to the VSLs for CIP-007-5 were suggested, and the SDT discussed each of the suggestions and adopted those that were consistent with NERC and FERC guidelines for VSLs.

A number of commenters made reference to the need to consider risk in assigning VSLs. Risk is not a factor in VSL assignments – a VSL is a measure of the degree of non-compliance, where a Severe VSL indicates total non-compliance or compliance that entirely misses the reliability intent of the Requirement, and a Lower VSL indicates that the entity was compliant with a substantial portion of the Requirement, but was not 100% compliant.

One commenter recommended changing the VRF for Requirement R2 from Medium to High. The drafting team did not adopt this suggestion because the comment seemed to be conflating VRFs and VSLs.

A small number of commenters suggested assigning multiple VRFs to each Requirement based on whether the systems in question were Medium Impact or High Impact. The SDT did not adopt this suggestion because each Requirement is required to have a single VRF. A single commenter suggested that the Requirements be split into separate Requirements for High and Medium Impact systems, for the same reason, and the drafting team declined ot adopt this suggestion because the team believes that VRFs and VSLs are used in combination with the particular facts of an entity's performance in determining a fair sanction for non-compliant performance.

QUESTION 34 – CIP-008 R1:

CIP-008-5 R1 states "Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity

- Requirements - Use of the phrase, “initially upon the effective date” in Requirements
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The two most commented on issues for CIP-008-5 R1 were (1) coordination with the drafting of EOP-004-2 and (2) the applicability of R1 to all Responsible Entities.

Regarding the draft EOP-004-2, commenters expressed concern with the parallel drafting of EOP-004-2 and CIP-008-5. Some commenters noted the identification of reportable incidents was already covered in EOP-004-2 and the proposed requirements in CIP-008-5 resulted in double jeopardy. In response, the SDT continues to coordinate with Project 2009-01 in their revisions to EOP-004-2. CIP-008-5 requires a process to identify Reportable BES Cyber Security Incidents and EOP-004-2 requires the actual reporting. EOP-004-2 is being revised to refer to “reportable Cyber Security Incidents identified in CIP-008-3 and successor Standards”. We have also reverted to using the term “Cyber Security Incident” to allow the Standards to synchronize. We still propose the glossary term “Reportable Cyber Security Incidents” with a capital “R” as a means of scoping the types of Cyber Security Incidents for which an entity must test, review and perform lessons learned activities. These are also the types of incidents to which the draft EOP-004-2 refers as reportable Cyber Security Incidents. Several commenters also expressed concern about the absence of direction in 1.2 and 1.3 on which entities/agencies should receive reports on Reportable BES Cyber Security Incidents.

Many commenters disagreed with the expanse in scope of CIP-008-5 R1 to include all Responsible Entities. In particular, several noted the applicability was inappropriate because these cyber systems did not have requirements for an ESP and a PSP as referenced in the initial draft definition of BES Cyber Security Incident. In response, the applicability to all Responsible Entities for incident response is appropriate here because having an incident response capability is one of the more effective security controls to address multi-site cyber-attacks on the grid. Please refer to our summary consideration for question 49 regarding the inclusion of certain requirements applicable to all Responsible Entities. All requirements previously posted in CIP-004-5 through CIP-011-1 applying to Low Impact BES Cyber Systems or All Responsible Entities have moved to CIP-003-5 and apply to All Responsible Entities. We have made this change in response to comments to ensure these requirements have similar wording and measures. Also, the definition of BES Cyber Security Incident includes those incidents affecting the BES Cyber System in addition to those incidents associated with the ESP and PSP. Thus, the requirement to implement an incident response plan for High and Medium Impact BES Cyber Systems is now addressed in CIP-003-5, Requirement R1 – and the requirement to implement an incident response

plan for BES Cyber Systems not identified as High or Medium Impact Cyber Systems is addressed in CIP-003-5 Requirement R2. The revised CIP-008-5 does not include any requirements with applicability that says, "All Responsible Entities."

A few commenters expressed concern that applying requirements for incident response implicitly requires protection and monitoring controls. In response, we note the requirements to monitor for security events in CIP-006-5 and CIP-007-5 are applicable to only Medium and High Impact BES Cyber Systems. CIP-008-5 R1 only requires entities have a process to identify BES Cyber Security Incidents. There is no further requirement regarding the operation of event sources that may inform the identification of such incidents.

Some commenters noted that some of the change descriptions and justifications for Requirement R1 and its Parts were not correct. In response, we have modified the rationale and change descriptions for the main requirement and each of its Parts and added details to the justifications where previous documentation was insufficient or incorrect.

Other modifications include an expansion of requirement Part 1.3 into multiple requirement Parts to improve clarity. We also added "groups" in addition to "individuals" for response roles as recognition that incident response tasks may be assigned to a group rather than specific individuals. Guidance was added to CIP-008-5 R1 at the end of the document based on several commenters suggestions, including adding references to assist entities in developing an incident response plan.

QUESTION 35 – CIP-008 R2:

CIP-008-5 R2 states "Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 –BES Cyber Security Incident Response Plan Implementation and Testing.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the requirement and its Parts and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date” in Requirements
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The three most commented on issues for CIP-008-5 R2 were (1) the use of “initially upon the effective date” for periodic performance requirements in Part 2.2, (2) various concerns and disagreement with documenting deviations from the response plan and (3) having data retention requirements in requirement Part 2.3 instead of the compliance section.

In response to the first issue, references to the initial performance in requirements to test and review in CIP-008-5 have been moved to the implementation plan and allow a 12 month time period after the effective date to perform these tasks.

Several commenters noted the requirement to document deviations is administratively burdensome with no real security benefit. They state that entities should not be required to follow the plan because of all the uncertainties associated with a security incident. The SDT agrees that allowances should be made to deviate in the execution of a plan. The addition of this requirement is to address a concern expressed in the FERC Order 706 paragraph 694. This requirement ensures the plan will be used but does not restrict entities from taking needed deviations.

> Order 706 Paragraph 694: For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan. We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard

Commenters also state an explicit requirement to “implement” the plan in Part 2.2 is redundant with the main requirement. In response, we note Part 2.2 further indicates how the BES Cyber Security Incident response plan may be implemented according to the required periodicity and is therefore not duplicative of the main requirement R2. The requirement to “implement” the plan means the plan must be used, but this does not imply all parts of the plan are exercised.

In response to having data retention requirements, Part 2.3 has been modified to remove the actual retention period to

avoid conflicting with the retention periods specified in the compliance section of the Standard. However, the requirement to retain incident documentation is still necessary to ensure data for post-event analysis remains available.

Some commenters noted that some of the change descriptions and justifications for Requirement R2 and its Parts were not correct. In response, we have modified the rationale and change descriptions for the main requirement and each of its Parts and added details to the justifications where previous documentation was insufficient or incorrect.

Corporate Compliance noted the requirements in R2 applied to BES Cyber Security Incidents which can be very expansive. We agree and have modified the scope of these requirements to Reportable BES Cyber Security Incidents.

Other modifications include switching the order of Parts 2.1 and 2.2 to emphasize the main subject of the requirement. We also improved the wording in what is now Part 2.2 based on multiple commenters' suggestions. Guidance was added to CIP-008-5 R2 at the end of the document based on multiple commenters suggestions to add details about expectations with respect to exercising the response plan.

QUESTION 36 – CIP-008 R3:

CIP-008-5 R3 states "Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3, Parts 3.1 through 3.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date" in Requirements
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The primary issue raised by commenters for CIP-008-5 R3 was the clarity in time intervals. Many commenters felt the 30 day window for performing the lessons learned review and additional 60 days for updating was too short in some instances. In response, we have modified the language according to multiple suggestions to make clear the time intervals. We mistakenly proposed 60 calendar days in the posted version, not realizing there was already 30 days to perform the review. The 30 calendar days given to identify any changes from lessons learned and additional 30 days to update the plan (total of 60 days from response plan test) is consistent with FERC directives in Order 706 paragraphs 651, 728, and 731 that 30 calendar days is sufficient for updating documentation. Many commenters also distinguished that the review period in R3.2 should be initiated after the event has completed.

> Order 706 Paragraph 651: The Commission adopts a modified version of the CIP NOPR proposal. We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days. The Commission believes that 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation.
>
> Order 706 Paragraph 728: The Commission stated its concern that individuals responsible for activating and implementing a recovery plan must have the most current information available, and its belief that a 90-day time lag between when a weakness in a recovery plan is discovered and when it is corrected and communicated to such responsible personnel is too long.172 We noted that failure for the responsible personnel to have current information about a recovery plan could cause unnecessary delay in restoring critical cyber assets to service and thereby jeopardize the reliability of the Bulk-Power System. Therefore, the Commission proposed to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans to 30 days, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. We stated our belief that a 30 day requirement for updating the recovery plans will promote timely incorporation of

lessons learned during exercises and actual events, while acknowledging that 90 days is reasonable for the completion of personnel training sessions, due to varied shifts schedules and other feasibility issues with regard to facility and organization.

