NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form D
Definitions and Implementation Plans

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

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

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

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

Index to Questions, Comments, and Responses

The Industry Segments are:

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

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

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

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

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

2.	Group	Annabelle Lee	NESCOR/NESCO										

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

3.	Group	Jason Marshall	ACES Power Marketing						X				

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

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

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

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

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

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

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

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

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

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

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

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

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

9.	Group	Alan Johnson	NRG Companies					X	X			

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

10.	Group	Greg Rowland	Duke Energy	X		X		X	X			

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

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

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

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

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

13.	Group	Connie Lowe	Dominion	X		X		X	X				

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21.	Group	Rick Terrill	Luminant					X					

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

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

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

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

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

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

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

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

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

Questions with Summaries Included:

QUESTION D8 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified some of the definitions. 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

Several commenters stated that the definition of BES Cyber Asset was confusing, citing the complex construction of the definition and the fact that it stated that each BES Cyber Asset must be part of a BES Cyber System while the background and technical basis stated that Responsible Entities had flexibility in using BES Cyber Asset or BES Cyber Systems. Many provided alternative language. Multiple commenters asked whether there is a need for network connectivity between BES Cyber Assets to be considered a BES Cyber System. The SDT made the addition of the statement about each being part of at least one BES Cyber System to the definition of BES Cyber Asset to ensure that each Cyber Asset would be included in at least one BES Cyber System, and did not preclude the option of having a BES Cyber System that consists of a single BES Cyber Asset. The SDT believes this preserves entities' flexibility while providing better homogeneity in the application of requirements: requirements uniformly apply to BES Cyber Systems. There is no presumption of connectivity options in the definition of a BES Cyber System, but Responsible Entities may find that application of requirements and relationship with other definitions such as ESPs may be significant input to the Responsible Entities' options.

Several commenters suggested that the definition of BES Cyber Asset include an addition in its qualification for connection to a network within an ESP in addition to connection to a Cyber Asset within an ESP. The SDT believes that the clarification is useful in ensuring the application to those transient cyber assets that are connected to the network as well as directly to the Cyber Assets within an ESP and has made the modification to address the comment.

One commenter suggested modifications to definitions of Cyber Asset. The SDT considered these comments and does not believe that these suggestions are substantively different or would add clarity to the definitions.

One commenter suggested dropping the word "misused" from the definition of BES Cyber Asset. The SDT has specifically included the word "misuse" in response to comments from FERC Order 706 and believes that it includes intent of a malicious compromise that is not otherwise conveyed.

Mid-American's comment with respect to the use of the capitalized term "Systems" has been addressed and the definition now used the more generic term "systems" instead of the defined term.

One comment was on the use of the verb phrase "affect the reliable operation…" The SDT considered these comments and believes that this verb phrase is appropriate as it applies to the Facilities, systems and equipment, not the BES Cyber System.

Many commented on the complexity of the parenthetical sentence in the definition of BES Cyber Asset and suggested alternative language: the SDT considered these comments and believes that the suggested alternatives do not add additional clarity to the definition. In addition, other commenters stated that the parenthetical qualification should be used in defining the term Transient Cyber Asset. The SDT considered the options and chose to not have a separately defined term because of the very small number of requirements where it is used.

Many entities commented on the use of "adversely impact" in the definition of BES Cyber Asset and suggested using the defined term "Adverse Reliability Impact" instead. The SDT considered the use of the defined term and believes that the defined term describes an impact which is much more severe than the intent of the term used in the definition.

Several commenters requested clarification of the terms "within 15 minutes": the SDT has included additional clarification in the guidelines and technical basis section.

–One commenter suggested to remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. In response, 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.

Many entities commented on the qualification on “redundancy” in the definition of BES Cyber Asset. The SDT believes that the impact of a cyber asset on the function of a given Facility, system or equipment is independent on whether that Facility, system or equipment is redundant or not: in most cases, the redundancy is configured to handle loss of a Facility, but does not consider degradation or misuse of that Facility, system or equipment. The application guidelines and technical basis section contains a discussion of this concept.

One entity suggests that the definition of BES Cyber Asset is much improved still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. It is not the purpose of the definition to prescribe methods of documentation. That flexibility is left to the entity. Assets connected on a transient, temporary basis are not intended to be a BES Cyber Asset, and the 30 days in the definition is intended to clarify that temporary connections, e.g., for maintenance purposes, are not intended to be included within the definition.

BES Cyber Systems

One commenter suggested replacing “to perform” with “used to facilitate the performance of…”, citing examples where the BES Cyber System may not directly perform a reliability function, but may support one or more functions. The SDT believes that the introduction of the proposed language would result in further questions on the meaning of the word “facilitate” and the extent of the scope of that term.

In response to a suggestion to use the word “identified for functions…” the SDT believes that the suggested wording did not bring additional clarity to the definition of BES Cyber Systems.

One commenter stated that the use of the term “Responsible Entity” is confusing, citing overlap, redundancy or conflict with the term Functional Entity. The SDT believes that these are two distinctly different terms: the Responsible Entity refers to the set of Functional Entities that is responsible for compliance to the requirements of the standard. Within a given standard, a given set of requirements may apply to different Functional Entities, depending on the specific requirements. The term “responsible entity” is defined in the applicability section. The application of the defined term that contains the term “responsible entity” in a standard is subject to the preamble in Section 4.

Cyber Asset

Multiple comments were provided on the use of the word “programmable” in the definition of Cyber Asset, citing that it was too broad, and the need for a routable connectivity qualification. The SDT considered these comments and notes

that the definition of Cyber Asset as it pertains to “programmable electronic devices” is part of the current approved definition. The SDT further believes that consideration of connectivity in this generic definition is inappropriate.

One commenter stated that the qualification of “…data in these devices…” ignores data in motion. The SDT believes that the inclusion of data other than that in these devices has unintended consequences in the application of requirements.

Other

Multiple commenters suggested the addition of a defined term BES Site, or similar concepts: the SDT has considered the rationale and has opted to use the concepts in the drafting of new language and approach in the requirement language and attachments, instead of defining a term that would be used in only a few requirements.

One commenter requested that the language for the defined term Protected Cyber Asset be reviewed for clarity. The SDT has reviewed the definition and made modifications to the definition and added guidance in the background section to clarify the concept.

QUESTION D9 – DEFINITIONS:

Do you have any comments on the changes to the proposed definition of Control Center? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, 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.

Many commenters questioned the need for a definition of Control Center, citing standards in other reliability standards that also have control center applicability without the need for a formal definition. The SDT notes that the Control Center is subject to a number of High and Medium Impact criteria and that they host a large number of BES Cyber Systems that are essential to the reliable operation of the BES. The SDT believes that, because of these necessarily crucial functions, a formal definition is appropriate to clearly define the scope of applicability, as demonstrated by many questions on differentiation between a facility's control room, which is typically considered part of the facility, and Control Centers, which are considered separate facilities hosting operating personnel controlling and monitoring multiple facilities. Many commented that a formal definition used in the CIP context could be confusing to the industry in the context of other reliability standards that apply to control centers. The SDT believes that a formal definition clarifies the scope of applicability for Control Centers and would not affect other reliability standards that have not used the defined term, but rather a "common" undefined term for control center. NERC's standard use of capitalized terms for NERC Glossary defined terms provides clarity on when the defined term is used.

Two commenters proposed alternative language for the definition of the Control Center that uses Functional Entities. The SDT has considered the alternatives and believes that the proposals contain a circular reference that would not provide better clarity. The SDT has carefully considered the current proposed language and believes that it accurately describes the intended target of applicability.

