Consolidation of Comments

Cyber Security Concept Paper: *"Categorizing Cyber Systems — An Approach Based on BES Reliability Functions"*

This Consolidation of Comments summarizes the comments received during the 45 day industry comment period for the Cyber Security Concept Paper: "*Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*," developed by the Project 2008-06 — Cyber Security Order 706 Standards Drafting Team (CS 706 SDT).

The 45-day comment period began on July 21, 2009 with an email industry stakeholders from NERC staff. Commenters were to email their comments to NERC staff at sarcomm@nerc.net by September 4, 2009 with the following subject line: "**Categorizing Cyber Systems Comment Form**".

As shown in Table 1, Listing of Commenters, question responses and comments on the subject concept paper were received from 52 sets of commenters. These question responses and comments have been forwarded to the CS 706 SDT to assist then in developing Reliability Standards Requirements for the next version of Standard CIP-002.

Comments were solicited from industry in response to 11 specific questions, as well as general editorial comments on the concept paper itself. This document represents a consolidation of all comments received. All comments are identified by a unique commentor identifier.

Responses to the questions are grouped by question, and presented in the same order as the commentors are listed in Table 1. Some commentors elected to only comment on a subset of the sections. If a commentor did not submit a comment for a particular section, no reference to that commentor is included in that section.

Comments submitted as general editorial comments to the concept paper are ordered by the section page number and line number to which the comment relates, thereby grouping like comments together. Some commentors elected to not provide general edit comments. No indication is provided for non-commentors to this section.

Table 1 – Listing of Commenters

Cyber Security Concept Paper: "*Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*"

		Commenter	Organization	Identifier
1.	Individual	Steve Alexanderson	Central Lincoln People's Utility District	CLPUD
2.	Individual	David Martorana	Tenaska, Inc.	TNSK
3.	Individual	Bill Hellinghausen	Eagle Energy Partners	EAGLE
4.	Individual	Alice Murdock	Xcel Energy	XCEL
5.	Group	Ruth Blevins	Virginia Electric and Power Company	DOM
		John Calder	Virginia Electric and Power Company	
		Vern Colbert	Virginia Electric and Power Company	
		Marvin Walker	Virginia Electric and Power Company	
		Louis Slade	Virginia Electric and Power Company	
		Michael Gildea	Virginia Electric and Power Company	
		Mike Garton	Virginia Electric and Power Company	
		Connie Lowe	Virginia Electric and Power Company	
		Dennis Sollars	Virginia Electric and Power Company	
		Paul Rodi	Virginia Electric and Power Company	
		Dan Goyne	Virginia Electric and Power Company	
		Linda Krepp	Virginia Electric and Power Company	
		Perry Esposito	Virginia Electric and Power Company	
		Chip Humphrey	Virginia Electric and Power Company	
		George Wood	Virginia Electric and Power Company	
		Randy Reynolds	Virginia Electric and Power Company	
		John Loftis	Virginia Electric and Power Company	
		John Rainey	Virginia Electric and Power Company	

		Commenter	Organization	Identifier
		Marc Gaudette	Virginia Electric and Power Company	
		Dave Connelly	Virginia Electric and Power Company	
		Karen Curtis	Virginia Electric and Power Company	
		Jalal Babik	Virginia Electric and Power Company	
		Johmar Frias	Virginia Electric and Power Company	
6.	Individual	Frank Gaffney	Florida Municipal Power Agency and Some Members: Lakeland Electric, Beaches Energy Services, Kissimmee Utility Authority, Fort Pierce Utility Authority, and City of Vero Beach	FMPA
7.	Individual	Gary W. Cox	Southwestern Power Administration	SWPA
8.	Individual	John Brockhan	CenterPoint Energy	CPE
9.	Individual	Anthony Wright	Georgia Transmission Corporation	GTC
10.	Individual	Ron Blume	Dyonyx	DYONYX
11.	Group	Denise Koehn	Bonneville Power Administration	BPA
		Curt Wilkins	Bonneville Power Administration	
		Kelly Hazelton	Bonneville Power Administration	
		Huy Ngo	Bonneville Power Administration	
		Kelly Gardner	Bonneville Power Administration	
		Pete Raschio	Bonneville Power Administration	
		Sharon Brown	Bonneville Power Administration	
		Karin Butler	Bonneville Power Administration	
		Kevin Dorning	Bonneville Power Administration	
		Laura Demory	Bonneville Power Administration	
		Rita Coppernoll	Bonneville Power Administration	
12.	Individual	Dave Batz	Edison Electric Institute	EEI
13.	Individual	Randy Schimka	San Diego Gas and Electric Co.	SDGE

		Commenter	Organization	Identifier
14.	Individual	Guy Andrews	Georgia System Operations Corp.	GSOC
15.	Individual	Ed Carmen	Baltimore Gas and Electric Company	BGE
16.	Individual	John Allen	City Utilities of Springfield, Missouri	CUSMO
17.	Group	Greg Fraser	Manitoba Hydro	MH
		Jackie Collett	Manitoba Hydro	
18.	Group	Roger Fradenburgh	Network & Security Technologies, Inc.	NST
		Nick Lauriat	Network & Security Technologies, Inc.	
		Nic Ziccardi	Network & Security Technologies, Inc.	
19.	Group	Guy Zito	Northeast Power Coordinating Council	NPCC
		Ralph Rufrano	New York Power Authority	
		Alan Adamson	New York State Reliability Council, LLC	
		Gregory Campoli	New York Independent System Operator	
		Roger Champagne	Hydro-Quebec TransEnergie	
		Kurtis Chong	Independent Electricity System Operator	
		Sylvain Clermont	Hydro-Quebec TransEnergie	
		Manuel Couto	National Grid	
		Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	
		Brian Evans-Mongeon	Utility Services	
		Mike Garton	Dominion Resources Services, Inc.	
		Brian L. Gooder	Ontario Power Generation Incorporated	
		Kathleen Goodman	ISO - New England	
		David Kiguel	Hydro One Networks Inc.	
		Michael R. Lombardi	Northeast Utilities	
		Randy MacDonald	New Brunswick System Operator	

		Commenter	Organization	Identifier
		Greg Mason	Dynegy Generation	
		Bruce Metruck	New York Power Authority	
		Chris Orzel	FPL Energy/NextEra Energy	
		Robert Pellegrini	The United Illuminating Company	
		Michael Schiavone	Nation Grid	
		Peter Yost	Consolidated Edison Co. of New York, Inc.	
		Gerry Dunbar	Northeast Power Coordinating Council	
		Lee Pedowicz	Northeast Power Coordinating Council	
20.	Group	Larry Bugh	ReliabilityFirst Corporation	RFC
		Lew Folkerth	ReliabilityFirst Corporation	
		Steve Garn	ReliabilityFirst Corporation	
21.	Group	Jim Brenton	ISO/RTO Council—Security Working Group	IRC
		Ann Delenela	ERCOT	
		Joe Pereira	ISO-NE	
		David Dunn	IESO	
		James Sample	TVA	
		John McGlynn	PJM	
		Philip Propes	SPP	
		Christine Hasha	ERCOT	
		Ann Delenela	ERCOT	
		Jason Marshall	MW-ISO	
		Jeff Maddox	ERCOT	
		Tim Lockwood	Cal-ISO	
22.	Group	Doug Hohlbaugh	FirstEnergy	FE

		Commenter	Organization	Identifier
		Rob Martinko	FirstEnergy	
		John Olszewski	FirstEnergy	
23.	Individual	Thad Ness	American Electric Power	AEP
24.	Individual	Joseph G. DePoorter	Madison Gas and Electric Company	MGE
25.	Individual	William Lucas	Wisconsin Electric Power Company	WE
26.	Individual	Eric Scott	Ameren	AMEREN
27.	Individual	Laura Lee	Duke Energy	DUKE
28.	Group	Hugh Francis	Southern Company	SOCO
29.	Individual	Robert Tallman	E.ON U.S.	E-ON
30.	Individual	Jason Shaver	American Transmission Co.	ATC
31.	Individual	Terri Pyle	Oklahoma Municipal Power Authority	OMPA
32.	Group	William Gallagher	Transmission Access Policy Study Group (TAPS), representing transmission dependent utilities in more than 35 states	TAPS
33.	Group	Katherine Hamilton	GridWise Alliance, Interoperability/Cyber Security Work Group	GWA
34.	Individual	Jason L. Marshall	Midwest ISO	MISO
35.	Individual	Jamie Starling	SCE&G	SCEG
36.	Group	Dan Powell	ReliabilityFirst CIP Committee (RFC CIPC)	RFC-CIP
			Indianapolis Power & Light Company	
		Mark Stefaniak	DTE Energy	
37.	Group	Sheryl Byrd	GE Energy Infrastructure	GEEI
		Matt Thomson	GEEI	
		Barry Littlefield	GEEI	
		Robert Boring	GEEI	
		Doug Cole	GEEI	