Order 706 Paragraph 731: The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans. We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective. As we stated with respect to change made pursuant to CIP-007-1, the Commission believes that having correct documentation is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could attempt to operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation. Northern Indiana has not provided us sufficient reason to change the CIP NOPR proposal. Finally, as stated with respect to the documentation requirements in CIP-007-1, the 30 day period should begin upon final implementation of the modifications.

For requirement Part 3.4, several commenters noted that the term “organizational changes” is overly broad. In response, we have modified the Part 3.4 to specifically include organizational changes from the required plan components in R1. This has also been modified to limit these changes to those that “impact the ability to execute the plan”.

For Part 3.5, we have replaced the requirement to “communicate updates” with more specifically, “distribute updates”. Several comments also asked that the phrase “initially upon the effective date of the standard” in Part 3.1 be changed or moved to the implementation plan, and this change was adopted – the implementation plan now allows a 12 month times period after the effective date to perform these tasks.

Some commenters noted that some of the change descriptions and justifications for Requirement R3 and its Parts were not correct. In response, we have modified the change descriptions for the main requirement and each of its Parts and added details to the justifications where previous documentation was insufficient or incorrect.

Guidance was added to CIP-008-5 R3 at the end of the document based on multiple commenters’ suggestions. In particular, we have added timelines to illustrate the timing intervals in R3.

QUESTION 37 – CIP-008 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to VSLs but made no changes to the VRFs.

Please see the redlined version of the standard for the complete set of revisions.

The majority of commenters expressed the need for gradated VSLs, particularly in the timed requirements. In response, we have modified the VSLs to include varying degrees of severity based on the number of days/months late in performance of a requirement.

We incorporated a suggestion to include requirement references to the VSL parts to make it easier to see that noncompliance with each of the Parts is addressed in the set of VSLs associated with each requirement.

We have also updated the VSL language to reflect the changes made to the language in the requirements in CIP-008-5.

QUESTION 38 – CIP-009 R1:

CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement T1 and Parts 1.1 through 1.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"

- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 1.1 - Rationale has been corrected per comments received by removing the reference to Order 706.

(2) Part 1.2 - Returned to the original wording which refers to roles and responsibilities for recovery plan but does not require identification of individuals responsible for the recovery efforts

(3) Part 1.3 - “Protection” requirement has been removed as it was duplicated elsewhere in the CIP-011 requirements.

(4) Part 1.3 - Replaced “restore” with “recover” in order to reinforce the concept of BES system recovery and to specifically exclude full facility restoration.

(5) Part 1.4 and 1.5 - Column headings have been corrected.

(6) Part 1.5 - Was changed to require entities to have a process or guidance to preserve data in their plan and excepting the preservation of data for CIP Exceptional Circumstances so as to not impede or restrict system restoration. The SDT determined that this requirement should remain in the recovery standard versus moving to the response standard, the recovery sequences can have preplanned preservation of data not requiring TFEs.

Some commenters made generic suggestions for improvements to the set of CIP standards and the response to these comments is included in the "Summary Response to Generic Comments" at the front of this report.

QUESTION 39 – CIP-009 R2:

CIP-009-5 R2 states “Each Responsible Entity shall implement one or more processes that collectively address the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.”* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R2 Parts 2.1, 2.2 and 2.3 and to the

associated rationales, and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 2.1 – Replaced "implement" with "test" and deleted the requirement to complete the initial test upon the effective date of the standard.

(2) Part 2.2 – Changed, "…test any information…" to "…test information…"

(3) Part 2.2 – Wording was changed to ensure that recovery information on backup media is "useable and is compatible with current system configurations. " The change was in response to comments that "reflecting current configurations" would be too difficult, as the term "current" was too vague.

(4) Part 2.2 – In response to concerns over requirement language implying that the information must "reflect" current configurations, the SDT believes that it would be sufficient to test that the information remains compatible with current system configurations and has clarified the language to specivy that the test "is compatible with" current configurations.

(5) Part 2.3 – In response to stakeholder concerns that testing plans was burdensome, changed the applicability to require testing only for High Impact BES Systems to focus this requirement on the most critical systems.

(6) Part 2.3 – In response to stakeholder comments indicating that Part 2.3 duplicates Part 2.1 the SDT disagrees because Part 2.3 requires a more thorough operational exercise once every three years than the simpler test required in Part 2.1.

QUESTION 40 – CIP-009 R3:

CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3 Parts 3.1, 3.2, 3.3, and 3.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has made changes to in response to stakeholder comments. Highlights of the changes are shown below. Please see the redlined version of the standard for complete set of revisions to the requirements and measures.

(1) Part 3.1 - In response to many comments disagreeing with the need for an initial review, the SDT essentially removed all Part 3.1 review requirements. Adequate reviews are in the requirements that follow, and the SDT substituted the requirement to conduct reviews with a requirement to document any identified deficiencies or lessons learned associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the

test or recovery.

(2) Part 3.2 – Part 3.2 was moved to Part 3.1. CIP-009-5 Requirement R1 already compels the responsible entity to have a recovery plan, and the plan will already have been reviewed when it was developed and approved. In addition, there will be reviews as each recovery plan test or actual incident recovery lessons learned are incorporated .

(3) Comments regarding improving alignment with CIP 008-5 were received. Part 3.2 essentially remains as it was previously in Part 3.3 while maintaining consistency with CIP 008-5, with 30 days to update the recovery plan after completion of Part 3.1 documentation of deficiencies or lessons learned.

(4) Part 3.3 – Part 3.3 was rewritten align with CIP 008-5 while clarifying, in response to comments, that the responsible entity has the lead in determining changes that would impact its ability to execute the recovery plan.

(5) Part 3.4 – Replaced "communicate all" with "distribute" to clarify and improve the audit ability.

(6) Measures – Associated measures were also updated to reflect the changes to the associated requirements

Following is a response concerning stakeholder objections to the language in Part 3.1 to have the review of the recovery plan "initially upon the effective date":

In several instances in the Version 5 requirements, the SDT proposed periodic performance of some requirements, and they specified in the first posted draft's requirement language that the first iteration must be performed "initially upon the effective date." Several commenters raised concerns with this language, and they suggested that not all initial performances should occur upon or before the effective date. The SDT agrees, and it has evaluated each periodic performance requirement. Consequently, the drafting team has removed "initially upon the effective date" from all the CIP standards, and references to the initial performance in the requirements have been moved to the implementation plan.

Former part 3.2 (now part 3.1) – Some stakeholders indicated that 30 days was not sufficient to update documentation and the SDT disagrees. Given the importance of having these plans in place the SDT believes that 30 days is sufficient to update documentation.

Former part 3.4 (now part 3.3) – Some stakeholders questioned the need for Part 3.4 – the requirement to update the recovery plans. The SDT believes that current part 3.3 is in alignment with FERC Order 706, paragraph 686.

> Order 706 Paragraph 686:"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills,

and responses to actual incidents, all of which must include lessons learned. The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.

QUESTION 41 – CIP-009 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all of the requirements in CIP-009 but made no changes to the VRFs.

The majority of commenters who provided comments on proposed VRFs and VSLs asked for gradated VSLs, particularly in requirements specifying a time period. In response, the SDT has reworked all of the VSLs. They are now gradated, and they are based on the number of days/months late for particular requirements that specify periodic performance. In most cases, the team fully gradated the requirement to account for Low, Moderate, High, and Severe VSLs.

Some commenters were concerned that the VSLs require 100% compliance, but the SDT notes that the FERC and NERC guidelines for VSLs require each VSL to account for all levels of noncompliance. However, as noted earlier, the SDT has made significant efforts to make the VSLs in this standard gradated in nature, such that smaller violations fall within the "lower" VSL. Other comments recommend a Corrective Action Program (CAP) be implemented by registered entities, but the SDT notes that a Corrective Action Program is not the same as a VSL. A VSL accounts for the level of noncompliance, and the Corrective Action Program comes after one has already determined some level of noncompliance. While noting the value of Corrective Action Programs in certain circumstances, the VSL or the standard itself is distinct from this enforcement mechanism.