Others suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that

trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

Multiple commenters expressed concern that in certain instances, a facility may not be performing the function of a TOP 24/7 and remains unmanned the rest of the time, and suggested the addition of the 24/7 qualification. The SDT sees no rationale in adding this qualifier, since the impact of the facility that performs these functions remains the same. In the same comment, commenters cited the case of a TOP registration for a single facility. The SDT responds that the "control and monitoring" facility of a single facility does not meet the definition of a Control Center, but rather as part of the facility it is controlling.

Several commenters suggested slightly modified language which focuses on hosted BES Cyber Systems rather than operating personnel. One commenter suggested that the Control Center is the BES Cyber System that performs these functions. The SDT believes that operating personnel is central to the traditional understanding of a Control Center facility. The definition currently specifies one or several facilities. In the facilities (or site) based approach, the identification of the BES Cyber Systems that perform the Control Center functions may bring in other facilities such as data centers that perform these functions.

Many commenters requested clarifications on the terms "facility" and "locations" used in the definition of the Control Center. The SDT uses the general term "facility" (as opposed to the glossary term "Facility") in its generic sense of one or several physical structures that comprise a Transmission substation or station, a generating plant or a Control Center. In the case of a Control Center, a facility could be considered a building or campus consisting of several closely located buildings. However, additional facilities may be brought in as the BES Cyber Systems are defined, including associated data centers that perform the reliability tasks. In the context of the definition of Control Center, a location generally refers to the set of BES Facilities at a single site, and generally constitutes a single point of connection to the BES. Because of the many types of configurations, the SDT used the generally accepted concept of geographic location rather than including all the nuances of the different ways Facilities are connected to the BES.

One commenter requested a definition for data center. The SDT believes that "data center" is a well understood term and that many definitions of data center exist elsewhere that adequately explain what they are.

One commenter pointed out that the SDT uses the term reliability functional tasks and reliability tasks interchangeably in the standard. The SDT has used the terms interchangeably for the reliability tasks defined in the NERC functional model. The SDT has made the change in the definition of Control Center to be consistent to the use of reliability tasks elsewhere.

One commenter requested further qualification of the term “operating personnel”. The SDT notes that this term is used in many reliability standards, in particular, the PER series of standards. They are used to refer to personnel that perform the real-time control and monitoring operations necessary for the real-time functions for RC, BA, TOP and GOP functional entities. The definition of the Control Center refers to these functions.

One commenter suggested the addition of “NERC Certified” to operating personnel. The SDT notes that the addition of the term NERC Certified restricts the applicability of the term to just RCs, BAs and TOPs, since there is no requirement for certification of GOP operating personnel. This is not the intent of the SDT in drafting this definition.

One commenter suggested that Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations, and that this single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. The commenter suggested that a capacity qualifier be added to this definition. The SDT does not think that the threshold should be in the definition, but has amended the criterion for generation Control Centers in the Medium Impact category that addresses this comment. BES Cyber Systems for Control Centers below the Medium Impact threshold must still be protected as Low Impact. See the response to A03 - Attachment 1, Medium Impact.

QUESTION D10 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the comments related to these definitions largely noted minor improvements to the definitions rather than identifying major issues or disagreement.

BES Cyber System Information
Several comments about the definition of BES Cyber System Information highlighted minor issues with the structure of the definition rather than its content. Commenters suggested re-organizing the definition such that the list of examples came last. The SDT considered this comment and agreed that it made the definition more readable without changing its overall intent. This suggestion has the effect of collecting the explanatory language together to improve comprehension of the definition. Some commenters suggested that the examples should be removed from the definition altogether. The SDT noted that it is not uncommon to find examples in definitions in the NERC Glossary of Terms Used in NERC Reliability Standards (e.g. Facility, Operating Plan, Year One, etc.). Additionally, the SDT had concerns about removing the list of examples, since a similar list of examples has been used since the version 1 CIP Standard to provide direction as to what information should be included in the NERC CIP information protection program. The SDT believed that continuing to provide a list of examples would facilitate a transition between Version 3 and 4 of the CIP standards to Version 5.

Additionally, some commenters took issue with the phrase "developed by the Responsible Entity" as it relates to security procedures and security information. The commenters noted that protection of security information might be appropriate even if this information was developed by an outside party. The SDT agrees with this comment. The intent of the SDT was to prevent the inclusion of information that might be publicly available. Therefore, the SDT has modified the definition to better align with the intent and has clarified that security procedures and security information "not publicly available" are examples of BES Cyber System Information.

Some commenters noted ambiguity in the definition of BES Cyber System Information in the phrase "unauthorized distribution" of information. The SDT appreciates the concern over ambiguity, but encourages the industry to consider this definition in context of the overall information security program that is required under NERC CIP-011-1 and related

requirements in NERC CIP-004-5. Consideration of "unauthorized distribution" should be taken in the context that access to locations where information that has been judged to meet this definition is stored is required to be authorized in CIP-004-5 R4, part 4.1, element 4.1.3 and proper handling of this information is required in CIP-011-1 R1, part 1.2. The Responsible Entity should use this context to determine whether this information, in the hands of someone who has not been granted access "based on need," could lead to a compromise in security, directly or indirectly, of the BES Cyber System.

Other commenters noted ambiguity over the phrase "pose a security threat" and recommended that this phrase be removed. The concept of posing a "security threat" to the BES Cyber System should also be considered in context of the requirements of the NERC CIP Standards, particularly CIP-011-1 R1. BES Cyber System Information is intended to be identified and protected in accordance with an overall information protection program. As such, it is anticipated that the Responsible Entity will include some process to identify the information applicable to this program. As not all information will lead to directly gaining access to BES Cyber Systems but may in other ways compromise the overall security of the BES Cyber System, the SDT does feel that it is prudent to remove this phrase.

CIP Exceptional Circumstances

Several commenters identified an issue with the phrase in the definition of CIP Exceptional Circumstances that included "an imminent or existing hardware, software, or equipment failure." Commenters pointed out that the collection of forensic data in CIP-009-5 Requirement R1.5, draft 2 was subject to CIP Exceptional Circumstances. Through the inclusion of hardware, software, or equipment failure as a CIP Exceptional Circumstance, a Responsible Entity could essentially choose to never comply with the collection of forensic data. After consideration, the SDT chose to modify the requirement in CIP-009-5 R1.5 to indicate that data preservation should not impede or restrict recovery. The SDT believes that hardware, software, or equipment failure is a reasonable component to include as a CIP Exceptional Circumstance given the cyber-physical relationship of the electric grid and its supporting Cyber Assets.

Additionally, commenters noted that the involvement of the conditions identified in the definition of CIP Exceptional Circumstances is not always known ahead of time. Specifically, commenters suggested that the SDT add the phrase "threatens to involve." The SDT considered this suggestion and decided that given the supporting framework required through the cyber security policies in CIP-003-5 to invoke a CIP Exceptional Circumstance, this was a reasonable and beneficial modification to the definition.

Commenters also questioned when CIP Exceptional Circumstances can be invoked. No modification was made to the standard, but in response, the intent of the SDT is to allow the use of CIP Exceptional Circumstances only where specifically identified in the language of the requirement. Additionally, CIP Exceptional Circumstances should be declared using the provisions identified in the Responsible Entity's cyber security policy as per CIP-003-5 R1.

CIP Senior Manager

Numerous commenters suggested minor modifications to the definition of CIP Senior Manager. The intent of the SDT was to include a definition of CIP Senior Manager in the NERC Glossary of Terms Used in NERC Reliability Standards so as to make clear who the required approver is when the term is used across the body of CIP Standards. The SDT did not intend to modify the content of the definition, which has remained unchanged since version 2 of CIP-003-2 when the role of the senior manager was clarified in response to FERC Order 706, paragraph 381. The SDT was compelled, given the current state of the CIP Standards being in their 5th version, by comments that suggested that in addition to the authority and responsibility for leading and managing the implementation of the requirements, that the CIP Senior Manager should also have the overall authority and responsibility for leading and managing "continuing adherence" to the requirements within the NERC CIP standards.