		Commenter	Organization	Identifier
		Dietmar Breitkreuz	GEEI	
		Daiane Carneiro	GEEI	
		Holly Chase	GEEI	
		Ruben Altunian	GEEI	
		Missam Momin	GEEI	
		Lisa Whelchel	GEEI	
		Charlie Campione	GEEI	
		James Fealey	GEEI	
		Gary Gray	GEEI	
		Jack Shoffstall	GEEI	
		George Runkle	GEEI	
		Martha Saker	GEEI	
38.	Individual	Paul Crist	Lincoln Electric System	LUS
39.	Group	Carol Gerou	MRO NERC Standards Review Subcommittee	MRO
		Neal Balu	Wisconsin Public Service	
		Terry Bilke	Midwest ISO	
		Ken Goldsmith	Alliant Energy	
		Jodi Jensen	Western Area Power	
		Terry Harbour	MidAmerican Energy Company	
		Joe Knight	Great River Energy	
		Alice Murdock	Xcel Energy	
		Scott Nickels	Rochester Public Utilities	
		Dave Rudolph	Basin Electric Power Cooperative	
		Eric Ruskamp	Lincoln Electric System	

		Commenter	Organization	Identifier
40.	Individual	Steve Newman	MidAmerican Energy Company	MEC
41.	Individual	Chris Klemm	PSEG	PSEG
42.	Individual	Shawn Barrett	Michigan Public Power Agency	MMPA
43.	Individual	Robert J. Kang	Southern California Edison	SCE
44.	Individual	Michael Goggin	American Wind Energy Association	AWEA
45.	Individual	Allen Mosher	American Public Power Association	APPA
46.	Individual	Paul Golden	PacifiCorp	PAC
47.	Individual	Martin Bauer	Bureau of Reclamation	USBR
48.	Individual	Mike McClain	Portland General Electric Co.	PGE
49.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	BRAZOS
50.	Individual	Chantel M. Haswell	Florida Power & Light	FPL
51.	Individual	Robert S. Lynch	Southwest Transmission Dependent Utility Group representing: Aguila Irrigation District, Ak-Chin Energy Services, Buckeye Water Conservation and Drainage District, Central Arizona Water Conservation District, Electrical District No. 3, Electrical District No. 4, Electrical District No. 5, Electrical District No. 6, Electrical District No. 7, Electrical District No. 8, Harquahala Valley Power District, Maricopa County Municipal Water District No. 1, McMullen Valley Water Conservation and Drainage District, City of Needles, Roosevelt Irrigation District, City of Safford, Tonopah Irrigation District, Wellton-Mohawk Irrigation and Drainage District	SWTDUG
52.	Individual	Paul McClay	Tampa Electric	TECO

Specific Questions:

1. Section C, BES Reliability Functions discusses a categorization approach based on reliability functions. Is the concept of categorizing by function instead of by asset clear? If not why?

Name	Comment
CLPUD	No. It is unclear if an entity starts with owned/operated equipment that is included in the NERC definition of BES and sorts them into the various BES subsystems, or sorts all equipment to see if they fit into the subsystems and assumes if they fit they are included in the BES. If the later is intended, this alters the NERC definition of BES.
TNSK	The Section C, BES Reliability Functions is very clear in that the categorizing will be done by function instead of by asset. This section should also specify that the Regional Coordinator will supply the impact assessment of the BES subsystem as it applies to the Generator Owners and Generator Operators.
XCEL	Yes
DOM	Yes, the concept is clear, but its scope is far too broad. Rather than using a risk based process to identify and focus on critical assets, it appears that this process could require every device used by every utility to be assessed equally. An approach that does not consider potential BES impacts and the probability of their occurrence early in the evaluation process exposes the industry to a very cumbersome risk-based evaluation process that will be extremely resource intensive to the point that it may be difficult to effectively implement and execute. Using load management as just one example of the issues raised by this "all in approach", if smart meters are being utilized, would every smart meter have to be assessed? Also, since there are requirements for load management in other existing reliability standards (i.e.: EOP-001, EOP-002, MOD-002, MOD-006, MOD-019, and MOD-020), which are applicable to many entities (BA, TOP, LSE, RC, TSP, PA, and RP) will each of these entities also have to evaluate smart meters under their jurisdiction against each applicable reliability standard requirement? How will owners of reliability functions be identified? Functions are typically shared by multiple entities and security levels, and protections would need to be coordinated among multiple entities. The owner of each device will also have to be involved in the decisions in determining what protections are required and why. Also, different reliability functions will have different impacts. Will there be a hierarchy of functions and of applicable reliability standard requirements? How will conflicts be resolved if they arise? Under the proposal as Dominion understands it, the entity(ies) responsible for each reliability function will have to play a much larger role in critical asset identification than they do currently. The reliability entity (PJM for the majority of Dominion's assets) will have to evaluate all the BES equipment that contributes to

	reliability and prioritize each piece of equipment's impact on the BES function and cyber vulnerability. This will entail that the reliability entity identify and understand every specific process, procedure and system from every member company (547 Members for PJM) necessary to achieve an adequate level of reliability ("ALR") and communicate these to the owners of all the assets necessary to achieve that ALR. These asset owners would then have to protect the equipment based on the highest evaluation provided by their reliability entities. This may require a much higher level of coordination than is required currently. It is also unclear how market rules may factor into implementation of this concept. Reliability standards contain the term 'load management', however the industry has been encouraged to increase the use of demand response and treat it in a manner similar to a generator. The technology implementing demand response is already being used in capacity markets of various RTOs/ISOs. The growth in this technology is expected to move into all aspects of load balancing and perhaps ancillary services such as regulation and reserves. This could mean that changes to the Functional Model as well as changes to existing, or the development of new, reliability standards and requirements will be needed. As demand response becomes an element of long term planning, the complexities increase. This paper should anticipate questions such as who will 'own' future load management (demand response) end–use customers, and who will determine how CIP standards will be met. There seems to be agreement that the one-size-fits-all approach should be abandoned. However, we are concerned that a literal interpretation of this concept paper as now written implies that every piece of equipment or software in, for example, a power station, substation, and/or control room is involved with reliability. This extreme viewpoint would mean that every device and every piece of software will need to be evaluated. Such evaluations are outside the scope of these CIP standards. Reliability of the BES itself is and should be covered by the other NERC standards already in place. The purpose of these CIP standards should be to protect against cyber attacks. Critical assets (however they are defined and identified) may need higher protection, but the one size-fits-all approach needs to give way to a more practical approach that accomplishes the goal of cyber protection without making it so onerous that owners will find it difficult to comply with the cyber standards themselves.
FMPA	First, let us say that we appreciate the efforts of the SDT to publish a concept paper on this very important topic to gain industry feedback early in the process. We believe the SDT is wise in doing so. Also, FMPA wants to make it clear that we believe that cyber security is essential and we support these important efforts to increase the security of one of our society's vital infrastructures; but, we also believe that these efforts needs to be focused on what is really important so that the efforts are most effective and not overly burdensome to the industry and to the Regional Entities. FMPA also agrees that a "yard-stick" is needed to determine whether a cyber system ought to be regulated by these standards. However, FMPA believes the yard-stick ought to be the definition of reliability as described in the Federal Power Act, Section 215(a)(4): "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements". Section 215 is clearly focused on avoiding "instability, uncontrolled separation, or cascading failure" and not on local impacts. Bearing Section 215's definition of reliability in mind, FMPA believes that an "Adequate Level of Reliability" ("ALR") is not the appropriate yard-