Some commented on the evidence retention period for the standard and expressed concern over the authority for a CEA to ask an entity to provide other evidence to show that it was compliant for any period since the last audit that may exceed the specified evidence retention period. The commenter noted concern that the guidance is contradictory. The SDT notes that the evidence retention language the commenter is concerned about is boilerplate language for the evidence retention section, and it is meant to specify that the evidence required during that additional period is not necessarily the full amount of evidence that is otherwise required during the specified evidence retention period. The Rules of Procedure Appendix 4c - Section 3.1.4.2 that became effective Jan 1 2011 identifies that the CEA can ask an

entity to demonstrate that it was compliant for the full period of time since the last audit without regard to what is stated in the evidence retention section of the standard.

One commenter suggested that periodic requirements that require performance "...initially upon the effective date..." be moved to the implementation plan. The SDT agrees, and all periodic requirements' initial performance is now outlined in the implementation plan.

Finally, the drafting team notes that it has updated the VSLs in the standard to reflect the draft requirement language in CIP-009-5.

QUESTION 42 – CIP-010 R1:

CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R1, but did make significant changes to its rationale and to Parts 1.1 through 1.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Numerous comments were centered around several main issues. In response to those comments, the SDT has made revisions to the main parts and sub-parts in Requirement R1. Please see the redline version of the standard for complete revisions. Below is a highlight of the revisions:

(1) Part 1.1 - Removed physical location from part 1.1.1.

(2) Part 1.2 - Removed CIP Senior Manager language for authorization of deviations to existing baseline configurations.

(3) Part 1.3 - Added clarity around updating documents around NERC Standards to CIP-005 and CIP-007.

(4) Part 1.4 - Removed scripts from formerly part 1.1.4 now part 1.1.3.

(5) Part 1.4 - Added clarity around cyber security controls to reference CIP-005 through CIP-007.

(6) Part 1.5 - Allowed for TFEs and production environments where the test is performed in a manner that minimizes adverse effects.

Following are responses to comments:

Part 1.1 – 'Grouping' is one method that an entity could use to identify multiple software programs. Requirement R1 Part 1.1 is written to allow flexibility for entities to develop their baseline configuration with the items required as they see fit.

Part 1.3 – The phrase "as necessary" is used to limit the amount of effort required in regards to updating the baseline configuration and other documentation required by a NERC CIP Standard.

Part 1.1.3 – The intent of CIP-010-1 Requirement R1 Part1.1.3 is to be able to define what commercially available application software should exist on the responsible entity's BES Cyber System. If additional software has been unintentionally installed, the entity should be able to document this so as to be able to identify software that was maliciously installed in future assessments. The SDT believes that even certain software changes can unexpectedly lead to exploited vulnerabilities or other adverse effects. Therefore, changes include any changes that deviate from baseline configurations.

Part 1.1.3 – The SDT intent of "commercially available" and "intentionally installed" in regards to application software was to be able to restrict the identification of "notepad" applications, but include the identification of commercially available software such as Linux or Windows.

Formerly Parts 1.1.5 and 1.1.6 (Parts 1.1.4 and 1.1.5 in the revised standard) - The SDT intentionally used “any” as a modifier for the items that should be included in a baseline configuration. The term “any” suggests that if the item does not exist on the BES Cyber System, then the entity would not need to include the item in its baseline configuration. If “any” was not included, then an entity would be required to have an item on its baseline configuration that may not be installed on the BES Cyber System.

Parts 1.4.1 and 1.5.2 – Work together in an effort to ensure changes are tested properly. Prior to implementing a change to a BES Cyber System that deviates from the existing baseline configuration, an entity must determine the impacted cyber security controls (added language specifying cyber security controls identified in CIP-005 through CIP-007) according to CIP-010-1 Requirement R1 Part 1.4. CIP-010-1 Requirement R1 Part 1.5 asks entities to test the controls prior to implementing the change in a production environment. Entities are then to verify that the controls determined in CIP-010.1 Requirement R1 Part 1.4.1 were not adversely affected by the change.

Part 1.4.2 – The SDT’s use of availability is in regards to the BES Cyber System’s ability to operate as designed after a change to the baseline configuration has been made. The concept presented here is to be able to meet the FERC Order 706 directive around “processes that permit a reasonably high level of confidence modifications do not have unintended consequence”.

Parts 1.4 and 1.5 – CIP-010-1 Requirement R1 Part 1.4 Part1.5 are different requirements that can be taken as complementary rather than duplicative for Control Centers. CIP-010 R1 Part 1.5 requires testing changes in the test environment, while CIP-010-1 Part 1.4 requires researching and documenting changes. Due to the level of impact of a compromised Control Center, the SDT believes that testing changes in a test environment is necessary and contributes to the overall prevention of unauthorized modifications of the BES Cyber System.

Part 1.5 – The SDT believes that CIP-010-1 Requirement R1 Part 1.5.1 written as is presents a sufficiently, clear objective. The precursor to Part 1.5.1 and Part 1.5.2 is “entrance criteria” text ensuring the related parts are only applicable if there is a change that deviates from the existing baseline configuration for Control Centers. The SDT believes “including a description of the measures used to account for any differences in operation between the test and production environment” is necessary since it may not always be possible for test environments to exactly mimic production environments.

Parts 1.5.1 and 1.5.2 – The language of CIP-010-1 Requirement R1 Part 1.5 requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that its model takes into account the details of CIP-010-1 Part 1.5, then the entity would not be in

violation of the requirement.

Following is response to comments concerning applicability:

The SDT has modified the applicability sections of all of the CIP Version 5 standards for consistency.

Following is a response to comments concerning baseline configuration:

Part 1.1 – The SDT believes that CIP-010-1 Part 1.1 does indeed adhere to FERC Order 706, paragraph 399.

> Order 706 Paragraph 399: Many of the comments address practical issues involved in addressing accidental consequences and malicious actions, and we recognize that such issues exist. We, thus, agree with Puget Sound that change control and configuration management processes for critical cyber assets cannot ensure 100 percent integrity for those assets when making changes. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. However, we reject Puget Sound's proposal that the Reliability Standard should expressly recognize that absolute assurances are not required.
>
> We also believe that our revised directive to the ERO on Requirement R6 addresses Puget Sound's concern about the limitations imposed by a test environment.

The SDT believes that establishing a baseline configuration is the first step to "provide an express acknowledgment of the need for change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." Accordingly, the SDT believes that the baseline configuration should be included in CIP-010-1 Requirement R2 Part2.1. CIP-010-1 Part 1.1 has been modified in consideration of your comment. The SDT believes that monitoring for changes to baseline configuration, in combination with the change management processes defined in CIP-010-1 R1, can aid in preventing unauthorized modifications to BES Cyber Systems. This new requirement was also added to address the remaining objectives of FERC Order 706 (Paragraph 397).

> Order 706 Paragraph 397: Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP-003-1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management
>
> that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST

Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems

should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

Following are responses to comments concerning documentation:

Some comments suggested that the Version 5 standards should not have any documentation requirements. In general, the SDT has endeavored to remove or minimize requirements that exist solely for purposes of creating documentation. However, there are other factors that support the use of requiring documentation in certain instances. The SDT has attempted to strike the appropriate balance.

The SDT notes that many NERC standards require some level of procedure documentation to support the pre-thought responses to known conditions or to ensure consistent responses when known events happen. Furthermore, certain documentation is essential to measure what needs to be secured. The SDT has sought to minimize such documentation requirements, and it has tried to provide detailed guidance. However, guidance alone is not a sufficient place for such documentation needs, as guidance is not mandatory or enforceable.

Following are responses to comments concerning evidence retention:

Some commenters raised concerns about the evidence retention periods in the standards, to include concern that they are not the same as those in Version 4, that they increase the period from one to three years, or raised concerns that they have a general misunderstanding over retention when the period between compliance audits may exceed the frequency stated.

The evidence retention periods in the compliance section of the standards have been modified to make clear the expectation from the CMEP that entities have compliance evidence for the entire audit period. Furthermore, in some cases, compliance retention is different than records retention for the purpose of security analysis. The “requirement” level retention, where applicable, relates to maintaining records long enough to analyze them for security purposes, anomalous behavior, etc. – these retention periods are for records that are retained by the responsible entity for the responsible entity’s own use; “compliance” retention, as specified in the compliance section of the standard, deals with demonstrating that the requirement has been met (e.g., to demonstrate that the entity has maintained a “rolling” 90-day set of logs throughout the entire compliance audit period where the requirement specifies logging for 90 days) – these

retention periods are solely for the purpose of demonstrating compliance. With respect to increases in the evidence retention periods from one to three years, the SDT notes that the initial evidence retention language pre-dates the establishment of the compliance program and its associated documented procedures. The compliance program requires that entities must "demonstrate compliance" for the entire compliance period (not that they must maintain all records for the entire compliance period). Note the distinction between demonstrating compliance and maintaining all records noted in the requirements (e.g., again, to maintain records for 90 days for security analysis vs. demonstrating that records have been kept for a rolling 90-day period for an entire compliance period, whether 3 or 6 years).