The SDT also received comments that the definition of CIP Senior Manager should specifically call out CIP-002 through CIP-011 as this is the set of cyber security standards to which the CIP Senior Manager has the authority and responsibility for. The SDT received similar comments in response to draft 1 of the posting of this definition. At that time, the SDT responded that the definition was only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which at the time was planned for retirement as part of project 2009-1. However, given the dynamic nature of project 2009-1 and the relative ease to which this definition could be modified in the future should additional standards be added to which the CIP Senior Manager authority should apply, the SDT is persuaded to include a reference specifically to "CIP-002 through CIP-011" in the definition of CIP Senior Manager.

QUESTION D11 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the SDT has address all comments and has made clarifying changes to the definitions.

Physical Security Perimeter (PSP)
One commenter proposed modifying the definition to apply only for applicable BES Cyber Systems. However, applicability cannot be determined by a definition. We have clarified in the applicability column in standards CIP-004 through CIP-011 that PSPs are not applicable solely upon meeting the definition.

One commenter requested that a list of example Cyber Assets that should be included within a PSP. In response, the standards specify more clearly which Cyber Assets must reside in a PSP.

One commenter suggested the definition of PSP should reference the correct defined term: Electronic Access Control or Monitoring Systems, and the SDT has made this change.

One commenter suggested that the definition is ambiguous about (1) whether the perimeter is two or three dimensional, (2) whether there are different expectations for High and Medium BES Cyber Systems and (3) what size hole provides access. In response, the additional specificity for the perimeter and access points would limit the options entities have in applying the requirement. The SDT believes we have struck the right balance in this requirement to allow entities flexibility in their approach while describing the end result. In regard to the difference between physical protection in High and Medium Impact BES Cyber Systems, this is specified in CIP-006-5.

Physical Access Control System (PACS)
Several commenters proposed removing "alert" from the definition to avoid the interpretation that security guard workstations are included in scope. In response, the alerting component should include the system sending out the alert

and does not include all recipient persons or devices of the alert. We do not believe this needs further clarification in the definition.

One commenter suggested that examples should not be included in the definition and the wording “exclusive of devices…at the PSP” could exclude more asset than intended. In response, we note that examples should not change the definition but can be helpful in forming context. For PACS, these examples are useful for explicitly clarifying perimeter devices, which by nature cannot have the same physical protection are outside of scope.

One commenter suggested putting a comma to make clear the example applies to Cyber Assets. In response, the example does modify the locally mounted hardware and devices and not the Cyber Assets. In other words, the example is for the exclusion.

One commenter suggested that the SDT needs to ensure electronic visitor log books are not captured in the definition and that the exclusion uses “or” instead of “and” for the examples. In response, a visitor log book would not be within scope because it logs visitors and not access, and including an electronic visitor log book could cause the interpretation that any additional logging would be considered out of scope. Also, “or” and “and” are logically interchangeable in the example list, and we do not find a need to make any change.

One commenter suggested that monitoring Cyber Assets should be included in the definition. In response, we did not include monitoring devices because those are typically outside of the PSP and serve as a supplementary protection. Although these can be used to comply with monitoring requirements, it becomes problematic to apply additional CIP Standards requirements without creating a complex protection loop.

One commenter suggested changing the word “exclusive” to “excluding”, but the SDT chooses to retain the originally posted wording.

One commenter suggested the definition should include workstations used to provision physical access and monitor alarms. In response, the proposal would expand the definition scope beyond what the SDT considers unacceptable risk. The level of effort required to protect this significant population of assets would far exceed the security benefit of doing so. As an example, this could include all cell phones and pagers carried by staff for responding to alarms.

QUESTION D12 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, clarifying language was added to each definition to highlight stakeholders concerns.

Interactive Remote Access
Several commenters requested clarification for the inclusion of dial-up access in the definition. Upon further review, this has been removed from the definition. The important part to note is that Interactive Remote Access is when using a remote access client or other remote access technology, regardless of the type of connectivity.

One commenter proposed that the definition of Interactive Remote Access be modified to exclude serially connected, non-routable, non-network connected devices. The definition did not include serially connected, non-routable, non-network connected devices. However, the definition has been modified to specifically address the use of a routable protocol.

Several commenters requested restructuring of the definition to highlight the criteria for identifying Interactive Remote Access. The definition has been updated as requested to highlight that the first criteria is the use of a remote access client or other remote access technology.

Several commenters requested more information regarding examples of a remote access client or remote access technology. Additional information is available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that list item two, "Cyber Assets used or owned by employees" be modified as "Cyber Assets used by employees". The commenter considers employee-owned devices inappropriate for use in Interactive Remote Access. Employee-owned devices were added to the definition based on comments received in Project 2010-15:

Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

One commenter recommended adding the words “owned by or under the control of the Responsible Entity” to prevent the inclusion of equipment owned by Managed Security Providers in the standards. Connections by vendors, contractors, and consultants should be protected to the same standard as assets owned by the entity. Assets owned or used by vendors, contractors, and consultants were added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

Multiple commenters noted that the sentence beginning with “Remote access may be initiated from ...” adds no value, does not address all circumstances, and should be deleted. They further noted it is possible to initiate remote access from assets owned by others not listed. The information was added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. Please see the opposing perspective noted by other entities. The definition states that access “may be initiated” and not “shall be initiated” to allow for flexibility and not define the three scenarios as the finite and final list.

Intermediate Device

One commenter was concerned with the phrase “performing access control” existing as part of the definition of an Intermediate Device. It is the SDTs intent that an Intermediate Device is classified as an Electronic Access Control or Monitoring System. The definition of Electronic Access Controls or Monitoring Systems has been modified to include Intermediate Device.

One commenter requested clarification as to the types of devices that could be used as an Intermediate Device. The SDT specifically did not list proxy or other technology to allow flexibility in how an entity may implement a solution that best meets their needs. Per CIP-005-5 Requirement R2.1, the Intermediate Device must be used before accessing a BES Cyber System or Protected Cyber Asset. Per the definition, the Intermediate Device must not be inside of an ESP. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Multiple commenters noted concerns with the language, “The Intermediate Device must not be located inside the Electronic Security Perimeter”. Comments were received that this should be added to the requirements and removed from the definition. Some consider the second sentence of the definition to be unnecessary, too prescriptive, and should be deleted. Some offered recommendations for changes to the definition to allow for future technology developments.

- The SDT considers this language to be defining and clarification of the device. The performance under the requirement is that an entity utilizes the intermediate device. Further, definitions are part of the standards and carry the same force as the requirements.
- The location of the Intermediate Device was included in the definition to address numerous industry questions on this matter both in Project 2008-06 Cyber Security Order 706 Version 5 CIP standards and Project 2010-15: Expedited Revisions to CIP-005-3. Many entities have raised questions regarding the location of the device based on termination point of encryption and other issues.
- The only restriction placed on the Intermediate Device is that it not be inside of an ESP. Access authentication should be performed before the user is granted access through the ESP. Encryption should be terminated outside of the Electronic Security Perimeter so that event logging within the ESP is not negatively impacted. The SDT specifically did not list other specifics to allow flexibility in how an entity may implement a solution that best meets their needs whether through the use of a multi-purpose device or other architecture. Additional references regarding the Intermediate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter noted concerns that the term "device" is not clear in defining the Intermediate Device. They recommend using the term “Intermediate Cyber Asset”. The definition includes the term “Cyber Asset” which is defined as “programmable electronic devices including the hardware, software, and data in those devices”. The SDT has chosen the unique term “Intermediate Device” to allow for the use of one or more Cyber Assets making up the device.

QUESTION D13 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the SDT clarified language to the definitions.