	stick for these standards. FMPA believes that, because these standards apply to "critical" cyber assets, the correct yard-stick is the definition of reliability in Section 215, which essentially refers to avoiding wide-area blackouts, and not the ALR yard-stick which would include local area issues that have no consequence to the wide-area. Using ALR as the yardstick will likely sweep in nearly all cyber systems that touch the BES because entities plan, design and operate the system to achieve ALR without much margin, otherwise there would be an opinion that we are "gold-plating" the system. We do not believe that it is the intent of these standards to regulate all cyber assets, but only those most "critical", meaning a subset of cyber systems that are, using synonyms, indispensible or vital that, if maliciously used, could cause "instability, uncontrolled separation, and cascading outages". FMPA agrees that Risk Management principles are the correct principles to use in determining which cyber systems ought to be regulated by the standards and how. FMPA also agrees that the existing methodology of identifying "critical assets" followed by "critical cyber assets" is flawed and prone to overlooking interactions. However, there are multiple ways to perform a risk management assessment, only one of which is the one proposed by the SDT. The fundamental premise of risk management is: 1) to inventory threats (or risks); 2) to evaluate the impacts of those threats; and 3) to develop methods to address those threats commensurate with their impacts and frequency of occurrence. FMPA believes that the bottom line of the CIP 002 assessment ought to be just that and the method by which an entity gets to the point of inventorying threats ought to be left up to that entity (e.g., the standard ought to regulate the "what", not the "how"). For instance, if the entity wants to define BES Reliability Functions, then BES Subsystems, to then proceed to an inventory of cyber assets and their threats, then, that should be the entity's choice. If another entity wants to proceed directly to inventorying cyber assets and associated threats, then that should be their choice. The standards / concept paper ought to reflect only the bottom line – inventorying threats and their impacts. Developing new definitions and new concepts such as BES Reliability Functions and BES Subsystems adds a level of complexity and overhead costs to the process that is not needed. The SDT might believe that the methodology described in the Concept Paper avoids inventorying all cyber assets by defining BES Reliability Functions and BES Subsystems first and using those to screen cyber systems; however, FMPA believes that the methodology, as laid out, does not cause entities to avoid a complete inventory of cyber systems that touch the BES (e.g., it would eliminate systems like billing systems, for instance, but, it does not eliminate relays, RTUs, and other cyber systems used for BES purposes). Also, the industry has faced criticism that we may have overlooked cyber systems and their interactions. Hence, FMPA believes that we will likely need to inventory all of our cyber systems that touch the BES anyway, so why have two intermediate steps of defining BES Reliability Functions and BES Subsystems, why not proceed directly to an inventory of cyber assets that touch the BES and a threat analysis of those cyber systems? Rather than creating a new definition of BES subsystems, the risk-based methodology for determining critical cyber assets might be better served in categorizing types of threats that can cause "instability, uncontrolled separation, and cascading outages", e.g., 1) sudden loss of supply, 2) sudden loss of demand, 3) threat of thermal cascading (e.g., loss of one facility causing an overload on another facility causing that facility to trip, then overloading another facility causing that facility to trip, etc.) and any resultant mismatch of supply and demand, 4) threat of voltage collapse and the resultant mismatch of supply and demand, etc. FMPA is aware of some people's concern of malicious use of lower impact cyber systems (e.g., a relay or RTU) to access

	more critical cyber systems such as Energy Management Systems, using the lower impact cyber systems as "gateways". However, it makes more sense to regulate the fortification of the Energy Management System from such malicious use than to regulate fortification of every digital relay. As an analogy, the electronic banking system is another one of society's vital infrastructures. For such as system, it makes sense to regulate cyber security of central banking systems that, if maliciously used, could dramatically impact our economy. It does not make sense to regulate cyber security on personal computers individuals use to perform on-line banking. It is important to understand that the intention of the standards is NOT to regulate every aspect of an entity's business, but only those aspects that can cause "instability, uncontrolled separation, and cascading outages". Just because the standards may not apply to non-critical cyber systems does not mean that entities will not have cyber security measures for those cyber systems. We are simply expressing that there is no need to regulate the security measures on those non-critical systems.
SWPA	Yes, the concept is clear. But why do we need another approach? There has not been sufficient time for the industry to judge the effectiveness of the current Critical Asset/Critical Cyber Asset approach. Give this a chance. If the issue is with entities that are dodging the process by creating a methodology that guarantees them to have no Critical Assets, then address that problem before you throw it all out. In other words, define what equipment/systems are critical cyber assets. Perhaps a hybrid of both is the best approach? Regardless of whether you use the "reliability functions" approach or the "Critical Cyber Asset" approach, the scope of the CIP Standards should be limited to systems that could cause instability, uncontrolled separation, or cascading failures on the BES as a result of a cyber security incident. In Section 215 of the 2005 Federal Power Act there is a definition for "reliability standards". This definition does not direct the ERO to apply burdensome standards to all facilities or systems owned or operated by a registered entity regardless of impact. It is not reasonable to require entities to be responsible for monitoring compliance on facilities and systems that have little or no impact to the BES. This will force entities to divert a large amount of resources away from system improvements or disconnect communication lines or both. It is our opinion that the results of this proposed change will ultimately decrease BES reliability and further burden the limited resources that NERC has for monitoring compliance to standards that are proven to enhance BES reliability.
CPE	While the concept may be clear, CenterPoint Energy disagrees with the concept and believes it unnecessary and premature to so completely alter this fundamental step before CIP-002 is implemented by a majority of responsible entities. Much time and effort has been expended trying to understand and implement the current requirements. Indeed, Table 2 entities are already required to be compliant with CIP-002 and Table 3 entities are well on their way. To suggest a radically different approach at this stage is, at best problematic and at worst, may cause some entities to rethink their positions and possibly miss the implementation date and therefore risk non-compliance. The suggested approach of viewing the BES holistically and identifying BES functions is overly broad and not needed. Most entities do not have the capability needed to view the BES holistically. Identifying assets that are critical to the reliable operation of the BES and those cyber systems that are essential to the operation of those assets is a much more concrete

	approach and, CenterPoint Energy believes, renders results that are at least comparable and possibly better than the suggested approach. Market functions should not be considered as critical to the reliability of the BES. It is common for emergency procedures to include the suspension of certain market activities until the emergency condition is resolved and yet the essential BES operations continue. This suggests that market functions are not critical to the reliability of the BES. Including distribution feeders as a BES Subsystem is another issue with which CenterPoint Energy disagrees with the SDT. In a blackstart restoration process, it becomes necessary to add load to stabilize the system. However, there are many options when it comes to which distribution feeder to use therefore, criticality of individual feeders to the restoration process is lessened. The inclusion of distribution feeders using a "function based" approach illustrates the pitfalls of such an approach. An asset based approach enables consideration of the diversity of assets to perform reliability functions. CenterPoint Energy believes the current process of identifying Critical Assets and then the Cyber Assets essential to the operation of the Critical Assets is a reasonable approach. CenterPoint Energy believes it is the best interests of all parties to allow the full implementation of the current CIP-002 Standard. As with any other Standard, compliance audits and spot checks may reveal additional issues for future consideration.
GTC	GTC agrees that this concept is clear in that it ties the categorization to the reliability of the Bulk Electric System, which is the goal of NERC standards in general. It is unclear, however, how this categorization takes place for a subsystem owned by a single entity where the subsystem performs functions of the BES for multiple entities (i.e. a substation RTU that is performing Control and Operation for one entity, performing situational awareness for another, and System Stability for yet another entity.)
DYONYX	First, the industry has spent hundreds of millions of dollars addressing the concept of Critical Assets and Critical Cyber Assets, reconfiguring network architectures to minimize exposure, and designing appropriate compliant security programs with an array of physical and cyber security protective measures. Now we are proposing a completely different paradigm to identify Critical Assets, hence forth to be defined as "BES Subsystems", with an astonishing level of detail that may well supersede a large component of the effort made to date. The point is that the particular categorization of systems by functions methodology proposed herein is way too complex and therefore hard to understand. In review of Sections I, J, and K, it is totally overkill, very time consuming, and in our opinion, unsustainable. While protecting these infrastructures is extremely important, we believe some degree of prudency and consideration for workability and sustainability should be taken? Having said this, we believe the concept of categorization of cyber systems by their impact on the reliability "functions" is conceptually a very logical approach. The drafting committee is to be commended for their effort. However, from a practical perspective, by starting with a "generalized" definition of reliability, e.g., the ALR definition, the number of "BES Functions" and ultimately "BES Subsystems" and "BES Cyber Systems" for analysis will increase significantly. The ALR may be appropriate for other "operating" standards, but does not appear to be appropriate for identifying Critical Assets / BES Subsystems. There