Following are responses to comments concerning the test and production environments in Requirement R1, Part 1.5:

The language of CIP-010-1 Part 1.5 requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that their model takes into account the details of CIP-010-1 R1.5, then the entity would not be in violation of the requirement.

The language of CIP-010-1 Requirement R3, Part 3.2 requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that their model takes into account the details of CIP-010-1 R1.5, then the entity would not be in violation of the requirement.

Prior to implementing a change to a BES Cyber System that deviates from the existing baseline configuration, an entity must determine the impacted cyber security controls (added language specifying cyber security controls identified in CIP-005 through CIP-007) according to CIP-010-1 Part 1.4 (CIP-010-1 Requirement R4, Part 4.1.1). CIP-010-1 Part 1.5 (applicable to High Impact BES Cyber Systems only) asks entities to test the controls prior to implementing the change in a production environment and then document the results. Entities are then to verify that the controls determined in CIP-010.1 Part 1.4.1 were not adversely affected by the change (CIP-010-1 Part 1.4.2). This process ensures that (quoting FERC Order 706) "a reasonably high level of confidence modifications do not have unintended consequence".

Following is a response to comments concerning measures:

The SDT reminds commenters, as stated in the Background of the standard, "Measures… provide examples of evidence to show documentation and implementation of specific elements required in the documentation process".

QUESTION 43 – CIP-010 R2:

CIP010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R2 but did make significant changes to Part 2.1 and the associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has made several changes to CIP-010-1 Requirement R2 in consideration of industry comments:

(1) Clarity has been added regarding monitoring for configuration changes.

(2) Part 2.1 - The language "monitor for changes to the baseline configuration" to "monitor continuously or periodically, not to exceed once every 35 calendar days". The 35 calendar days reflects, generally, a "monthly" timeframe while allowing for slight flexibility for weekends, holidays, etc., that might fall at the beginning or end of a particular month.

Following are responses to various comments:

The applicability of CIP-010-1, Requirement R2 incorrectly identified Medium Impact BES Cyber Systems during the last posting. This was a transcription mistake from earlier drafts, and Medium Impact BES Cyber Systems have been removed

from the applicability.

In response to how to automate finding the difference between ephemeral and unauthorized ports. CIP-010-1 Requirement R1's baseline configuration identifies available ports for the BES Cyber System (while CIP-005-5 references the enabling of ports).

An unauthorized change would be a change that deviates from what the entity had identified on its baseline configuration. Recall that the baseline configuration is looking only at logical network accessible ports. A concern of double jeopardy between Requirements R1 and R2 was raised. The SDT believes that Requirements R1 and R2 in combination provide for the effective "monitoring of the configuration of the BES Cyber System and provides an express acknowledgement of the need to consider malicious actions along with intentional change." The SDT does not feel this creates double jeopardy.

Comments were received concerning the burden of detecting unauthorized changes and the load placed on systems caused by automation. The SDT believes that monitoring for changes to baseline configuration, in combination with the change management processes defined in CIP-010-1 R1, can aid in preventing unauthorized modifications to BES Cyber Systems. This new requirement was also added to address the remaining objectives of FERC Order 706 (Paragraph 397).

> Order 706 Paragraph 397: Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP-003-1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

As stated in the CIP-010-1 Guidelines, "It should be understood that the intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). It is for this reason that automated technical monitoring was not explicitly required and an entity may choose to accomplish this requirement through manual procedural controls."

Following is a response to comments concerning evidence retention:

Some commenters raised concerns about the evidence retention periods in the standards, to include concern that they are not the same as those in Version 4, that they increase the period from one to three years, or a that they have a general misunderstanding over retention when the period between compliance audits may exceed the frequency stated.

The evidence retention periods in the compliance section of the standards have been modified to make clear the expectation from the CMEP that entities have compliance evidence for the entire audit period. Furthermore, in some cases, compliance retention is different than records retention for the purpose of security analysis. The "requirement" level retention, where applicable, relates to maintaining records long enough for the responsible entity to analyze them for its own security purposes, anomalous behavior, etc.; "compliance" retention, as specified in the compliance section of the standard, deals with demonstrating that the requirement has been met (e.g., to demonstrate that the entity has maintained a "rolling" 90-day set of logs throughout the entire compliance audit period where the requirement specifies logging for 90 days). With respect to increases in the evidence retention periods from one to three years, the SDT notes that the initial evidence retention language pre-dates the establishment of the compliance program and its associated documented procedures. The compliance program requires that entities must "demonstrate compliance" for the entire compliance period (not that they must maintain all records for the entire compliance period). Note the distinction between demonstrating compliance and maintaining all records noted in the requirements (e.g., again, to maintain records for 90 days for security analysis vs. demonstrating that records have been kept for a rolling 90-day period for an entire compliance period, whether 3 or 6 years).

Following are responses concerning technical feasibility exceptions:

In regards to technical feasibility, the SDT notes the technically feasible language in CIP-010-1 R2 is consistent with its use in other V5 standards.

Some commenters asked whether the Technical Feasibility Exception ("TFE") process in the NERC Rules of Procedure, Appendix 4D, will be revised upon changes made to these standards. The SDT notes that requirements that require the submission of a TFE are identified in the NERC Rules of Procedure and changes to that document are outside of the scope of this SDT. Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a TFE when alternative measures are implemented. It is expected that the NERC TFE process will be modified to specify which requirements of Version 5's standards will require TFE submissions once the standards are finalized and submitted to the Commission.

Other commenters were concerned that "where technically feasible" suggests that an entity may unilaterally decide that a requirement does not apply, without filing for a TFE. The SDT respectfully notes that entities are required to be compliant with all NERC reliability standards for which their function is applied. In some cases, compliance is

demonstrated by showing that the entity has no applicable assets; in other cases, compliance is demonstrated through the TFE process. In no case does any language in a NERC reliability standard grant an exemption from compliance to applicable Responsible Entities.

QUESTION 44 – CIP-010 R3:

CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R3 but did make significant changes to Parts 3.1 through 3.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has made several changes to CIP-010-1 Requirement R3 parts and the associated measures in consideration of industry comments. Below is a highlight of the revisions. Please see the redline version of the standard for a complete set of revisions to the requirements and measures:

(1) Part 3.1 - Removed “initially upon the effective date”.

(2) Part 3.1 - Clarified security controls to refer to CIP-005 through CIP-007.

(3) Part 3.2 - Removed “initially upon the effective date” and replaced with “where technically feasible”.

(4) Part 3.2 - Allowed for production environments where the test is performed in a manner that minimizes adverse effects.

(5) Part 3.3 - Applicability – added Associated Protected Cyber Assets.

(6) Part 3.3 - Added …” and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).”

(7) Part 3.4 - Added “any remediation or mitigation action items.”

(8) M3.1 - Changed to “once” every calendar year and added “or”.

(9) M3.2 - Changed to “at least once every 36 calendar months between assessments.”

(10) M3.3 - Removed BES.

(11) M3.4 - Added …“documented” proposed dates of completion “for the action plan...”

Following are responses to various comments:

Requirement R3 – When asked about Vulnerability Assessments, the SDT responds that Vulnerability Assessments act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the posture of BES Cyber Systems. This new requirement was also added to address the remaining objectives of FERC Order 706 (Paragraph 644).

> Order 706 Paragraph 644: The Commission agrees with ISO-NE that hardware and software is implemented in diverse ways throughout the industry, but does not believe that this renders providing guidance infeasible. We also agree that overly rigid guidance could result in responsible entities failing to properly test for vulnerabilities specific to the entities’ environments and systems. The Commission does not believe that the revised Reliability Standard should be inflexible. It should encourage responsible entities to take into account emerging and diverse technologies and newly discovered vulnerabilities as they emerge. The Commission believes that it is appropriate to leave such guidance to the Reliability
>
> Standards development process. Further, we leave it to the ERO’s discretion whether to put guidance in the

revised Reliability Standard or a reference document.

Requirement R3 and parts – Please note that neither Requirement R3 nor its parts use the term passive vulnerability assessment.

Part 3.1 - A request for clarification of whether variances noted in the assessment would be required to self-report was noted. No, the purpose of a vulnerability assessment is the ability to detect vulnerabilities that have been previously unknown.