Electronic Access Point
Multiple commenters asked for clarity if an Electronic Access Point (EAP) must be routable on both sides. In response, the SDT's intent is that if the device is accessible from outside the Electronic Security Perimeter (ESP) with a routable protocol then an EAP must be put in place. Therefore, just as in the Critical Cyber Asset Identification Guidelines of today, the 'inside' does not have to be routable. For example, if the entity has a digital relay and has the serial port used for console access (non-routable serial communications) attached to a serial-to-IP gateway such that the relay's command console is addressable from outside the ESP via a routable protocol (e.g. <IP Address>:<Port #> will connect you to the relay), then this meets the definition of External Routable Connectivity and an EAP is required.

One commenter provided an alternate definition that included the phrase "externally routable bi-directional communication" and added "or inbound communications to a Cyber Asset within the Electronic Security Perimeter" to the end. In response, the SDT notes that the direction of the communication is an aspect of External Routable Connectivity definition. The Electronic Access Point is an intentionally broader definition and its main function is to deny all access by default and only allow needed traffic to cross the ESP, regardless of direction.

One commenter asked that it be clarified as to whether an EAP is part of the ESP or not? In response, the SDT notes that an EAP is part of an ESP as it is the point where the routable communication from outside the ESP is allowed to cross the ESP to Cyber Assets inside the ESP.

One commenter suggested that the term "interface" be removed and have the definition reference a Cyber Asset. In response, the SDT notes that the inclusion of interface is meant to address the situation where an entity has a firewall as an EAP that has numerous interfaces to different networks and only one goes to a network that has applicable Cyber

Assets. The inclusion of 'interface' means the requirements would be concerned with only those interfaces that communicate with applicable Cyber Assets and not to interfaces that do not have any applicable Cyber Assets. The SDT also notes that the requirements in CIP-005 that apply directly to EAPs concern an interface (deny by default, methods for inspecting for malicious communications, etc).

One commenter suggested that the definition add "allows or is capable of allowing" to include dual homed Cyber Assets including laptops with wifi that is not hardware disabled. In response, the SDT believes that for a mandatory requirement the enforceable point should be binary – either communication is allowed to cross an ESP or it isn't – and the standards should avoid dealing with all possible capabilities.

One commenter asked for confirmation of the notion that Cyber Assets only communicate with other Cyber Assets. In response, the SDT notes that Cyber Asset is the basic unit of these standards and there is no lower level term. As Cyber Asset is a 'programmable electronic device', the SDT believes this covers most all situations. The SDT notes that Cyber Assets includes most all network gear as well, not just servers and workstations.

Electronic Security Perimeter

Several commenters suggested that examples should be included. In response, the SDT is not including examples in this term. Since terms such as ESP often refer to cyber technology that is constantly changing and developing, there is a tendency for examples to become outdated. The SDT used guidance instead to discuss examples rather than definitions. When the term is then used in a requirement, there is a tendency for the examples to then become prescriptive and mandatory, which is not the purpose of examples.

Multiple commenters provided some clarifying questions: Does an ESP presume the presence of EAP? Does a BES Cyber System with no External Routable Connectivity fall into scope? In response, the SDT clarifies that the ESP does not presume the presence of an EAP and BES Cyber Systems without External Routable Connectivity are in scope of the CIP standards. The ESP is a 'logical border' around a routable protocol network to which a BES Cyber System is connected. An isolated network with no external connectivity has an ESP; a logical border. The ESP is used to determine the 'Associated Protected Cyber Assets' as well as the collection of Cyber Systems and Assets that will be elevated to the impact level of the highest impact BES Cyber System/Asset in the ESP (see the definition of Protected Cyber Asset). If routable protocol communications cross the ESP, then an EAP is required.

Several commenters stated that this should be applicable to BES Cyber Asset instead of BES Cyber System. In response, the SDT notes that the BES Cyber System grouping is up to the entity and the concepts of electronic and physical security perimeters need to be taken into account. An entity is free to define every individual BES Cyber Asset as its own unique BES Cyber System and in essence make the entire standard Cyber Asset based. The grouping into systems is at the entity's discretion, but should be done with the requirements in mind.

External Routable Connectivity

Multiple commenters suggested that clarity is needed concerning the focus on Cyber Asset connectivity, rather than a 'system' with connectivity. Does a 'system' with one routable device mean all cyber assets in the system meet the applicability? This applies to the ESP definition as well. In response, the SDT has updated the definition to be at the Cyber Asset level rather than the BES Cyber System level. The intent is that Cyber Assets that have External Routable Connectivity must meet the applicable requirements and Cyber Assets that do not meet the definition are exempt from the requirement.

Several commenters suggested that the definition should include the OSI network layers. The SDT has chosen to not include Open System Interconnection (OSI) layers in the definition at this point. It is believed that with the history of the CIP standards being based on 'routable protocol' since its inception that there is a sufficient understanding of these terms at this point.

Multiple commenters suggested that the definition should be reworded to be a property of a BES Cyber Asset, not the asset itself. In response, the SDT agrees and has changed the definition to begin with "The ability to access…"

One commenter suggested that the definition should only apply if routable connection goes all the way to a BES Cyber Asset within the ESP. In response, the SDT is trying to incorporate the situation (identified in the current CCA Identification Guidelines) where an Ethernet/serial gateway is used at the perimeter. A BES Cyber Asset may have a serial connection from its console port to the Ethernet/serial gateway such that from outside the ESP the device's console port is directly addressable using a routable protocol, usually simply in the form of <ip address:port #>. The SDT's intent is for the definition to capture any device that is accessible from outside the ESP with a bi-directional routable protocol.

One commenter suggested that the definition needs to consider inside to outside connectivity not just outside in. In response, the SDT does consider 'inside out' connectivity in the requirements (e.g. outbound rules on EAP's). However, the intent with this definition is to focus on the higher level of threat that outside-in connectivity presents as well as to

give some credit for more secure network architectures that only push data out and don't allow outside-in connectivity (data diodes, etc.).

A few commenters commented that the definition should be Cyber Asset based rather than strictly limited to BES Cyber Systems. In response, the SDT has clarified that access is from a Cyber Asset that is outside of the BES Cyber System's associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Protected Cyber Asset

Multiple commenters suggested that the parentheses should be removed, keeping the sentence concerning temporarily connected Cyber Assets. In response, the SDT agrees and has made the suggested change.

One commenter suggested that the temporarily connected Cyber Asset exclusion should be pulled out and made into a separate definition. In response, the SDT in this instance would be defining a term simply to use the term in the definition of another term. Therefore the SDT believes it is more straightforward to include a more complete definition in the ultimate term we are defining, and see no issue with stating what something is and what it is not while defining it.

Multiple commenters suggested that this should allow for network connection of temporarily connected Cyber Assets, suggesting that 'directly' be removed to allow connection within the ESP without requiring connection through a Cyber Asset. In response, the SDT notes that a network switch is a Cyber Asset and thus network connections are included. However, the SDT agrees that this point needs more clarity and has deleted the word 'directly' and clarified that it is a connection either to a Cyber Asset in the ESP or the network within an ESP.

One commenter suggested that a separate definition for Transient Cyber Asset should be included and have a requirement to scan for malware before connection. In response, the SDT notes that this was included in previous drafts but was removed in this draft in response to comments. Numerous comments were received pointing out the audit issues of such a requirement. How does one prove that a list of temporarily connected devices is complete? How does one prove that virus scans were done on a device that was there one minute and gone the next? How does one maintain and prove a complete inventory of all temporarily connected devices? Commenters also pointed out that the object of protection is the BES Cyber System – the goal is to protect BES Cyber Systems from all threats including temporarily connected devices. There were also numerous issues raised concerning TFE's as many troubleshooting and maintenance devices are 'programmable electronic devices' and would thus be Cyber Assets but have no antivirus available. A cable scanner used to diagnose cabling issues may be a programmable electronic device and then require a TFE. In response to

all these issues, the SDT decided to remove the requirement. However, the SDT notes that CIP-007 R3 requires an entity to deploy method(s) to deter, detect, or prevent malicious code and it is expected that such measures as scanning temporarily connected laptops and other similar devices may be included in these methods.