	are too many subjective terms in the ALR definition and accordingly the translation to the example set of defined "functions" appear to be prescribed. For example, the sixth characteristic defined under the ALR definition states; "The Bulk Electric System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components." What exactly does this have to do with the need to apply a high level of security to specific assets when the real problem is in the inadequacy of the design of the BES itself, i.e., insufficient generation capabilities, etc.? While the proposed approach appears to be designed to facilitate a means to establish various "levels" of criticality, is it really necessary to identify and categorize the systems at this level of detail? Do "Low", "Medium", and "High" attributes tell us anything relevant about the different measures that should be applied to BES Cyber Systems? We believe the two categories of "Critical" or "Not Critical" are indeed adequate. The current CIP Reliability Standard CIP-002 specifies that Critical Assets may be facilities, "systems" or equipment. We believe the current approach, with appropriate recognition of the impact "systems" can have on the reliability of the BES infrastructures and specific enhancements (many of which were identified in the Guideline), is a more feasible, less complex, and workable approach. In this regard, "Systems" are defined as Critical Assets themselves if, when compromised or otherwise removed from service, can impact the reliability of the BES. A "System" can impact the reliability of the BES if they impact other Critical Assets or "Non-Critical Assets together of which" impacts the reliability of the BES, e.g., an "EMS "system" that controls a large array of substations, neither of which is a Critical Asset, but "together" impacts the reliability of the BES, will be deemed a Critical Asset. This approach also eliminates the confusion about "control room" and "control centers"; it is the impact that the underlying "systems" within the control room or control center have on the reliability of the BES that is important, which has nothing to do with the definition of the "facility". See comment in Question # 5. With this approach, "reliability" of the BES from a Critical Asset perspective needs to be more precisely defined rather that the broad definition of ALR as proposed. Recommendation: Keeping in mind the concept of "common mode failures" as discussed in the "Security Guideline for the Electricity Sector: Identifying Critical Assets" and the analysis of systems as discussed above, we believe an extension of the existing CIP-002 R1 / R2 Standards utilizing the asset-based perspective builds on existing operational thinking, is less confusing, and will certainly be less onerous to administer and implement. The conceived functional approach, coupled with the proposed level of detailed, will generate hundreds of controversies, endless topics of subjectivity, and literary millions of hours of analysis. Adding in third party dependency analysis provisions amplify our concerns. In summary, the categorization of systems approach, while theoretically logical, is too cumbersome and complex. It has not worked well in the federal space.
BPA	Yes – "but the implications are not clear." – Over arching all the standards?

	– A Lot of work – same results. The indication was non-inclusive regarding the examples and the BES Function relationships. If non-inclusive, does that mean entities have the ability to exclude a Subsystem or Cyber System?
EEI	On behalf of its member companies, EEI appreciates the opportunity to provide comments on the ***Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*** **concept paper** developed by members of the Drafting Team. 1) EEI recognizes that: a. In Order No. 706, the Commission determined the CIP standards to be Mandatory and Enforceable. In that Order, the Commission also: i. Determined that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. (Order No. 706 at P 253.) ii. Believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. (Order No. 706 at P 25.) b. Congress has voiced concern regarding appropriate protection of critical infrastructure, including recent hearings and draft legislation discussions in the: i. Senate Committee on Energy and Natural Resources, ii. The House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. 2) EEI agrees that the appropriate identification and protection of Bulk Electric System (BES) critical assets and critical cyber assets are vital to the interests of the electric consumers and the nation. Asset owners recognize their commitment and obligation to protect cyber assets and cyber asset subsystems that are essential to the reliability of the BES. 3) EEI believes that the introduction of the concept paper represents a significant development for the protection of the BES. a. The concept paper identifies the opportunity to consider the evaluation of cyber assets and cyber systems that may impact the reliability of the BES but may not be directly connected to or associated with a single critical asset, such as a particular transmission substation or specific control center. b. The concept paper correctly identifies: *A crucial undertaking for the drafting team lies in developing these security controls in such a way as to* mitigate *risk while maximizing the value of the associated cyber security investment for the industry. To accomplish this objective, the drafting team seeks to develop a library of controls (requirements) appropriate to the degree and type of protection needed.* (concept paper, page 3, line 36)

   c. The concept paper identifies potential dependencies of elements of the BES upon cyber systems that may not be initially obvious.

4) EEI recommends the following improvements for the concept paper, and subsequent standard draft language:

   a. Elements to add to the concept paper:

      i. Additional language regarding risk assessment, including consideration of probability, or likelihood of adverse acts against critical cyber assets.

      ii. Definition of threat basis. In order to appropriately assess potential threats, including impact assessment, and subsequent mitigation strategies it is imperative that the threat be defined. Failure to define the threat can result in misallocation of resources that may leave the BES unprotected.

      iii. Given the current negative financial climate that our customers, companies, and regulatory agencies are operating within, it is important for mitigation methods to focus on reducing the greatest amount of risk for the least cost.

      iv. It may be appropriate for the concept paper to identify that certain cyber systems simply do not affect the reliable operation of the BES.

      v. Identification of potential contingencies that need to be considered in light of electromagnetic pulse (EMP) or geomagnetically induced current (GIC) events

   b. Elements to modify or eliminate from the concept paper:

      i. Care should be taken to avoid identification of functions that are inconsistent with the NERC Functional Model, or established utility practice.

      ii. The use of over-broad functions that may have elements with differing risks or impacts should be avoided, as this may lead to confusion and/or inappropriate (ineffective) security control identification. As an example from the concept paper itself:

> *Identical cyber systems may also be implemented in different environments, resulting in different impacts on the BES functions they support. For example, a control system in a small generating facility may have a different reliability impact on the BES than an identical control system operating a larger or several generating facilities.* (concept paper, page 15 line 27)

5) We believe that the interest of protecting the reliability of the BES would be best served through the application of the following principles:

   a. The industry has made a significant investment and concerted effort toward protecting critical assets and critical cyber assets under the original identification framework. We recommend that the valuable elements of the new approach be used to augment or enhance the legacy identification framework, rather than face the risk of loss of

	momentum and forward progress while the industry wrestles to understand and incorporate an entirely new methodology. b. An example of positive forward progress using the legacy identification framework, is the development of new guidelines for identifying critical assets and critical cyber assets. The opportunity is to build on the existing identification framework. c. The focus on identifying cyber assets or subsystems deserving of extra protection should be tied directly to a role that is *essential* for the reliable operation of the BES. We are concerned that the concept paper may call for a disproportionate level of protection for a vast number of cyber assets. d. Language developed within the concept paper or subsequent standards should be written in a way to be able to retire/reduce the need for Technical Feasibility exceptions (TFEs). e. Language developed within the concept paper or subsequent standards should provide for methods of identification of criticality and due process in the event of disagreements over designation. f. Careful consideration should be given to the discussion of multi-layer criticality matrix identification methods. The industry may be better served with a simpler method of designation and identification. g. The requirements for documenting the determination of criticality should be designed to minimize unnecessary administrative overhead. h. We suggest that the drafting team focus on the "What" of security control outcomes rather than the "How". i. We suggest that the drafting carefully consider issues of flexibility, sustainability, scalability, and repeatability when identifying options for security controls.
SDGE	Yes, the concept of categorizing by function is clear. It helps to provide a "Big-picture" viewpoint to the categorization process instead of starting by selecting assets.
GSOC	The concept as a whole is headed in a way to achieve better consistency in categorizing assets. This section is brief and could easily lead to confusion.
BGE	• Parts are abstract, hard to understand, and will sometimes demand a large amount of documented analysis to reach an obvious conclusion. It for example contains an example that a relay may be a relevant (in-scope) cyber system because it supports a transmission line (a BES subsystem), and the loss of the line may result in the impairment of the ability to manage loading constraints (A BES reliability function). The sheer burden of documenting and evaluating the one to many relationship between any relay or set of relays and a less than definitive catalog of BES reliability functions

	compares unfavorably with the simpler approach that we use under the current standard (A relay in a "critical asset" station is in scope). Not sure that avoiding one-size-fits-all security measures is an economical trade off; it seems properly scaled security could have been approached in a simpler way such as defining different levels of criticality for critical stations based on established contingencies (including the successful hack of a discrete ESP) and transmission planning criteria. • In general, this is a dramatic change in philosophy that will take some time and resources to accomplish the change. There should be a clear time frame for implementation that is possible to meet. • Section C is implying that any system which does the function listed in table 1 can be considered as BES Cyber System. Based on Table 1 Load Management Section, any system providing Demand Response and Smart Grid functions will be a Cyber System affecting BES. However, in the Figure 5, AMI System is shown as just a Collateral System. Does this mean AMI System by itself is not a Critical Cyber System? Elaborating Section C and Table 1 by providing specific examples around AMI and Demand Response System will be very helpful.
CUSMO	Yes, the concept is clear. But why do we need another approach? There has not been sufficient time for the industry to judge the effectiveness of the current Critical Asset/Critical Cyber Asset approach. Give this a chance. If the issue is with entities that are dodging the process by creating a methodology that guarantees them to have no Critical Assets, then address that problem before you throw it all out. In other words, define what equipment/systems are critical cyber assets. Perhaps a hybrid of both is the best approach? Regardless of whether you use the "reliability functions" approach or the "Critical Cyber Asset" approach, the scope of the CIP Standards should be limited to systems that could cause instability, uncontrolled separation, or cascading failures on the BES as a result of a cyber security incident. In Section 215 of the 2005 Federal Power Act there is a definition for "reliability standards". This definition does not direct the ERO to apply burdensome standards to all facilities or systems owned or operated by a registered entity regardless of impact. It is not reasonable to require entities to be responsible for monitoring compliance on facilities and systems that have little or no impact to the BES. This will force entities to divert a large amount of resources away from system improvements or disconnect communication lines or both. It is our opinion that the results of this proposed change will ultimately decrease BES reliability and further burden the limited resources that NERC has for monitoring compliance to standards that are proven to enhance BES reliability.
MH	The concept to categorize based on reliability functions is clear. Using NERC's definition of Adequate Level of Reliability (ALR) as foundation to categorize cyber assets is a good idea. If the revised CIP Standards require Responsible Entities to use this approach for their individual assessment then the terms "reliability function" and "BES subsystem" should be added to the NERC Glossary of Terms. The list of reliability functions should be vetted within NERC by the Operating and Planning Committees in addition to the project team. The concept to categorize based on reliability function could be used by the project team to develop a prescriptive table for use