Part 3.1 – A commenter notes the annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed and suggests allowing two years between vulnerability assessments. The SDT notes that Part 3.1 requires a paper or active vulnerability assessment to determine the extent to which the security controls identified in CIP-005 through CIP-007 are implemented correctly and operating as designed. The SDT does not prescribe what should be included in an entity's paper or active vulnerability assessment as this is left for the entity to determine. The annual timeframe is carried over from CIP-007-4 Requirement R8 and at this time the SDT does not have sufficient data to justify extending the timeframe as proposed.

Part 3.2 - Requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that its model takes into account the details of CIP-010-1 Part 1.5, then the entity would not be in violation of the requirement.

Part 3.2- Request for clarification of what a "test environment" is compared to a "production environment." As stated in Guidelines, "Additionally, the entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a control center BES Cyber System which may not be able to be replicated such as a legacy map-board controller or the numerous data communication links from the field or to other control centers (such as by ICCP)."

Part 3.3 - CIP Exceptional Circumstances is a newly defined term that will be included in the NERC Glossary of terms with NERC CIP V5 standards approval. CIP Exceptional Circumstances are defined as "A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of

large scale workforce availability." The intent was to capture circumstances that may require exceptions to the NERC CIP standards.

Part 3.3 - Is not covered by the Implementation Plan by design, as it is a requirement specifying vulnerability assessments for adding Cyber Assets to High Impact BES Cyber Systems.

Part 3.4 –A question was asked about what date the auditor will audit against if there is not an exact time period listed in the requirement e.g. 90 days. The SDT notes that an auditor would audit the requirement based on the planned date that identified and documented by the responsible entity in its action plan. The SDT did not specify acceptable deviation between the environments as the requirement language only requires documentation and the measures used to account for any differences.

Part 3.4 - A concern was expressed about the potential need for a CAN around the acceptable deviation between test and production that auditors will allow. The SDT did not specify acceptable deviation between the environments as the requirement language only requires documentation and the measures used to account for any differences.

Following is a response to comments concerning measures:

The SDT reminds commenters, as stated in the Background of the standard, "Measures… provide examples of evidence to show documentation and implementation of specific elements required in the documentation process".

Following is a response concerning wireless review in the Guidelines section versus the Requirement section:

Since wireless can be a potential attack vector, "Wireless Review" and "Wireless Scanning" elements were included in the Guidelines and Technical Basis section for CIP-010-1 R3. Guidance provides details on the elements that should be included within an active vulnerability assessment. In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

QUESTION 45 – CIP-010 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all requirements, and changed the VRF for R1 and R2 from Lower to Medium. In addition, the SDT added another time horizon, "Long-term Planning" to R3.

Several comments were received concerning the severity of the VSLs. While the SDT appreciates the perspectives of the

commenters, the SDT notes the VSLs are aligned with mapped requirements from Version 4 of related standards.

A comment was received concerning the VSLs having the potential to cause double jeopardy. The SDT notes that only requirements can put an entity in the position of double jeopardy.

For comments related to evidence retention and baseline configuration, the SDT refers the commenters to the summary for Question 42.

QUESTION 46 – CIP-011 R1:

CIP-011-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-5 Table R1 – Information Protection*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Comments regarding Question #46 dealt with several topics, including: (1) the scope of CIP 011-5 R1, (2) confusion concerning assessments, (3) measures used to identify BES Cyber System Information, (4) overlap with access control, and (5) consistent wording.

(1) Scope of CIP 011-5 R1

Several commenters responded that the scope for CIP 011-5 was too broad. In keeping with prior versions of CIP, the "Associated Protected Cyber Assets" has been removed from the scope of CIP 011-5, thus narrowing the scope of the standard further.

Some commenters were confused about which requirements applied to Low Impact BES Cyber Systems. The scope of CIP 011-5 does not apply to any Low Impact BES Cyber Systems. With the next posting, the drafting team has taken additional actions to make clear which requirements apply to Low Impact systems. These requirements have been grouped in the policy requirements of CIP-003-5.

Some commenters asked how the requirement to protect information applies to third parties with whom the entity may do business. The requirements to identify and control access to information apply to entities and also to third parties with whom the entity may share the information. If the third party is not registered as an entity, it may be difficult for NERC to enforce the standard upon the third party. The drafting team believes it is incumbent upon the Responsible Entity to ensure that BES Cyber System Information is handled in accordance with the CIP standards if that entity decides

to share the information with a third party.

Entities asked if CIP 011 R1 pertains to information concerning BES Cyber Systems or if it pertains to information stored within BES Cyber Systems. The SDT discussed this matter during drafting team meetings. CIP 011 R1 is about information concerning BES Cyber Systems regardless of where such information is stored. Both information "about" the BES Cyber System and information residing "in" the BES Cyber System would be within the scope for Requirement R1 in CIP 011.

There were multiple comments suggesting that CIP 011-5 R1 was overly burdensome. The drafting team does not agree that CIP 011-5 is overly burdensome. The components required in CIP 011-5 are that the entity have a BES Cyber System Information protection program, that BES Cyber System information can be identified, that the program include procedures for handling the information, that adherence to the program is annually assessed, action is taken to address deficiencies identified in the assessment, and that BES Cyber System information is removed from devices prior to their destruction or release for re-use. These requirements are very similar to what has been required in previous versions of CIP standards.

(2) Confusion Concerning Assessments

There were many comments regarding the initial assessment as required in CIP 011-5 Requirement R1, Part 1.3. Regarding Part 1.3., the SDT agrees with these comments concerning the initial assessment and has modified this language. The words "initially upon the effective date of the standard" have been removed from the requirement. The initial instance of periodic requirements is addressed in the revised Implementation Plan.

Multiple commenters asked if a deficiency identified in the annual assessment would become a self- report. The drafting team consulted the NERC Compliance department and was informed that the discovery of a deficiency (if it is a "possible violation") is reportable as a self-report.

(3) Measures Used to Identify BES Cyber System Information

There were many comments about measures, interpretation of measures, and changes to measures. The SDT believes that measures are meant to show the types of evidence that might be used to demonstrate implementation of the requirement. The measures are not intended to be a prescriptive list of what must be utilized to demonstrate compliance unless there is only one way of demonstrating compliance. If a requirement states that the responsible entity must have a procedure, then the measure clearly states that the responsible entity "must" have the procedure to demonstrate compliance. Most requirements to "have" a documented procedure also have a requirement to "implement" that procedure. Because there are typically many ways of demonstrating that the entity has "implemented" a procedure, then the associated measure provides examples of ways entities "may" demonstrate compliance. The measures are intended to provide guidance to the entity and are not meant to be mandatory and enforceable. The SDT

does not intend the measure to be an exhaustive list of acceptable forms of evidence, but rather a list of possible examples. However, at the urging of comments, the SDT added more specifics concerning what types of measures are acceptable. Although labeling or marking information was mentioned in the measure for Requirement R1 Part 1.1, it is not specifically required. The entity has flexibility to use some other method to identify its BES Cyber System Information.

There was some confusion about the "methods" to identify BES Cyber System Information in Requirement R1 Part 1.1. The SDT added the language "documented and implemented" to Part 1.1 to clarify that the methods selected by the entity to identify BES Cyber System information must be written and that evidence of implementation is required.

(4) Overlap in Access Control

There were several comments pointing out the overlap between access control for information, which was included in both in CIP 011-5 R1.2 and also in CIP 004-5. The Requirement for procedures relating to access control was removed from CIP 011-5 and is only referenced in CIP 004-5, thus eliminating duplication.

(5) Consistent Wording

Some commenters objected to the use of the words "protection process" when the reference in previous versions was to "protection program." Regarding the use of the phrase "protection process" in R1.3, the drafting team agrees with the comments and has modified the language so that R1 and R1.3 are in agreement and reference information "protection program."

Commenters asked that the phrase "date of the order" at the beginning of the standard be replaced with the phrase "effective date of the order." The drafting team agrees that the phrase "effective date of the order should be used for clarity, and this change was implemented in the "Effective Dates" section of the revised standard .

Multiple commenters asked that the Summary of Changes in the Rationale section include the specific previous requirements from which CIP version 5 was developed. The SDT agrees, and a corresponding change has been made to include those requirements.

QUESTION 47 – CIP-011 R2:

CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-5 Table R2 – Media Reuse and Disposal*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

There were several summary topics of interest to commenters: (1) scope of the requirement, (2) footnote used in the posting, and (3) application within the same physical boundary, and (4) amount of specific direction included in the requirement and (5) alternative wording suggestions. (1) Scope of the Requirement

Multiple commenters requested changes in applicability to reduce the scope of this requirement. The SDT considered the suggested changes to applicability. However, the posted applicability is in keeping with previous versions of CIP, and the SDT believes the applicability is appropriate. Therefore, the SDT has decided not to make changes in applicability as suggested by the commenters.