QUESTION D14 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, several changes have been made to clarify language in the definitions.

General Comments
Several commenters stated that the phrase "reliability tasks of the functional entity" is unclear and needs to be replaced or further defined. In response, the phrase reliability tasks of the functional entity comes from the definition of BES Cyber System and the reliability tasks are those specified in the NERC Functional Model.

Several commenters suggested that the terms compromise and disrupt need to have their own definition. In response, the words compromise and disrupt carry forward from the previously approved definition and we have not received compelling indication that these terms need further clarification.

Several commenters suggested that the phrase "was an attempt to compromise" is vague and should be deleted. In response, this phrase captures those incidents that do not necessarily succeed but should prompt investigation.

One commenter suggested replacing the phrase "reliability tasks of the functional entity" with "reliability tasks identified for functions in the NERC Functional Model." The SDT does not specify the NERC Functional Model, which is not a document subject to the standards development process, but the SDT believes that the phrase adequately conveys those tasks.

One comment was on the phrase "malicious and suspicious" is subject to interpretation and proposed adding the qualifying phrase, "as determined by the Responsible Entity." In response, the definition should not include this phrase because it is not a requirement, and CIP-008-5 already specifies the obligation for the Responsible Entity to make this determination.

One commenter suggested qualifying the term ESP and PSP with BES Cyber System to avoid having to demonstrate compliance with perimeters that do not protect BES Cyber Systems. In response, the requirement in CIP-008-5 makes this distinction in the applicability section.

One commenter suggested that the definition of Control Center uses a different term "reliability functional tasks" and requests clarification if this term means something different. In response, the SDT has clarified the language to read "reliability tasks".

One commenter suggested that the DOE OE-417 form should be considered to allow entities to comply with both requirements. In response, the SDT has reviewed the latest version of this form and do not find any reporting requirements that would conflict with those in CIP-008-5.

Cyber Security Incident

Several commenters suggested replacing the phrase "was an attempt" with "has the potential" in the definition of Cyber Security Incident because an attempt implies knowing the intent of the perpetrator and it excludes accidents which have the potential to compromise the BES Cyber System. In response, we have not significantly changed the currently approved definition and do not find the need to incorporate the proposed modifications. Both phrases communicate the desired result that an unsuccessful attack or compromise would be considered a Cyber Security Incident.

There was a suggestion that the definition of Cyber Security Incident now includes PSPs and the impact will be difficult to assess. In response, the current approved definition includes PSPs.

One commenter proposed to amend the definition of Cyber Security Incident to include: "Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered ESPs or PSPs." In response, violation of policies can be covered in an entity definition of a cyber security incident, but the Glossary definition has a focus on impact in order to broadly apply the standard.

One commenter suggested that physical security incidents should have its own definition and not be included as part of a Cyber Security Incident. In response, a physical security breach into a perimeter protecting the BES Cyber System provides enough cause for concern in the integrity of the BES Cyber System to warrant classification of a Cyber Security Incident. Individual entities may use distinct terms and response teams for these types of incidents, and the obligations in CIP-008-5 would still apply.

Several commenters proposed removing the phrase “suspicious event” from Cyber Security Incident. In response, the term suspicious event captures those incidents prompting further investigation in which the entity may not determine the cause or motive.

Reportable Cyber Security Incident

SPP RE expressed concerns that Reportable Cyber Security Incidents would not include those incidents in which redundancy mitigated the impact. In response, we have provided guidance in CIP-008-5 that Reportable Cyber Security Incidents would also include those that triggered an activation of redundant systems.

There was a proposal to replace “Any” with “A” to start the definition of Reportable Cyber Security Incident and we have done so.

One commenter proposed the following definition of Reportable Cyber Security Incident: “Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC.” In response, this proposed definition includes a requirement, which should remain in the standard. The requirement in CIP-008-5 still provides leeway to the entity in determining Reportable Cyber Security Incidents.

One commenter stated that the definition needs to be coordinated with the EOP-004-2 drafting team. In response, both the CIP Version 5 and EOP-004-2 drafting teams have agreed to move all reporting obligations for Cyber Security Incidents to CIP-008-5.

One commenter proposed the definition for Reportable Cyber Security Incident in order to avoid using the term functional tasks, “A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site.”

One commenter proposed to add additional guidance in CIP-008-5. In response, the use of functional tasks ties the reportable incident to a specific reliability function. Without this qualification, the definition can easily be interpreted to include nominal security events as reportable. The SDT has already added additional guidance on distinguishing a Reportable Cyber Security Incident.

QUESTION D16 – IMPLEMENTATION PLAN:

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

SUMMARY:

Based on stakeholder comments, there were not many changes made to the Implementation Plan, but the comments and comment responses below provide clarity into some of the concerns regarding the proposed effective date, the possibility of bypassing Version 4, and the initial performance of certain periodic requirements.

Proposed Effective Date

One commenter suggested that the effective date conflicts with the initial performance of requirements section and should specifically mention this in the effective date language as an exception. In response, we do not feel this is necessary. The implementation plan enumerates any exceptions to the effective date of the standard. The alternative of including all such exceptions in the effective date language would make the language unreasonably complex.

One commenter agreed with the approach to focus on the high and medium impact BES Cyber Systems but questions the need for an additional year of implementation time for low impact BES Cyber Systems particularly if no inventory is necessary. SPP RE also agrees an additional year for compliance with CIP-003-5 R2 is unnecessary. In response, the need for an additional year of implementation for low impact BES Cyber Systems exists to allow entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists.

Several commenters questioned why the effective date is so far out given that the standards have been in development for more than two years. In response, the development timeframe of the standards do not determine when entities begin planning compliance. Rather, entities have assurance in the finality of the standards upon FERC approval. The number of cyber systems applicable in this standard far exceeds any previous version of the standard. The SDT reasons it will take two budget cycles for entities to plan and implement these standards.

Bypassing Version 4

Several commented that language to extend the Version 3 effective period and bypass Version 4 should be removed because the recent FERC Order has solidified the effective date for Version 4 as April 1, 2014. Other comments request a

transitional plan to address the period of compliance between Version 4 and 5. In response, the SDT observes that the provisions to bypass Version 4 remain in the implementation plan and are subject to approval by the industry and FERC. This is explained in greater detail in the summary section at the beginning of this document.

Initial Performance of Certain Periodic Requirements

One commenter stated that for non-periodic requirements, the IP should state entities comply with all other requirements on the effective date. In response, this is already stated in the effective date language. The periodic requirements are exceptions to this language.

Several commented that CIP-010-1 requirement part 3.2 and CIP-009-5 requirement part 2.3 have a 36 month periodic performance requirement and should have an initial performance not exceeding 36 months after the effective date. Yet, although the periodicity for this requirement is 36 months, the initial performance should occur closer to the effective date of the standard. However, we are persuaded by arguments that initial exercises should be conducted prior to the operational exercise active vulnerability assessment.

Several commented that the language "…Notwithstanding any order to the contrary…" is unnecessary because the FERC can approve or remand any part of the implementation plan if it so chooses. While this is true, the inclusion of this language allows that decision to be made without the tremendous overhead of going through the standards development process.

One commenter argued that the periodic requirements section requires compliance as early as 14 days after the effective date, but the effective date allows 24 months. In response, this is true, and all of the specified periodic performance requirements occur after the effective date, which is at least 24 months.