	within the CIP Standards. The Responsible Entities could then use the table to categorize each of their BES subsystems. In this scenario, the reliability function definition and detailed description might not be necessary as part of the CIP standard.
NST	We believe the explanations in Section C and related sections are adequately clear.
NPCC	Agree on the concept but have implementation concerns.
RFC	Yes
IRC	Yes—the new concept and paradigm for categorization by BES Functions are clear. The external third-party review requirements of FERC Order 706 (section 322) were not addressed in this paper. FERC Order 706 stated that "an external review of critical assets by an appropriate organization is needed to assure that such lists are considered from a wide-area view (i.e., from a regional perspective) and to identify trends in critical asset identification." FERC indicated in Order 706 that allowing external review as a voluntary measure would not be adequate. While many Registered Entities want the RCs to perform this function for them, the use of RCs to perform the oversight role is problematic since 12 of the 17 current RCs are also registered to perform functions such as BA, TOP, IA, etc. How can an ISO RC conduct an external review of the same ISO BA functions? The SWG reiterates that we do not believe that RCs/BAs (that do not own the bulk electric system assets (e.g., generation/transmission) should play a functional role in identifying or providing oversight of "cyber assets" among such asset owning companies.
FE	The concept is fairly clear but the approach is too complex and over-reaching in the number of cyber systems that can practically be implemented and implies that all cyber systems have some level of BES impact. The industry should not significantly deviate from the process of first identifying Critical Assets and then the Critical Cyber Assets but rather aim to refine, improve and achieve a more consistent Critical Asset determination across industry. FE believes the appropriate path forward is to continue to focus on the guideline documents developed by the Security Guidelines Working Group (SGWG) for the currently effective version of CIP standards. The guidelines for Identifying Critical Assets and Critical Cyber Assets should be the basis for what forms the next generation of mandatory and enforceable reliability requirements for the CIP-002 standard. The industry has made a significant investment and concerted effort toward protecting Critical Assets and Critical Cyber Assets

	under the current identification framework, and it is on the eve of full implementation after 3 years of development. To take such a dramatic and complicated departure from the current path with the proposed concept would undermine progress and impede momentum. It is not evident that the proposed approach would provide a significant improvement in reliability over the existing approach or that any marginal benefit would be cost-effective given the labor intensive process outlined by the concept paper. While some elements of the new approach may be used to augment or enhance the current identification framework, FE recommends working from the current framework rather than the proposed concept going forward. Therefore, the team should consider a hybrid approach that simplifies and improves the Critical Asset determination by requiring a certain class of facilities such as Extra-High Voltage (EHV) that form the backbone of the BES classified as Critical Assets and thereby requiring a detailed inventory and assessment of any cyber assets related to their reliability function. Such an approach can improve reliability by cost-effectively protecting a broader set of BES assets. Regardless, the final approach taken should ultimately recognize that not all cyber assets should require enforceable regulatory oversight and that only the most essential functions or class of facilities should be covered.
AEP	AEP appreciates the drafting team posting the concept paper for review and allowing the industry the opportunity to comment. The approach outlined in the concept paper is challenging to understand as a result of the proposed paradigm shift. Moreover, this concept paper introduces numerous new concepts/terms and uses many interrelated terms, which could result in the terminology being convoluted. While the proposed methodology is less ambiguous than the current methodology, this concept paper is a potentially significant expansion of project scope without a commensurate reduction of risk. In addition, this framework makes the process very complex, which does not necessarily advance the intended objective of improving security and reliability. In general, more complex requirements may result in less security and reliability of the BES. The requirements of the current NERC CIP standards provide an adequate technical/regulatory framework to achieve the desired security improvements, as well as the basis for enforcement actions to address identified noncompliance. We suggest that the industry builds upon the framework that has been developed in versions 1 and 2 of the CIP cyber security standards through a set of structured interim progression of steps. It appears there are some concerns around the implementation of version 2 of CIP-002. We support modifications to address those concerns, with the exception of implementing a significant paradigm shift and a complete do-over without giving any recognition to what has already been done. AEP believes the concept of categorizing by function instead of by asset significantly broadens the scope and complexities without any significant benefits and without giving due consideration to what already has been done. The present methodology, which is based on the concept of asset protection, is well known and understood by the industry. Moreover, not all elements within a broad categorization by function are equal, nor have equal potential impact, if any, to the BES. We strongly urge the Drafting Team to reconsider the function-based concept. We recommend the Drafting Team continue with what has been implemented and enhance the current asset based system, as required.

Question 1

MGE	The proposed idea of "functions" is one possible way of identifying BES Subsystems that affect the reliability of the BES. Disagrees with the term of "operability" within the first sentence of section C. Unless it is used as it is defined by section 215 of the Federal Power Act: The term `reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements. If the term is not used as described, this could lead to an interpretation that all assets will be categorized as BES Subsystems. The SDT used a yet to be defined term "Reliability Functions" (and BES Function). This question cannot be totally answered until 1, Reliability Function is defined or 2, a supporting document is presented as to what the basis is of the defined Reliability Function. As written within this Concept Paper, "Situational Awareness" is given as an example. This should be removed from the applicability except for RC, TOP, and BAs, due to it is redundant to Control and Operations, the SCADA or EMS is designed to give the entity awareness of their system and status states, this will give others entities the ability to perform situational awareness of their system.
WE	While the concept is clear, Wisconsin Electric does not support changing the current risk based assessment to determine critical bulk electric system assets and associated critical cyber assets. If there's concern over uniform application of a risk based methodology by responsible entities, then we recommend further refinement of the current process to perform the risk analysis. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	The broad concept is fairly clear, but the details are not well articulated, and the approach may be too complex for the industry to embrace. We do not believe the methodology should proceed from the Adequate Level of Reliability as it is defined here. The sixth characteristic, supplying load at all times, would inappropriately expand the scope of the cyber security standards to distribution assets and systems. Supplying load is a service reliability issue as opposed to a BES reliability issue. The Introduction section implies a vastly expanded scope for the standard development in using terminology such as "at all times" and "identify all cyber systems". Order 706 required a risk based methodology. Risk is a measure of both consequences and probability – this methodology is based solely on consequences while ignoring probability of failure, which accounts for part of the vast scope increase. The concept would also be clearer if it was stated exactly what the cyber security standards are trying to protect against – is it intrusion and subsequent disabling of centralized control systems that would results in collapse of the BES, or is it physical or cyber damage to discreet transmission assets that could cause cascading failure, or both? In order to facilitate a common understanding, definitions should be provided for the BES Functions.
SOCO	Yes, the concept is clear.
E-ON	Yes. The BES function of assets is an integral part of the risk-based methodology currently employed to determine whether an asset is critical to BES reliability. However, while the concept is straightforward the manner in which the Concept Paper

	proposes to implement the concept is very disconcerting. The BES characteristics that are intended to inform the identification of BES Reliability functions go beyond what is required to maintain BES reliability
ATC	The concept paper does not provide enough details associated with categorization of functions to answer this question. The existing concept of critical asset identifies the type of event a company needs to consider (Cyber related attack), and a list of assets that need to be studied and the level of protection required for critical cyber assets. The concept paper does not address the questions of the type and severity of incident we are expected to protect against and the associated level of protection. This paper needs to provide more detail as to why the proposed concept is an improvement over the existing system, how it will improve reliability, the compliance obligations (Cyber and Physical security) associated with these changes, and how the transition from the existing CIP-002 Critical Asset identification regime to the categorization approach will occur.
OMPA	OMPA understands that the concept paper is proposing a paradigm shift from identifying or categorizing cyber resources from equipment or assets to a process or systems approach. However, the application of using a methodology to identify all cyber systems which support the reliable operation of the BES based on NERC's definition of Adequate Level of Reliability (ALR) is still unclear. This appears to be an extensive and tedious process to flush out for an entity that does not currently own or operate critical assets. Can we assume "BES" is still based on the definition in NERC's Statement of Compliance Registry Criteria (v 5.0)? It is also unclear if, or how, this methodology will align or be incorporated with the actual standard and if, or how, this process/methodology will be monitored/audited.
TAPS	As an informal association of TDUs dependent on the grid, TAPS believes NERC is on the right track in focusing not on individual BES and cyber assets, but on the interaction of BES assets in identifying which cyber systems must be protected from cyber attacks. For our nation to cost-effectively protect the grid from the types of cyber attacks that Congress cared about in enacting Section 215—those that would threaten instability, uncontrolled separation, and cascading outages—the identification of cyber assets requiring protection needs to focus on the cyber systems supporting BES assets that could create those wide-scale outages. When we bank online, it is up to the bank to protect its systems from any virus that may have infected our home computers. In the same way, what is key for purposes of Section 215 cyber standards is protecting from cyber attack the cyber systems that matter, e.g., those cyber systems that could compromise the reliability of the BES, rather than putting armor on every computer that interfaces with such cyber systems or otherwise makes any contribution to keeping the lights on anywhere. While we respect the aim of the SDT, it went off course when it defined BES Reliability Functions for purposes of cyber security based on Adequate Level of Reliability. Use of the ALR criterion to define BES Reliability Functions and BES Subsystems would sweep in virtually all BES facilities, and the cyber systems that support them as BES Cyber Systems meriting some level of protection. As shown on page 4 of the Concept Paper, ALR includes "the ability to supply the aggregate

	electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components." The Concept Paper concludes, at page 4, "These BES subsystems may be defined as facilities, equipment, or systems performing functions to ensure that the BES achieves an Adequate Level of Reliability." Using the ALR construct as a guide, virtually all BES functions and facilities would be included in BES subsystems because, almost by definition, they have been planned to serve load during some time frames taking account of scheduled and expected unscheduled outages. Such inclusion would lead to inappropriately gold-plated cyber security requirements that do not advance Section 215's statutory objective – avoiding instability, uncontrolled separation, and cascading outages. Rather, the focus of categorization of cyber facilities that warrant protection by NERC cyber security standards should be guided by the statutory definition of "reliable operations" that reliability standards are intended to achieve: "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." FPA Section 215(a)(4). *See also* Order 706 P 234 & n.79, quoting the "reliable operations" definition as giving meaning to NERC's definition of "critical assets" as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Incorporating the statutory "security-focused" criterion for assessing BES reliability functions and subsystems (in lieu of the Concept Paper's ALR criterion) would result in a more appropriate subset of the facilities and cyber systems that make a difference in terms of avoiding instability, uncontrolled separation, and cascading outages, and which therefore merit protection from cyber attacks. Such a focus would also more appropriately target our cyber protection efforts (and resources) at protecting the assets that matter, rather than needlessly burdening the economy with expenditures to secure facilities that do not matter from a security perspective. Further, while we appreciate that the SDT circulated the Concept Paper before all the concepts have been fine-tuned, TAPS is concerned about how these concepts can be developed to produce clear and auditable standards that registered entities can apply with confidence as to their compliance and that do not unduly burden Regional Entities from an enforcement point of view. The determination and mapping of BES Functions beyond those identified in the Functional Model, and identification of BES subsystems by (as yet undisclosed) "predefined criteria" may be needlessly complicating steps. It might be clearer and more direct to require each registered entity to inventory and evaluate each of its cyber assets to determine whether they have an impact on BES facilities that are critical to system security — avoiding instability, uncontrolled separation, and cascading outages. Consistent with Order 706's directive, as reflected in Order 706-A at PP 30, 33-34, that NERC provide "relatively smaller" entities with guidance and technical support in determining whether their assets are critical to the reliability of the Bulk Power System (thus presupposing that some assets will *not* be critical), the focus should remain on "critical assets," not all BES assets.
GWA	Yes.

Question 1

MISO	Categorizing the functions into high, medium, and low categories is a significant paradigm shift from the current set of CIP standards. The drafting team appears to be operating with the assumption that this paradigm shift is appropriate and they just need the industry to weigh in on how to make the categorization effort better. The drafting team needs to determine if industry is agreeable to switching from the existing critical and non-critical approach to the high, medium and low impact categorization.
SCEG	Yes
GEEI	The concept of categorizing by function instead of by asset is clear, but there will be functional overlap in practical application. Examples of functions and their classification would be help to clarify.
LES	No. LES is in agreement with the comments submitted by the TAPS organization and additionally, LES believes the intent of the current version of standard CIP-002 has a better security focus than the proposed concept paper, and that the current version of standard CIP-002 should be maintained. The current version of standard CIP-002 identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to identify cyber systems critical to the operation of the BES sub-systems. It then goes one step further by differentiating between routable and non-routable connections to these cyber systems, since non-routable connections are inherently more secure against, and limit potential damage from, remote attacks. This appears to be a straight forward and direct approach to securing the BES from cyber attack, and LES does not see any reason to deviate from this approach. If the concern is too much latitude in the current version of standard CIP-002, then maybe the new risk assessment guidelines should be officially amended to the current standard, assuring that all entities identify critical assets under a similar, Engineering study based assessment. Replacing the existing standard with an entirely new approach does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security.
MRO	No, the proposed process in the whitepaper does not provide any additional clarity or value versus the current process that is currently in place in CIP-002. It appears that the categorization approach would replace CIP-002 Requirement 1. Section C does not appropriately apply the Adequate Level Of Reliability as listed in Section B. The MRO NSRS believes the intent of the current version of CIP-002 standard has a better security focus than the proposed concept paper and that the current version of CIP-002 standard should be maintained since this concept paper does not elaborate in Section A on the maximum value the industry will receive by switching to this next risk-based assessment methodology plus, in Section C of this concept paper, an impact assessment is mentioned but it was not described how this assessment will be accomplished. The current version of CIP-002 standard identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to identify cyber systems critical to the operation of the BES sub-systems. This appears to be a straight forward and direct approach to securing the BES from cyber attack and MRO NSRS does not see any

	reason to deviate from this approach. If the concern is too much latitude in the current version of the CIP-002 standard, then maybe the new risk assessment guidelines should be officially amended to the current standard, assuring that all entities identify critical assets under a similar engineering study based assessment. Replacing the existing standard with an entirely new approach does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security.
MEC	No, the concept of categorizing by function is not clear. MidAmerican recommends retaining the designation of which BES physical assets are Critical Assets as the first step in the process of selecting Cyber Assets to protect. This clearly sets priorities to ultimately ensure that the most BES consequential assets have been protected. CIP-002 can be improved to achieve more consistency within the industry without abandoning the concept of Critical Assets. Specifically, descriptions for three of the seven asset categories that shall be considered in CIP-002 R1.2 include more detail descriptive criteria than the other four that generically refer to "support the reliable operation of the Bulk Electric System." Replace this generic phrase in those four sub-requirements with suggested criteria that corresponds to and complements existing industry requirements that are already defined for BES operations. This proposed change is more direct, achievable and clear than functional categorization. MidAmerican is concerned with the impact categorizing by function may have on the remaining CIP standards, as well as possible further delays and more confusion in an already complicated process. In development of the list of Critical Assets, it is then essential to comprehend what type of threat the BES is facing. Cyber threats are different than traditional threats to the reliability of the system. When protecting against cyber threats invoked by a malicious entity each responsible entity must assume that all of its BES facilities are under attack simultaneously. The responsible entity needs to determine which of these facilities (control centers, substations, generating plants, etc.) is critical to the BES and ultimately which Cyber Assets or systems support these critical facilities. Security controls are then selected to materially lower the probability and/or impact of a significant event for a specific type of Cyber Asset (for example, a relay verses a Windows PC). MidAmerican's recommended approach leverages both NERC's functional model and NIST together to benefit the cyber security of the BES. The core competencies of the NERC functional model are leveraged in selection of the Critical Assets. NIST's security controls core competencies are then leveraged in protection of the Critical Cyber Assets essential to the Critical Assets. Additionally, this approach leverages risk management guidance from the International Organization for Standardization (ISO), a worldwide federation of national standards bodies. ISO/IEC Guide 51 provides a basic risk vocabulary to develop common understanding. This guide simply defines risk as the combination of probability of an event and its consequence. Consequences (impacts) are addressed throughout the concept paper. Probability has a material role in risk management, but is not fully developed in the concept paper.