Multiple entities commented that the information protection requirements were not wide spread enough and should cover all computer processing and storage assets such as in printer memory, email servers, etc. The SDT discussed this recommendation in drafting team meetings. It is not the intent of the drafting team to include email servers, printer memory, etc. in this requirement. The drafting team appreciates the comments that expand the scope of what is currently covered under CIP-011. While the drafting team agrees that such expansion of scope may increase overall security posture, the scope will not be expanded at this time.

Some commenters were confused about which requirements applied to Low Impact BES Cyber Systems. CIP-011 does not apply to Low Impact systems. The drafting team moved all requirements that apply to Low Impact systems into CIP-003-5.

(2) Footnote Used in the Posting

There were many comments objecting to the use of the footnote in the posting. The footnote was meant to clarify what the SDT meant when they referred to "media" within this standard. Footnotes are acceptable in standards provided the footnote provides clarity without including mandatory performance not addressed in the requirement itself. However, there was an overwhelming response from industry asking for removal or modification of the footnote. In response to industry's concerns, the SDT removed the footnote. The information contained in the footnote, which broadly identified

media, has been removed from Requirement R2, Part 2.1. The pertinent information has been incorporated into Part 2.1 for clarity.

Some commenters wanted the term "media" added to the NERC Glossary and they also questioned why the term "release for reuse" was used in R2 rather than the term "redeployment" While the SDT considered adding the term "media" to the Glossary, it has declined to do so since the term is only referenced within two of the CIP standards. The intent in changing from the term "redeployment" was to make clear that an entity could remove the asset from service without redeploying the asset. Requirement R2 in version 5 does not apply until the time the asset is released for re-use.

(3) Application with the Same Physical Boundary

Some comments related to reuse of the asset within the same physical control zone. The SDT agrees with the concerns expressed, and the SDT has modified the language in the requirement to address the concerns. Additional language has been added to specify that the requirement does not apply to reuse within the same BES Cyber System or associated Cyber Asset by adding the parenthetical "(except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset)". Comments were also received concerning the removal of the media from the Cyber Asset to allow off-line analysis, which would be neither reuse nor disposal. The SDT believes that the current language allows for off line analysis. The requirement applies prior to the time the asset is released for re-use. If the Cyber Asset is off line for analysis but has not been released for re-use, the requirement does not apply. Guidelines supplied in the standard cover this situation. Guidelines state: "This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as that should not constitute a release for reuse."

Commenters also wanted clarity around situations where the asset was removed from the Defined Physical Boundary. The SDT agrees, and SDT added additional language to address these concerns. Chain of custody must be maintained if the BES Cyber Asset is removed from the Defined Physical Boundary prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information.

(4) Specific Direction Included in the Requirement

Some entities asked that the requirement only specify that a process is needed and the method for sanitizing the information be left to the discretion of the entity. Other commenters asked that a specific method such as National Institute of Standards and Technology (NIST) SP800-88 be set forth . The SDT considered the benefits of each approach. The method that an entity chooses to implement to meet these requirements is left to the discretion of the entity. Guidance suggests that entities review NIST 800-88 for additional implementation methods. While guidance is provided for the sake of clarity, the guidance is not mandatory and enforceable.

Some commenters asked for additional clarity concerning the measures. Additional specific examples were added to the measures to provide the desired clarity including references to chain of custody if removed from the Physical Boundary and evidence of encryption if retained within the Physical Boundary.

(5) Alternative Wording Suggestions

Some commenters asked that the phrase "take action to prevent unauthorized retrieval" be changed to "prevent unauthorized retrieval." The SDT considered the alternate language but decided not to make the suggested change. The SDT does not believe the recommended change is appropriate. An entity can certainly "take action" to prevent unauthorized retrieval and such actions can be verified as stated in the posted requirement language. Take action is the phrase currently used in the requirement. The entity may not be able to present evidence that they have "prevented" any and all unauthorized retrieval as some commenters suggested in the proposed requirement language.

Industry comments pointed out that the original posting stated "Prior to the disposal of BES Cyber Assets…" the entity must take action to prevent unauthorized retrieval of information. Industry comments suggested that the phrase should read "Prior to the disposal of BES Cyber Assets that contain BES Cyber System information…" the entity must take action to prevent unauthorized retrieval of information. The SDT agrees that the recommendation clarifies the intent and has made a corresponding change to Requirement R2, Part 2.1 and Part 2.2 language so they both state "that contain BES Cyber System Information."

In some cases, entities asked that the two parts in R2 be consolidated such as: "Prior to the physical removal of BES Cyber Asset media from a Defined Physical Boundary, the Responsible Entity shall implement a 7-pass media overwrite, degauss, or physically destroy BES Cyber Asset media. Each instance shall be documented within thirty (30) calendar days of occurrence." While the SDT agrees that information related to the Defined Physical Boundary must be included, the SDT disagrees with the proposal to reduce the two parts to one, and has left the requirement as two parts because one part deals with reuse and the other with disposal.

Commenters pointed out that the last paragraph in the Guidelines section referred to "erased" and not "cleared". The SDT agrees and has made the conforming change to "cleared."

Some commenters objected to the use of the word "destroy" in R2.2. of the posting. The SDT understands the issue pointed out by the industry. The requirement provides an alternate path. Destruction is only needed in the event that unauthorized retrieval cannot be prevented. The SDT has modified the language in the requirement to more closely resemble the recommendation made by commenters. The revised Part 2.2 now states, "…to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media."

QUESTION 48 – CIP-011 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

There were several issues of interest to commenters concerning the CIP 011 VRFs and VSLs including: (1) lack of a posted VSL and VRF Analysis, (2) VSLs - various wording changes, (3) level prescribed for VRFs, (4) level prescribed for VSLs, and (5) question concerning the purpose of guidelines.

(1) VSL and VRF Analysis

Commenters stated that "A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards…" The SDT consulting with NERC staff on this issue. The VSL and VRF analysis is under development and will be posted soon.

(2) VSLs – Various Wording Changes

Some commenters proposed removal of the first paragraph in the VSLs for R1 as they indicated the paragraph was mirrored within the subsequent paragraphs that better frame the violation. The drafting team agrees with this recommendation but has modified the VSL language rather than remove the paragraph.

Other commenters proposed that the phrase "as stated in the requirement" be added to the CIP 011-5 R1 High VSL. The SDT has modified the VSLs to add clarity about the levels of noncompliance, and they have made them more consistent with the other standards.

In response to comments, the SDT has also modified the VSLs related to R2. Previously, the VSLs referred to preventing unauthorized retrieval from "media" and flash drives would have been in scope. That was not the drafting team's intent. The VSLs now refer to preventing unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. The modification more closely reflects the drafting team's intent. The flash drives do not meet the definition of a BES Cyber Asset and would not be in scope.

Some commenters asked that the VSLs be re-written by device type. The SDT considered this proposal, but has decided not to re-write the VSLs to reflect severity levels specific to device type as this would make the VSLs overly complex.

Some comments recommended a stepped approach for CIP 011-5 R2 such as: If the process to prevent unauthorized retrieval wasn't done on 1 device that would be low 2-5 moderate, more than 5 is high. The SDT considered an approach such as the one suggested. However, the SDT believes it would be very difficult to consider the various sizes of

entities in the approach. For example, a smaller entity may have only 1 or 2 devices to which R2 applies during a year. Therefore, using the logic that was suggested, failure to implement R2 for any device would result in a low or moderate VSL for that entity. The drafting team has decided not to adopt the approach suggested. The current VSLs are in keeping with the levels of VSLs which were previously approved by FERC for the corresponding requirements in previous versions, and the SDT believes they are appropriate.

(3) Level Prescribed for VRF's

Some industry comments indicated they believed a medium VRF for Requirement 1 was too high. The SDT reviewed the VRF assignment. The VRF of medium as assigned in CIP V5 is similar to the VRF that was assigned in previous approved versions of CIP. The requirement calls for an information protection program that includes methods for the identification of BES Cyber System information, procedures for handling the information, and a periodic assessment of the entity's adherence to its program with steps to correct deficiencies identified. CIP 011-5 does not apply to Low Impact BES Cyber Systems. The SDT believes that, given the importance of protecting BES Cyber System Information at the Medium and High Impact levels, the VRF of medium is reasonable. The VRF for R2 is lower as it is an administrative requirement and a violation would not, under any anticipated circumstances, lead to cascading, instability, or uncontrolled separation.