One commenter argued the initial performance of the requirement should be performed prior to the effective date. They questioned why a year would be necessary to hold the first training or verify provisioned access. In response, the SDT disagrees with compliance prior to the effective date for two reasons. First, the effective date of the standard indicates when Version 5 becomes effective and previous versions retire. Requirements that obligate performance on a specific day cannot technically be compliant prior to the effective date. Second, the specified periodic requirements are mostly verification assessments or updates for existing security controls, and the objective is to have the security controls in place upon the effective date.

Based on comments received, CIP-009-5 requirement part 2.3 has been added to the list of periodic requirements that must be implemented no later than 12 months after the effective date.

One commenter noted that CIP-009-5 Requirement R1.4 still contains language requiring an initial performance. However, the intent of this requirement was not to obligate an initial periodic performance, and we have modified the requirement language to remove the word "initial".

Planned or Unplanned Changes

Several commenters suggested all new or reclassified Cyber Systems have the same timeframe of 12 months to achieve compliance. In response, we have updated the implementation plan based on changes to CIP-002-5 that remove obligations to update the BES Cyber System categorization within 60 days. This provides entities additional time to demonstrate full compliance for planned changes. Unplanned changes resulting in a higher categorization continue to allow the additional year to demonstrate full compliance for the affected BES Cyber Systems.

The Planned or Unplanned Changes section was collapsed into one section based on multiple comments, and it has been clarified that for *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, with additional time to comply for requirements as specified and in the same manner as in the section *Initial Performance of Certain Periodic Requirements*. For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to timelines specified in a separate table, following the identification and categorization of the affected BES Cyber System, with the additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Time Periods for Disaster Recovery

Several commenters requested clarity on what constitutes the completion of the Disaster Recovery. In response, the use of the defined term CIP Exceptional Circumstance throughout the CIP Cyber Security Standards eliminates the need to define a special case in the implementation plan for Disaster Recovery. Entities can take exceptions from the Requirements where CIP Exceptional Circumstances is specified.

One commenter suggested that the Disaster Recovery section seems to suggest not holding up restoration for compliance but entities would need to be compliant when restoration activities are complete. In response, this section

has been removed and we defer to the use of CIP Exceptional Circumstances throughout the CIP Cyber Security Standards to provide entities clarity on when and where exceptions to the Requirements can occur.

Applicability Reference Tables

One commenter requested additional clarification regarding the purpose of the applicability tables and others noted inconsistencies with the table. In response, we have corrected inconsistency errors, changed the title and provided introductory remarks. These tables are intended only for convenience. The SDT chose not to include this in a background or guidance section because requirement numbering will change in future revisions.

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN:

If you have comments or specific suggestions that you have not been able to provide in response to the previous questions, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the implementation plan was modified appropriately and certain areas were modified for clarity. Entities should refer to the individual responses to comments in the definitions questions for the SDT's response to comments for individual definitions. Many commenters provided comments on the positive direction of the posted draft. The SDT thanks these commenters and appreciates the encouraging remarks.

Several comments were toward the approach to requirements that result in a zero tolerance aspect for deficiencies in compliance monitoring. The SDT has proposed additional language that, together with a framework that also includes VSL language and RSAW audit guidance language, addresses the larger issue and shifts the focus of certain requirements to correcting deficiencies. This is explained in greater detail in the summary explanation at the beginning of this document.

Several commenters expressed their concerns on the protection of Low Impact BES Cyber Systems and the compliance demonstration of requirements that apply to them. The SDT has spent considerable time and effort to work with stakeholders on addressing this issue and believes that the approach in the new proposed draft addresses the concerns.

Multiple commenters reiterated concerns on the broad application of CIP V5 irrespective of connectivity. The SDT has included consideration of connectivity in the applicability of requirements and believes that this approach appropriately addresses applicability differences due to connectivity type. The SDT reiterates its posture that, while connectivity is an important vector for cyber security threats, it is not the only one and that the CIP standards encompass a holistic approach to the protection of BES Cyber Systems.

There were multiple comments that suggested the phrase "but not limited to…" may be construed as required evidence. The SDT agrees with the comment and is using the standard language "Example(s) of evidence may include, but is not limited to…" to convey two concepts in the measure: the evidence in the measure are not required evidence but represents examples of quality evidence, and entities may present other evidence that may be presented in lieu of the ones described or in addition to them.

Multiple comments were based on the definition of periodic requirements, with another commenter citing the CAN on Annual that has been published. The SDT notes that CANs provide guidance for auditors, are not interpretations of standard requirements and are not the basis for changes to requirements. The SDT has considered all outstanding CANs as additional input to the development of these standards, and where the CANs result from unclear requirement language, the SDT has drafted language with a goal of eliminating the need of a CAN for auditing purposes. Since the word annual is not used in the V5 CIP standards, the term does not apply. The SDT has drafted language that reflects its intent while providing adequate flexibility to minimize zero defect effects.

Several commenters requested a global clarification similar to section 5 of CIP-003 that explains the significance of the use of bulleted and numbered items. Another comment was on the bullets in section 4, part 4.2.2. The SDT will insert a paragraph in the background section to include such explanations.

There were several comments on the use of a single VRF for each requirement, irrespective of whether it applies to High Impact or Medium Impact. Another comment was on the VSLs and the differentiation required to handle zero defect. VRFs are used as one of many input variables used to determine the sanction in the case of a violation of a standard. The current sanction table used for calculating regulatory sanctions is based on VRFs at a requirement level. However, there are many other considerations in the determination of a sanction for a specific violation. Until the current development of the evolving enforcement model is better defined, it is premature to effect changes to the VRF. Regarding VSLs, the SDT notes that VSLs are used after the fact, i.e. when a violation has already occurred. The SDT believes that VRFs, VSLs and RSAWs, together with appropriate requirement language, must together provide a complete framework to address the zero defect issue. The ballot for VRFs and VSLs is a non-binding ballot, and there is likely to be changes to accommodate evolving concepts in handling zero defect compliance and risk based compliance assessments.

Several comments were on the compliance section on records retention and retention requirements in standards requirements. Retention requirements, when specified in requirements, are requirements for technical reasons, such as event log retention for forensic purposes. The retention periods specified in the compliance section are meant to apply to records required for demonstrating compliance. For example, if 90 day event log retention is specifically required in a requirement, the Responsible Entity is expected to retain records that demonstrate that it has kept 90 days of logged events for the 3 years, not that it has kept 3 years' worth of these event logs. Under the compliance section, these could be log entries of the process that maintains a minimum of 90 days of log events.

Several commenters suggested that all sub-requirement parts should state the goal. The SDT generally provides the goal either in the body of the main text for the requirement, or in the rationale box. The SDT believes that the goal of each subpart is mostly self-evident given the overall requirement objective, and that addition of a goal for each subpart would be redundant and unnecessary in most cases.

There were several comments surrounding the need for a definition of Control Centers. The SDT directs entities to its summary response to Question D9 on this issue.

There were several comments on the removal of restoration resources from Medium Impact criteria, and cited the need to provide adequate justification. It is not clear to the SDT whether these comments were in support of this change. However, as a matter of normal SDT stakeholder input consideration, extensive debate on this issue was conducted in the NERC operating and planning technical committees, without a clear resolution. As a matter of procedure, the SDT must provide justification for changes from one release to another and has received stakeholder comments supporting this change.

There were multiple suggestions that a summary of the CIP Version 5 standards and the interaction between the requirements and their applicability be provided by the SDT. The SDT is focused on addressing technical issues from comments on requirements and on the standards themselves. The SDT appreciates any input provided by stakeholders, and it plans to facilitate distribution of an informational summary addressing this concern that was prepared by certain stakeholders that have been collaborating with the SDT. However, the formal posting with the standards would require other types of SDT, NERC and other stakeholder groups' review and/or approval and is not an appropriate venue for making compliance management tools available to stakeholders.