PSEG	PSEG supports the basic philosophy that future revisions should focus on the systems that protect the BES based on their significance to maintaining Adequate Level of Reliability, rather than their connection to a Critical Asset. However, the drafters need to be careful to ensure the work entities already have in place for CIP 002 Versions 1 and 2 compliance does not conflict with the Version 3 standard.
SCE	**GENERAL COMMENTS OF THE SOUTHERN CALIFORNIA EDISON COMPANY** Southern California Edison ("SCE") appreciates the opportunity to submit comments in response to the North American Electric Reliability Corporation's ("NERC") July 2009 concept paper titled "Categorizing Cyber Systems - An Approach Based on BES Reliability Functions" ("Concept Paper"). SCE understands that NERC drafted the Concept Paper in response to Order 706 issued by the Federal Regulatory Energy Commission ("FERC"). SCE continues to study the Concept Paper and reserves the right to supplement its comments as more information comes to light. However, assuming that the industry moves from the current risk-based approach to cyber security to the impact-based approach discussed in the Concept Paper, SCE makes the following comments intended to best ensure the reliability of the Bulk Electric System: First, the wholesale shift in direction proposed in the Concept Paper for Version 3 of CIP-002 would be so massive and revolutionary in scope that any changes to CIP-002 would affect its sister standards. For example, the Concept Paper notes that the shift to an impact-based system would require a new "library of controls" that would differ from asset to asset based on "the degree and type of protection needed." [Concept Paper, at pg. 30, lines 17-20]. Such controls would likely replace standards CIP-003 through CIP-009, which are calibrated to the current risk-based approach to cyber security. Therefore, in order to fully understand the potential impact of this new system, SCE urges NERC to present its proposed library of controls concurrent with version 3 of CIP-002. The common goal is to enhance the reliability of the Bulk Electric System. In order for the energy industry to determine whether the proposed revisions would accomplish that goal, the industry needs enough facts to make a reasoned analysis. Next, designing the proposed revisions will require careful thought and planning. As noted by the Concept Paper, the proposed move to an impact-based approach to cyber security represents nothing less than an industry-wide "paradigm shift." [*E.g.,* Concept Paper, at pg. 3, lines 44-45]. Simply "fast-tracking" the complex ideas presented in the Concept Paper would not necessarily enhance the protection of the bulk electric system. Instead, such an approach could lead to confusion and uncertainty as it would force the energy industry to grapple with hurriedly, and thus potentially poorly, drafted standards. Designing a paradigm shift for an entire industry requires a calm and deliberative development period with significant stakeholder and expert input. [*E.g.,* Concept Paper, at pg. 3, lines 50-51; pg. 8, lines 34-36; pg. 30, lines 31-32 (discussing opportunities for industry input)]. Finally, assuming that NERC's proposed revisions are adopted, SCE urges NERC consider a "phased in" approach to implementing this paradigm shift. By definition a paradigm shift is something that cannot be easily and quickly implemented. The energy industry will likely need time to acquire the technical, human and financial resources necessary to study, understand, and implement the impact-based system. A phased-in approach that implements this new paradigm shift in

	discrete, measured, chunks would likely enhance the reliability of the Bulk Electric System more effectively than by introducing this new system in one single installment. SCE also agrees with, and joins in, the following sections of the comments submitted by the Edison Electric Institute on this matter: Section 4(a)(i)-(iv); Section 4(b); Section 5(c) – (g).
AWEA	The concept is clear but the implementation is not. It is relatively easy to make a list of physical assets that is exhaustive and mutually exclusive (generators, substations, …) thus covering the entire system while also avoiding double counting. "BES Reliability Functions", on the other hand, can be defined in many ways. One example of a specific concern involves the categorization of variable energy resources such as wind plants and other renewable resources. They are predominantly energy suppliers with limited, but non-zero, capacity value. They are not peaking units or contingency reserve providers. They are not balancing resources. They may or may not impact frequency. Defining a robust system of BES Reliability Functions that is exhaustive and mutually exclusive may take more time than is available if a standard is to be posted for comment in 2009.
APPA	As an an initial matter, I agree with the SDT's general approach and I agree it is a paradigm shift. However, I find it difficult to envision how the industry will apply it in practice while ensuring effective compliance. The concept of categorizing BES Subsystems and Cyber Systems based on reliability functions to develop Cyber System Targets for Protection with different levels of protection based on the importance of the system makes a lot of intuitive and common sense. It responds to the common-mode failure risk associated with cyber systems associated with multiple BES systems. It responds to the fundamental problem that CIP-002 now presents – that once an asset is categorized as critical, an extreme level of cyber protection may be imposed under CIP-003 through CIP-009 – while no protection is required for assets that are not classified as critical. Nonetheless, I have major concerns that the SDT's conceptual approach will be extremely difficult to implement, particularly since the categorization proposal does not appear to be tied directly to NERC's other reliability standards. Developing an industry consensus around a set of BES Functions such as those shown in Table 1 would appear to be a precondition for implementing this approach. Developing that industry consensus in support of a well-defined set of BES functions, BES Subsystem Criteria, and a comprehensive identification of well-defined BES Subsystems and Cyber Systems within the industry is likely to be exceedingly difficult. Further the BES Functions and BES Subsystems (Facilities, Equipment and Cyber Systems) shown in Figure 1 overlap. The SDT could approach this task based on the NERC Functional Model – but that model is just that - a model of functional activities that does not consistently describe how specific registered entities have organized their operations. Each registered entity could attempt to develop its own functional analysis of operations and its associated BES systems and Cyber systems, but under that approach consistent application across entities is likely to be problematic and enforcement is likely to be burdensome, unless there are clear categorizations of facilities, e.g., all BA and TOP control centers that serve more than x

	MW fall in one risk bucket, while smaller control centers fall into a lower risk (and thus lower mitigation tier) bucket. Also, the reliance on Adequate Level of Reliability (page 4, lines 28-45) may be problematic, particularly the last definition, point 6. ("The Bulk Electric System has the ability to supply the aggregate electric power and energy requirements of the electric consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.") In the current context, this sub-criterion could be read to require all BES systems and cyber-systems to be identified as critical and thus requiring CIP protection since we are not in the business of building facilities that are not needed for the "reliability or operability of the system" (page 4, line 9).
PAC	No, the concept of categorizing by function is not clear. PacifiCorp recommends retaining the designation of which BES physical assets are Critical Assets as the first step in the process of selecting Cyber Assets to protect. The current approach of identifying critical assets ensures that the most consequential assets to the BES have been protected. This has become an accepted approached used by the industry as well as several Regional Organizations. The currently approved standards can be improved without abandoning the concept of Critical Assets. The concept paper defines several BES functions that were not specifically addressed in the evaluation criteria described in previous guidance documents of currently approved standards. PacifiCorp recommends adding these BES functions to the standard's language. In development of the list of Critical Assets, it is essential to comprehend what type of threat the BES is facing. Cyber threats are different than traditional threats to the reliability of the system. When protecting against cyber threats invoked by a malicious entity each responsible entity must assume that all of its BES facilities are under attack simultaneously. The responsible entity needs to determine which of these facilities (control centers, substations, generating plants, etc.) is critical to the BES and ultimately which Cyber Assets or systems support these critical facilities. Security controls are then selected that materially lower the probability and/or impact of a significant event for a specific type of Cyber Asset (example, relay verses Windows PC). PacifiCorp's recommended approach leverages both NERC's functional model and NIST together to benefit the cyber security of the BES. The core competencies of the NERC functional model are leveraged in selection of the Critical Assets. NIST's security controls core competencies are then leveraged in protection of the Critical Cyber Assets essential to the Critical Assets.
USBR	Page 9 line 10. Fundamentally, most entities have developed methodologies for the BES critical asset lists and critical cyber systems. They are in the process or have implemented significant modifications to their cyber asset and security protocols and hardware to protect those critical cyber systems. Accepting this approach will create the high probability that the entity which has achieved a level of compliance with the existing standards will not be compliant when the approach proposed by the drafting team is used to modify the existing standards. The registered entity must not reinvent its protocols and hardware for what may not be an improvement in the true vulnerability of the BES to failure of a critical cyber asset. The BES Functions

	described in the table are not specific enough to ascertain if a reliability impact for BES elements exists. Specific comments for the elements are described in question 2. In order to make it clear, the has to be specific determination that the subsystem will in fact have an impact on the BES Function. The language such as "whose compromise may result in" is not clear. The language should reflect a definite measurable impact "whose loss is demonstrated through system studies to result in" is specific and actionable.
PGE	Unclear. Shifting from an asset-based approach to a function-based approach would introduce additional ambiguity if each entity is made responsible for determining which functions are essential to maintaining an Adequate Level of Reliability. The determination of what constitutes an interconnection-wide Adequate Level of Reliability should include the input of the Regional Entities rather than being left to each individual entity. The approach in the concept paper would exponentially increase the scope of Cyber Assets potentially affected by the standard without providing entities with sufficient guidance to identify which assets are actually critical to the reliability of the BES. Such an approach would require the entity to undertake an extremely complex process which would be difficult to present to an auditor in an enforcement context. Additionally, the relationship between the reliability functions and the BES functions for which entities are registered is not clear.
FPL	1. We agree that the categorization by function is a good approach, however, as it is written there is still not a clear delineation of function vs. asset. The methodology as it is written, will still cause entities to go through a complete inventory of its cyber systems that touch the BES.
SWTDUG	I am writing on behalf of the Southwest Transmission Dependent Utility Group , a group of small utilities in the Southwest which occasionally intervenes in FERC proceedings to remind FERC that small utilities generally exempt from the Energy Policy Act of 2005 still exist. The purpose of this letter is to remind NERC and the Standards Drafting Team of the same reality. We will not comment substantively on the proposal for identifying various subsystems and this apparently new approach to identifying systems instead of cyber components and identifying them vertically down the system toward the ultimate consumer. Instead, we wish to offer a new construct we hope will be included in the effort. Just like improved technology to measure chemical components in drinking water does not, in and of itself, mean that that component in that quantity should be regulated, neither should the drafting team's ability to identify computer systems down the chain of communication into distribution systems change the regulatory structure with which we are currently living. In short, this exercise should not be an excuse for an attempt to expand jurisdiction and force entities that are not now registered