(4) Level Prescribed for VSLs

In some cases, the commenters indicated that the VSLs for CIP 011-5 R1 are too high and a few comments indicated that "perfection" was mandated in this requirement and the VSLs. The SDT reviewed the VSLs and does not agree with such comments.

The SDT believes that the need to have an information protection program, methods to identify the information to be protected, and handling procedures for BES Cyber System information are so basic that a VSL of Severe is appropriate if those things are not in place. The assessment of adherence is only required once per year, and a VSL of High seems appropriate to the SDT for failure to comply. The drafting team does not agree that this requirement or the corresponding VSL/VRF mandate perfection. The drafting team believes that the intent of the VSLs, which align with the previously approved VSLs for the corresponding requirements are appropriate and meet the NERC and FERC guidelines.

Some commenters indicated that the VSLs for CIP 011-5 R2 were too high and that a VSL of low or moderate would be appropriate. The currently approved VSLs for the previously posted requirement (CIP 007 R7) are comparable. To be rated as "lower" the noncompliant performance would have to have only a minor impact in meeting the reliability-related intent of the requirement. To be rated as "moderate" the noncompliant performance would have to meet a significant part of the reliability-related intent of the requirement. The SDT did add a "Moderate" VSL for the situation where the entity failed to maintain chain of custody but did not change other VSLs to Moderate as failure to prevent

unauthorized access or failure to destroy the media meet the criteria for a **Moderate VSL. Purpose of Guidelines**

Commenters requested that the material in the guidelines become part of the standard and that entities be allowed to reference such guidelines during audits. The SDT considered this issue. Guidelines are meant to provide context, examples, and illustrations to facilitate understanding for both the responsible entity and the compliance enforcement authority. With results-based standards, guidelines are attached to the associated standard and are posted with the standard as.

QUESTION 49 – Implementation Plan:
Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

SUMMARY:

There were several summary positions provided by commenters to this question in addition to those addressing the implementation plan. For the comments addressing the implementation plan, the primary issues or concerns expressed were: (1) the applicability to low impact BES Cyber Systems, (2) the 18 month time frame being too short, (3) general confusion about the version ¾/5 transition process and (4) initial performance of periodic performance requirements.

Applicability to Low Impact BES Cyber Systems:

Several commenters noted the significant effort necessary to implement requirements applying to Low Impact BES Cyber Systems. Many commenters did not feel the requirements should apply to Low Impact BES Cyber Systems at all. Several commenters also pointed out the proposed effective date of 18 months minimum cannot be achieved for low impact BES Cyber Systems.

All requirements previously posted in CIP-004-5 through CIP-011-1 applying to Low Impact BES Cyber Systems or All Responsible Entities have moved to CIP-003-5 and apply to All Responsible Entities. We have made this change in response to multiple comments to ensure these requirements have similar wording and measures.

Applying the said requirement in CIP-003-5 to all Responsible Entities recognizes the following characteristics about threats to cyber systems: (1) the imperfect nature of categorization, (2) the scale of magnitude in multi-site attacks and (3) the exploitation of trust relationships in lesser protected cyber systems.

First, the criteria in attachment 1 of CIP-002-5 provides improvement in the consistency of identifying and categorizing BES Cyber Systems, but it cannot account for the underlying complexity of the BES and its cyber systems. The criteria primarily account for larger cyber system targets of the BES at a point in time, but the risk to the BES is dynamic and

complex.

Second, the scale of magnitude for cyber-attacks is much more expansive than natural occurring hazards or physical threats. Cyber-attacks transcend the barriers of physical presence, which means a single attack may have no geographical limitations.

Finally, a cyber-attack can exploit trust relationships with lesser protected cyber systems, for example, through inter-utility data exchange. The target cyber systems identified through the Attachment 1 criteria have requirements applied in CIP-003 through CIP-011 that help prevent such exploitation, but the necessity of trusting the lesser-protected cyber systems introduces a risk that cannot be appropriately mitigated through internal controls alone.

The drafting team is unaware of any tools to model multi-site attacks and recognizes the complexity of doing so. Also, the drafting team is not implying an approach where everything must be protected at the same level. Instead, we propose an approach where each Responsible Entity has the foundational elements of a cyber-security program, which includes having a policy, increasing organizational awareness, implementing physical and electronic boundary controls, mitigating the use of default passwords and having an incident response capability.

This approach aligns with the NIST Risk Management Framework concept where all cyber systems have protection at some level and is responsive to the FERC Order 706 directive to consider applicable features of the NIST framework (paragraph 25).

> Order 706 Paragraph 25: The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

18 month Effective Date and Exceptions for Low Impact BES Cyber Systems:

We have extended the effective date in this posting to 24 months minimum based on feedback from a majority of commenters that 18 months was not sufficient. The purpose of having 18 months was to provide a reasonable path for bypassing version 4 of the CIP Cyber Security Standards, but the commenter feedback overall indicated more time for implementation in version 5 was more important than bypassing version 4.

We have also extended the effective date for requirements applying to those BES Cyber Systems not categorized as High or Medium to 36 months minimum. This reflects a risk-based approach to allow entities to focus on the high and medium impact BES Cyber Systems first and is responsive to the proportionally large number of low impact BES Cyber Systems for

an entity.

General Confusion about the Version ¾/5 Transition:

Many commenters expressed confusion and had questions about the transition from version 3 to version 4 to version 5. The majority of those commenting about this subject indicated the industry should not try to bypass version 4 as a tradeoff to approve version 5 faster. There were a few commenters who encouraged bypassing version 4.

In response, we recognize the unfortunate timing between version 4 and version 5. We also recognize the timeframes in the proposed implementation plan are contingent upon yet uncertain regulatory action. The commenter feedback overall indicated more time for implementation in version 5 was more important than bypassing version 4, and there should be a concerted effort with the compliance enforcement program to provide flexibility for entities to make the transition in a reasonable manner.

We have extended the effective date in revised Implementation Plan to a 24 months minimum. While this change will likely extend the effective date of version 5 beyond the effective date of version 4, we have left the option to bypass version 4 until the FERC issues a final order on version 4. These version 5 Standards address the additional directives from FERC Order 706 which version 4 did not address, and the SDT is attempting to address these in the most timely manner possible.

Initial performance of periodic performance requirements:

Commenters suggested the initial performance of periodic performance requirements should be addressed in the implementation plan rather than requiring the initial performance on or before the effective date throughout the Standards. In response, references to the initial performance in requirements having periodic performance obligations have been moved to the implementation plan and allow a 12 month time period for initial performance for most requirements. The quarterly review in CIP-004-5 R6 Part 6.4 allows a 3 month time period for initial performance, and the CIP Senior Manager approvals in CIP-002-5 R3 and CIP-003-5 R4 must be performed on or before the Effective Date.

QUESTION 50 – Other Comments:

SUMMARY:

In addition to responses submitted to the SDT for consideration through the use of the official comment form accompanying the formal comment period that ended on January 6, 2012, the SDT received some comments that accompanied a stakeholder's ballot or through email. In most cases, those comments were aggregated and included with the comment report for the question that most closely matched the issue. Others, as here, were consolidated into one

comment report. Even though the comment form did not ask a "Question 50," for organizational purposes, we have classified this report as "Question 50."

Several commenters provided alternative approaches, citing costs, complexity, or exceeding FERC Order 706 (e.g., not prescribing "low impact" standards). The SDT has reviewed carefully the directives in Order No. 706, and the alternatives suggested would not be responsive, collectively, to FERC Order No. 706. The team has approached the remaining directives in Order No. 706 by providing an impact-based framework that accounts for various levels of risk to the BES, and this approach balances experience in implementing Versions 1 through 3. The SDT must address all FERC directives in Order No. 706, and the SDT aims at being fully responsive to all directives. In particular, the SDT has responded to FERC's directive regarding consideration of the NIST framework.

Some pointed out that TOs do not have Control Centers. The SDT has modified the standard to remove TO Control Centers. However, TOs that have agreements with TOPs to perform some of the functional obligations by their Control Centers are in scope.

Some commenters were concerned with the possibility of a discrepancy with UVLS/UFLS systems and BES Cyber Asset. The SDT believes that there is no discrepancy between the definition of a BES Cyber Asset and UVLS/UFLS systems. The definition of the BES Cyber System includes a Cyber Asset, which excludes electro-mechanical relays by definition of a Cyber Asset. The SDT believes that Cyber Assets used in UFLS systems meet the modified definition of BES Cyber Assets in the updated draft.