There were several comments on the issue of physical access controls for High Impact, specifically on whether two different access control systems are required. The SDT has provided guidance on this issue in the guidelines and technical basis section of CIP-006 that indicate that the intent of the requirements is not to require different control systems.

Numerous commenters expressed concern with the term "Associated Protected Cyber Assets". In considering these comments, the SDT noted that the concept of high water marking for Impact Level within an ESP was not very clear. The SDT has defined a term Protected Cyber Assets to incorporate the concept of BES Cyber Systems, their associated Cyber Assets within the same ESP and the concept of High Water Marking for Impact level within an ESP.

There were several comments that a definition for dial-up connectivity is needed. The SDT has included a definition for "Dial-up Connectivity" in this draft proposal.

There were comments on the use of "Associated…" in the applicability column of requirement tables. The SDT has made some changes to the language used to clarify the applicability and has also used the defined term Protected Cyber Assets to further clarify applicability.

There were comments relating to a number of editorial and stylistic issues related to table headers, capitalization and inconsistencies of terms. The SDT has considered these comments and made the appropriate changes.

One commenter recommended that the exemptions section in the applicability section should be specific to the standard, and not say CIP-002-5 in standards other than CIP-002. The SDT agrees and has made the appropriate changes in the standards.

One commenter suggested that the application guidelines should be allowed to change from standard to standard and that glossary terms should not be defined again in the standard. The SDT disagrees that application guidelines should be the same for all standards, but does agree that there should not be any incompatibility or inconsistency between the guidelines and the standards. The SDT also agrees that there should not be any definitions repeated in a standard when they are proposed glossary terms. The SDT will ensure consistency between guidelines and standard requirements. The SDT notes that the notes on glossary terms in the guidelines or background section are intended to provide additional explanantion of the terms and not be replacement definitions for the proposed terms for the NERC glossary. The requirements in the standard are the ultimate source of authoritative text for compliance.

One commenter suggested that the requirements that should be subject to CIP Exceptional Circumstances should be extended to most requirements except those in CIP-002, CIP-003 and CIP-004, and provided a list of requirements that should be subject to CIP Exceptional Circumstances. The SDT has carefully selected requirements that it believes are appropriately suitable for a CIP Exceptional Circumstance in order to facilitate the handling of emergency situations and timely electronic and physical access for first responders. With regard to a comment on ensuring that CIP Exceptional Circumstance would not require a TFE, the SDT has no jurisdiction over Rules of Procedure and cannot predict what regulators will deem to be TFE triggering language in the future. It is not the SDT's intent that CIP Exceptional Circumstances be TFE triggering language, but rather, that the Responsible Entity has carefully defined its policies and

procedures for declaring and ending CIP Exceptional Circumstances as required in CIP-003, and that any specific CIP Exceptional Circumstance be documented as required to demonstrate compliance to the specific CIP requirement.

One commenter suggested that it should be clear that no policies or procedures are required for CIP-004 to CIP-011 Responsible Entities that do not have High or Medium Impact BES Cyber Systems. There is no requirement in CIP-004 through CIP-011 that is applicable to Low Impact BES Cyber Systems. This is clear in the applicability column of the requirements tables.

There was a comment on the incorporation of guidelines and technical basis in the standards, citing stakeholders' time constraints in reviewing guidelines during the comment period. The SDT has spent considerable time drafting guidelines and providing the technical basis for requirements as part of the structure of results based standards. The SDT believes that the guidelines and technical basis provides valuable information to stakeholders during the comment and balloting process. It provides valuable input to stakeholders on the intent of the SDT, both during the development and the implementation phases of the standards. This approach has received overwhelmingly positive feedback from stakeholders. While the SDT understands that these guidelines and technical basis are not intended to be used instead of, or in addition to requirements, the SDT believes they provide valuable context to the standards' requirements.

There was one comment on the use of attestations as measures, citing industry confusion on the appropriate use of attestations. The absence of "attestations" in the measures does not imply that attestations are not appropriate measures of compliance, but that the SDT chose to use more specific examples of evidence for these requirements. Whether attestations are appropriate measures of compliance depends on the requirement. The SDT has used attestations where it may more likely be the measure that can be produced as evidence of compliance, with no implication that it is the only way of demonstrating compliance.

One commenter suggested that part 4.2.3 of the applicability section (Section 4) may inadvertently create an exemption for Control Centers. While certain Functional Entities may not own BES Facilities as described in the NERC Glossary, they perform reliability functions as the Functional Entity listed in 4.1 for BES Facilities. The introductory paragraph of 4.2 specifically refers to "…Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above …"

One commenter requested clarification or a definition of "Adverse Reliability Impact": this term is defined in the NERC Glossary of Terms.

One commenter requested a formal definition for “Common Control System”: the SDT believes that the term control system is a widely understood term of art used in electric reliability operation and engineering and that it does not require specific definition in these standards.

One comment suggested that the standards use data and information interchangeably. The SDT notes that it has used data when referring to a set of values (numeric or otherwise) in its raw form, and to information when referring to data processed for a specific use.

One commenter noted that the CIP standards should be aligned more closely to the NIST or ISO standards. The SDT uses many frameworks (including the ones cited) as sources for the development of requirements. The SDT notes that both of the cited standards are general purpose cyber security standards and guidelines not intended for any specific industry use. The SDT believes that the mandatory nature for standards specifically for the BES poses unique challenges and requires an appropriately developed approach.

There was one comment that was extensively on the scope of applicability to asset owners and operators only, and the absence of compliance for suppliers and other third party providers. The SDT notes that these mandatory standards are developed under the jurisdiction of the ERO and that they can only be applied to NERC Registered Entities.

One comment was on the awareness and training requirement in CIP-004 R2 and role based awareness training. The comment was specific that the items in the table in R2 referred to systems while the requirement cited role based training. Table R2 contains the requirements for the required content of the training program, but the level at which the training is provided in each item is based on the role of the individual taking the training.

One comment was extensively on the 99.9% availability specification in CIP-006. The SDT has redrafted the requirement and the 99.9% specification has been removed.

There was one comment on the effect of the application of the CIP standards on small entities. The SDT notes that BES Cyber Systems are categorized based on reliability impact rather than on entity size. The SDT has developed the requirements to be commensurate with the level of impact on the BES. The SDT has not included entity size as an input to the applicability of requirements.

One comment was extensively on section 4.2.2. The SDT notes that section 4.2.2 is not intended to specify the impact criteria, but the scope. Consequently, many of the terms used are extracted from the registration criteria for DPs. Many of the comments presented have been incorporated in the proposed new draft, while a few are appropriate as part of the criteria.

One commenter made many remarks on global sections used in all standards. These will be reviewed by NERC standard staff as standard templates applicable to NERC standards.

There was a comment on the use of "where technically feasible" and the commenter suggested the use of language that would specify compensating controls. The SDT notes that there were requirements in CIP Versions 1-4 that had alternative language to allow compensating controls, but that the language was added to TFE triggers.

One commenter requested a definition of "Associated Data Centers". Please refer to the summary response on this issue to comments on D9.

One commenter was concerned with the periodic requirements, specifically on the 15 month period for periodic requirements intended to be performed annually. The commenters suggested alternative language that would ensure strict compliance with a 12 month period. The intent of the SDT in specifying a 15 month period for annual requirements is to provide some flexibility to entities in the framework of attenuating zero defect requirements. The comments imply that Responsible Entities would aim for strict minimum compliance at the cost of increased non-compliance risk. From the practical implementation standpoint, the SDT understands that most Responsible Entities will implement a process that would ensure the performance in a period less than 15 months (an annual period is easier to track from the compliance management standpoint) for assured compliance.