Some comments suggested concern with the evidence retention requirements, which the SDT has modified and made consistent. There is a difference between the retention specified in a requirement and the retention specified in evidence. For example, if a requirement requires logs for the last 90 days, the entity is only required the logs for the last 90 days. However, the entity must retain evidence that the entity has kept 90 days of log during the audit period (such as a record of the execution of the log closing script). Compliance Section: The boiler plate Compliance section has been reviewed by the appropriate NERC staff.

Guidelines and Technical Basis: The compliance requirements of standards are provided in the requirements section. The Guidelines and Technical basis section only provide contextual information to the requirements.

"On or before the effective date": The language has been removed and the initial requirements have been defined in the Implementation Plan.

Concerns with the Applicability Section 4 (confusion over application to facilities or entities): The Applicability Section has been substantively rewritten to provide more clarity and addresses the comments.

Measures. Concern with “must v. may”: (See language in Summary Document of common issues) The language in the measures for main requirements state measures that “must” be provided. The measures in the parts of the main requirement use the language “may” as these measures provide examples of quality evidence to demonstrate compliance.

Use of Definitions in Background: The SDT has made changes where appropriate in both the background and definitions.

In response to concern over a proposed defined term, “BES Reliability Operating Services” has been removed as a definition used in the standard, but has instead been moved to the Guidelines and Technical Basis section as guidance for Responsible Entities in an initial scoping for applicable BES Cyber Assets.

Other commenters raised specific issues with specific standards that are addressed in the summary responses to those questions. In particular, however, the SDT notes that it has changed VSLs to better match the requirement language, considering where appropriate to gradate the VSLs. In other cases, the VSLs remain binary, as the SDT considered guidelines for VSLs from FERC and NERC to inform their analsyis.

In response to concern over the criteria used to categorize BES Cyber Systems, and a suggestion to use Version 4’s bright line, The SDT has made significant changes to the standards to address these comments. The SDT has used Version 4 criteria with modifications to address gaps identified after version 4.

In response to concern over different entities that share facilities, and how that affects compliance with CIP-004-5’s PRA requirements, and a suggestion that attestations be allowed, the SDT expects that the Responsible Entity owning the asset is responsible for compliance to the CIP standards and will be responsible for the requirement. In a shared access situation, this Responsible Entity is required to perform the Personnel Risk Assessment according to the specified requirement. In cases where the Responsible Entity does not have access to the specific details of the personnel risk assessment, as would be the case for contractors or employees of another entity, attestations may be acceptable. The obligations of the other entity also owning other facilities may include risk assessments for their personnel under this requirement if such access is to BES Cyber Systems they own in the shared facility.

Finally, the Smart Grid Interoperability Panel (SGIP)of the Cyber Security Working Group (CSWG) provided an extensive matrix mapping the Version 5 requirements to the high-level security requirements (HLRs) in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

This mapping identifies any gaps between CIP v5 and the NISTIR 7628 HLRs and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were

identified.

The SDT appreciates the extensive analysis done by the SGIP/CSWG and has considered the specific comments provided by the CSWG in other sections of the comment document.

The CIP Cyber Security Standards are enforced by a strict compliance regime where non-compliance is penalized, with substantive financial penalties in many cases. This is in contrast to the SGIP NISTIR standards which are currently provided as guidelines for use in implementation of SmartGrid systems. In contrast to SmartGrid systems, the systems to which CIP standards apply range from a large range of legacy systems with very basic cyber security capabilities to newer systems implemented in the Bulk Electric System which have more extensive cyber security control capabilities. Hence, especially in the Low Impact section, the large number of devices and the extremely diverse capabilities of these devices would unduly subject entities to non-compliance if a strict base of requirements were imposed, as modeled in the NISTIR and the NIST-800-53 control catalog.

In recognition of the diversity and capabilities of covered devices, and recognizing the strict compliance model currently in force for the NERC Reliability Standards, the SDT chose an adaptation of the NIST model that would be practical and implementable in that environment. In reviewing controls, the SDT, in its early development, considered both the NIST 800-53 control catalog, as well as the DHS Catalog of Control Systems Security, which are largely based on NIST 800-53.

The mapping provided by the CSWG completes the work done by the SDT, for which the SDT expresses its thanks for the large effort required. The subteams for the various standards have separately provided responses to the CSWG's comments in the consideration of comments for each standard.

Regarding comments on the application of the NIST framework, the CIP Cyber Security Standards are enforced by a strict compliance regime where non-compliance is penalized, with substantive financial penalties in many cases. This is in contrast to the NIST standards which are currently provided as guidelines for use in implementation of systems. The SDT chose an adaptation of the NIST model that would be practical and implementable in the CIP environment. In reviewing controls, the SDT, in its early development, considered both the NIST 800-53 control catalog, as well as the DHS Catalog of Control Systems Security, which are largely based on NIST 800-53.

In response to comments on consistency of terms and language, the Drafting Team has reviewed all definitions and the language of the standard and has made appropriate corrections where applicable, including the reinstatement of terms such as Electronic Security Perimeter and Physical Security Perimeter. The SDT has made many changes to the definitions of BES Cyber Asset and BES Cyber System and has now consistently used BES Cyber System in the applicability column of requirements. Proposed defined terms are in a separate Definitions document, and will be part of the NERC Glossary of

Terms when approved.

With respect to communication links between Electronic Security Perimeters, the inclusion of these communication links in the applicability would introduce Cyber Assets that the Responsible Entity does not own, operate, or have control over, and the drafting team has therefore not removed the exclusion.

Regarding comments on CIP Exceptional Circumstances, the standards do not allow the invocation of CIP Exceptional Circumstances for all requirements, only for those that are explicitly allowed. The SDT has allowed such invocation in cases where a temporary suspension of the requirement is necessary in certain circumstances to allow for first responders.

In the standards, when the term “Cyber Assets” is used without “BES”, this is intentional, as these may include Cyber Assets other than BES Cyber Assets (such as Electronic Access Control or Monitoring Systems, Physical Access Control Systems, etc.).

In the context of these standards, the term “security plan” includes any plan required by the standards (e.g. physical security plan, incident response plan, and recovery plan).

In response to comments on Procurement Policies, NERC Reliability Standards apply to users, operators, and owners of the Bulk Electric System. The policy requirements specified in R2 are necessarily limited to those in which specific NERC requirements exist and Responsible Entities are required to demonstrate implementation. Procurement policies would require an implementation that has certain requirements on entities not covered by NERC Reliability Standards (e.g. vendors and manufacturers).

Regarding resiliency, the SDT believes that the resiliency policy is covered by the policy for system recovery.

Regarding policies for third party and outsourced partners, these would be included in the responsible Entity’s obligations for those systems under the scope of the CIP standards.

The SDT believes that availability is implicitly covered by the requirements of the Recovery Plan, especially related to the conditions for the activation of the recovery plan.

Regarding Personnel Risk Assessment of third party and outsourced vendors, the standard requires that the Personnel Risk Assessment be performed for any personnel, including third party and outsourced vendors for applicable systems.

The policy for Interactive Remote Access is appropriately in the Security management section as a policy requirement.

Language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity’s policies and

controls is not explicitly required, but would be a component of the Interactive Remote Access policy.

Regarding responsibility for compliance in a shared access environment, the Responsible Entity owning the asset is responsible for compliance to the CIP standard. In a shared access situation, this Responsible Entity is required to perform the Personnel Risk Assessment according to the specified requirement. In cases where the Responsible Entity does not have access to the specific details of the personnel risk assessment, as would be the case for contractors or employees of another entity, attestations may be acceptable. The obligations of the other entity also owning other facilities may include risk assessments for their personnel under this requirement if such access is to BES Cyber Systems they own in the shared facility.

"Where technically feasible" is not considered as a loophole as currently implemented. The SDT understands that there are devices which have integrated dial-up access capabilities where strict compliance is not achievable. In those cases, the Responsible Entity may use the Technical Feasibility Exception (TFE) process under the NERC Rules of Procedure, Appendix 4D, which includes compensating and mitigating measures and an implementation schedule for remediation monitored by a Compliance Enforcement Authority. TFEs are only allowed where there is triggering language in the standard.

For Dial-up access, this is included in the definition of Interactive Remote Access, and therefore included in the requirements for Interactive Remote Access.

Regarding testing of physical security controls, the SDT discussed this requirement and agreed that a reduction of the testing from once every 3 years to once every 2 years is appropriate.

Regarding the Protection of BES Cyber System Information, the SDT has required identification of, access control to and processes for handling of BES Cyber System Information and has left it to the entity on the exact way in which they can meet the performance requirements.