One comment was raised on the SDT's discussion of redundancy as not being a mitigation for cyber security vulnerabilities and stated that redundancy provide mitigation for some cyber security vulnerabilities. While redundancy provides some mitigation for recovery requirements, the SDT has not found a compelling case where strict redundancy of using an exactly mirrored system configuration would provide mitigation of a cyber security vulnerability. It is the SDT's opinion that such configurations have the unintended effect, from the cyber security (not operational) standpoint, of increasing the attack surface. The SDT does agree that configurations that provide redundancy of function rather than system redundancy can provide mitigation if implemented with systems dissimilar enough to provide mitigation of certain system specific cyber security vulnerabilities.

One comment was on the term Facility and its relation to systems, also stating that the term element is undefined. The SDT has used the term Facility in its defined meaning in the NERC Glossary when used in its capitalized form. The term Facility is used to refer to groups physical BES Elements. The NERC Glossary has a definition of Element used in the context of the BES. In cases where the SDT intends a broader scope to include systems, the SDT has used "Facilities, systems and equipment".

There was a comment on the exemption from the standards of cyber assets between discrete ESPs. In particular, the commenter suggested requirements to implement end-to-end encryption. The commenter seems to suggest that such encryption should be required for routable and non-routable protocols. In addition, the commenters suggest that EAPs should be subject to cyber security requirements. The SDT has not required specific technologies to protect information between ESPs, but has focused instead on the cyber security objectives of access control and monitoring of traffic across EAPs. The comments do not seem to take into account communication between ESPs of real-time, latency sensitive applications common in control systems. The authenticity and integrity of application data or information is not always implemented using communication encryption technology, but may be implemented at other layers of the overall stack without the latency overhead of encryption. The commenters also seem to interchangeably use EAPs and the cyber assets that implement the EAP. The CIP definition of an EAP is an interface. There are however requirements, including security event monitoring requirements, that are applicable to the Cyber Assets that perform access control and monitoring functions, including those that implement an EAP, for electronic and physical access.

A commenter suggested that BES information protection requirements should apply to third parties. The SDT agrees and expects the Responsible Entity to comply with requirements for protecting and handling BES protected information, whether such information is accessed or handled by its own employees and third parties. The requirements in CIP-011 require the Responsible Entity to implement processes to ensure such access control and handling.

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

One commenter suggested that the statement in the implementation plan that starts with "Not withstanding any order to the contrary…" should be amended in light of Order 706. The SDT believes that the window for the application of the statement is still possible given the deadline in Order 761.

One commenter inquired on when a cyber system would have to come into compliance as a result of an emergency. One commenter also inquired on how to treat temporary elevation. If the cyber system is re-categorized or is a new cyber system as a result of that emergency or unplanned change, the implementation table specifies 12 months.

There was a comment on missing requirements in item 5 of the Implementation Plan. The SDT has included these requirements.

One commenter pointed out that the background section dealing with reliable operation of the BES contains an unclear reference to the Functional Model. The SDT has added qualifications that clarify that both reliability tasks defined in the Functional Model and the functional entity's relationships with other functional entities are considered.

One commenter suggested that there are requirements where the text of the requirement specifies BES Cyber Systems when the applicability column specifies more than BES Cyber Systems. The SDT has reviewed the language of the requirements where this occurs to ensure consistency with the applicability column. In cases where more than BES Cyber Systems apply, the SDT generally uses "applicable Cyber Assets."

One commenter expressed the need for the concept of escorted electronic access for remote support using technologies such as WebEx. The fundamental concept in escorted access is not only that of continuous visibility on the actions of the escorted individual, but also the capability of timely intervention in the case of inappropriate action. The SDT believes that total support for this concept is not possible in an electronic access scenario.

One commenter stated that in its opinion, the functional entity Interchange Coordinator (IC) does not have any asset that would be included, and should therefore not be included in the applicability section. The SDT reviewed the reliability tasks for the IC function as well as the responsibilities of the IC Functional Entity in its relationship with other functional entities in the Functional Model and noted real-time responsibilities in the latter in relation to BAs and RCs.

Questions with Votes Only:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
FirstEnergy	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
ACES Power Marketing	No
SPP and Member companies	No
Comment Development SME List	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Hydro One	No
Ingleside Cogeneration LP	No
NIPSCO	No
Trans Bay Cable	No
Consumers Energy Company	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
American Transmission Company, LLC	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
ISO New England Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No

Organization	Yes or No
Deseret Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
US Bureau of Reclamation	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

2. Do you agree with the proposed definition of Control Center?

Organization	Yes or No
NRG Energy Companies	No
PNGC Comment Group	No
Madison Gas and Electric Company	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
IRC Standards Review Committee	No
National Rural Electric Cooperative Association (NRECA)	No
Southern California Edison	No

Organization	Yes or No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
PSEG	No
Texas Reliability Entity	No
Liberty Electric Power LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No

Organization	Yes or No
POrtland General Electric	No
Exelon Corporation and its affiliates	No
Farmington Electric Utility System	No
Indiana Municipal Power Agency	No
Deseret Power	No
Central Lincoln	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes

Organization	Yes or No
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
SPP and Member companies	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Progress Energy	Yes
Western Area Power Administration	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United Illuminating company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
Nebraska Public Power District	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
American Public Power Association	Yes

Organization	Yes or No
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Dominion	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
NCEMC	No
ACES Power Marketing	No
Southern Company Services, Inc.	No
National Rural Electric	No

Organization	Yes or No
Cooperative Association (NRECA)	
Dairyland Power Cooperative	No
Tri-State G&T - Transmission	No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Trans Bay Cable	No
Manitoba Hydro	No

Organization	Yes or No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes

Organization	Yes or No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes

Organization	Yes or No
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes

Organization	Yes or No
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?

Organization	Yes or No
Salt River Project	No
Trans Bay Cable	No
United Illuminating company	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Dairyland Power Cooperative	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Madison Gas and Electric Company	No

Organization	Yes or No
MRO NSRF	No
Duke Energy	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Comment Development SME List	No
CenterPoint Energy	No
NIPSCO	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No

Organization	Yes or No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Southern California Edison	Yes
ATCO Electric	Yes
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
NCEMC	Yes
SPP and Member companies	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Ingleside Cogeneration LP	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Farmington Electric Utility System	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes
Luminant	
American Transmission Company, LLC	

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
FirstEnergy	No
Duke Energy	No
Florida Municipal Power Agency	No
SPP and Member companies	No
IRC Standards Review Committee	No

Organization	Yes or No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
NIPSCO	No
Hydro-QuÃ©bec Production	No
Turlock Irrigation District	No
Bonneville Power Administration	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
NCEMC	Yes
ACES Power Marketing	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal	Yes

Organization	Yes or No
Wholesale Electric Company	
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Progress Energy	No

Organization	Yes or No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
ISO New England Inc.	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Utility Services Inc.	No
New York Power Authority	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
FirstEnergy	Yes
NCEMC	Yes

Organization	Yes or No
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison	Yes
Dairyland Power Cooperative	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes

Organization	Yes or No
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes

Organization	Yes or No
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Nebraska Public Power District	Yes
Alliant Energy	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

Organization	Yes or No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
Trans Bay Cable	No
Turlock Irrigation District	No
NextEra Energy, Inc.	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
MRO NSRF	No
NESCOR/NESCO	No
Duke Energy	No

Organization	Yes or No
Southern Company Services, Inc.	No
CenterPoint Energy	No
Consumers Energy Company	No
Manitoba Hydro	No
Snohomish County PUD	No
MidAmerican Energy Company	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
NYISO	No
Kansas City Power & Light	No
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
United Illuminating company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Brazos Electric Power Cooperative	Yes
Utility Services Inc.	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
American Public Power Association	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
California Independent System Operator	Yes

Organization	Yes or No
Madison Gas and Electric Company	
Luminant	
American Transmission Company, LLC	

END OF REPORT