	to become registered under the guise of "has a computer, will regulate". While we may have missed something in our review of the proposal, it seems to us that a seminal element is missing from your proposed inquiry. Simply stated, the study should identify the appropriate place in the arena of Registered Entities where proper control mechanisms and processes would best be placed to ensure that smaller adjuncts to the Bulk Electric System are not in a position to cause the problems that motivate this inquiry. Thus, the Regional Entity in question should not define the cyber system as an excuse to expand its jurisdiction but should look at the array of Registered Entities within that system as a template for installing protective facilities and measures. We hope that the Standards Drafting Team will accept this challenge and make it part of their inquiry and development of categorizing factors. Thank you for the opportunity to provide these informal comments on this proposal.
TECO	We would encourage the SDT to map these functions back to the NERC defined BES Reliability Functions. It is important that the subsystem criteria and subsystem examples be thoroughly vetted with the industry.

2. In Table 1, the BES Reliability Functions listed in the "BES Function" column were not meant to be comprehensive. Are there any other functions we need to address and why?

Name	Comment
TNSK	As a Generator Owner and a Generator Operator the following information may not be readily available to support an adequate level of ALR; Contingency Reserve, Impacts on Frequency, Acceptable System Voltages, Nuclear Interface Requirements, System Operating Limits, Constraint Loading Requirements, and use of data supplied as it might relate to operational decisions. The Regional Entity will need to work with other entities to assess these functions.
XCEL	No
DOM	The BES functions are comprehensive, but to some degree they seem to be placing 'the cart before the horse.' The purpose of the CIP standards should be to establish requirements for the protection of cyber assets that support the BES, not for the protection of the specific BES functions themselves. In Table 1 for example, it is helpful to show BES systems and subsystems as shown in the first three columns just for reference, but it would be more helpful to breakdown the cyber system examples shown in column four in the same manner. In other words, show Cyber Functions, Cyber Subsystem Criteria, Cyber Subsystems Examples, etc., to give the reader a better feel for what the concept paper is aimed toward.
FMPA	For the reasons described in response to Question 1, FMPA believes that creation of a BES Reliability Function list that departs from the Functional Model, may add needless complication. We believe developing categories of "threats" is more appropriate. Such categories of threats could then be limited to functions in the functional model for assessment. For example, a threat of loss of "situational awareness" may be appropriate for some RCs/TOPs/BAs whose inaction or mistaken action due to lack of information or misinformation might cause "instability, uncontrolled separation, and cascading outages", but is not relevant from a security viewpoint to others, such as a DP, LSE or GO.
SWPA	No, in fact some of the examples are going beyond the scope of BES Reliability. For example, the Load Management Function is centered on distribution equipment that is not a part of the BES such as systems that control water heaters. If there is evidence that these systems control enough load to be material to BES Reliability, then NERC should establish a threshold level for aggregated water heater loads that is worthy of consideration. Also, the "Other" category either needs to be defined

	or eliminated. This will lead to a wide open argument in an audit.
GTC	GTC questions the inclusion of the Load Management function as defined. Systems in support of "Load Control, Water heater, ac, etc." are outside of the purview of BES reliability. GTC also suggests further clarification of the "Other" category.
DYONYX	See comment in Question # 1. The functions, for purpose of identifying Critical Assets including "systems" which may be defined as Critical Assets, should be comprehensive and focused only on those specific functions that cause a direct impact on the reliability of the BES (see Security Guideline for the Electricity Sector: Identifying Critical Assets).
BPA	This list seems too large as is. BPA would be more inclined to reduce the list than add to it. A major point we found out with the Priority Pathways is keeping it simple is much better than complicating it. Lack of clarity for why criteria was included in the BES Subsystem Criteria. Lack of clarity of the relationship between the BES Function, BES Subsystem Criteria, BES Subsystem Examples, and Cyber System Examples. Does a system listed in one of the "Example" columns imply entities are required to consider this as part of our "target of protection"? How does this table of information relate to the paper production processes under NERC CIP? Page 12, BES Function: Control and Operation, lists "Inter-utility data exchange" as a BES Subsystem Criteria. We wonder if this "function" is related to EIDE, if so, how and why? Page 12, BES Function: Control and Operation, lists "Control centre functionality" as a BES Subsystem Criteria. What does this imply/mean?
SDGE	Table 1 seems to have a good selection of examples for BES Functions. I can't think of any other examples at this time.
GSOC	The table presented in section C, Table 1 is a good start in presenting the BES functions that affect the operability and reliability of the BES. In the table under BES Function 'Other', one function that should be considered is the fuel handling systems that supply the generating facilities, gas supply for larger Gas fired facilities, Coal Handling facilities, Hydro facilities head gates, etc. If these facilities were compromised it could result in a common mode failure for the whole facility. Cutting off the fuel supply for gas fired plants and hydro plants will have the same effect as tripping the breaker.

BGE	Comment provided in the response to Question 1.
CUSMO	No, in fact some of the examples are going beyond the scope of BES Reliability. For example, the Load Management Function is centered on distribution equipment that is not a part of the BES such as systems that control water heaters. If there is evidence that these systems control enough load to be material to BES Reliability, then NERC should establish a threshold level for aggregated water heater loads that is worthy of consideration. Also, the "Other" category either needs to be defined or eliminated. This will lead to a wide open argument in an audit.
MH	Generation (which is not part of restoration, load balancing or contingency reserve) should be included in a reliability function with appropriate criteria for inclusion in the analysis. Where do Special Protection Systems fit into the reliability functions? They could be added as a reliability function which would be in keeping with CIP-002-1 or they should at least be added as a BES Subsystem Example under "Other" reliability function.
NST	We do not have specific functions to be added to the list that appears in Table 1. However, we recommend that this list be periodically reviewed and updated as necessary to reflect industry experience, evolving technology (e.g., Smart Grid), and possible future refinements to the current definitions of "reliability" and "operability" as they apply to the BES.
NPCC	At this time, we cannot think of any other functions.
RFC	No, an adequate sample has been presented.
IRC	No. However, the concept paper appears focused on Generation/Transmission Asset Owners and Operators and does not specifically address many BES functions typically found at ISO/RTO Control Centers which support Reliability Coordinator, Balancing Authority, and Transmission Operator (RC/BA/TOP) functions. Suggest further refinement and analysis of BES functions to specifically include and separately structure those functions provided by RC/BA/TOPs with wide-area or regional responsibilities as separate from those BES functions for Generation and Transmission System Owner/Operators per the NERC functional model.
AEP	The BES Function in Table 1 broadens the scope downward to include lower voltage transmission and distribution into the requirements of NERC-mandated cyber controls. This would exponentially increase the assets in scope without any significant

	benefit to enhance the security and reliability of the BES, as interruptions at this level would be local in nature without any wide area impact to the BES. For example, according to Table 1, Load Management Systems can be included into the loose definition of impacting the reliability of the BES. This is analogous to generation located on the distribution system that is not in scope of the BES. The graduated levels of cyber controls could apply to many more devices in stations, such as RTUs and PMUs; will this reduce our security exposure? Similarly, all generation necessary to serve load appears to be included into the ALR definition and this is a significant departure from the current standards. Could the drafting team provide clarification on this?
MGE	The list of "BES Functions" needs to be based on an established set of functions that are presently used within NERC and the utility industry. Registered Entities have applied countless hours of labor and spent huge sums of capital in being compliant with the current CIP-002-1 standard. Introducing new, unheard of functions will only lead to more confusion and slow down the implementation schedule. The Functional Model was designed to assist in designing NERC Standards perhaps that would be a useful reference. Each defined BES Subsystem (within the BES Function) needs to have a minimum level that is required to be met before applying this new methodology to it. An example would be Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more (as written in the current CIP-002-1 Standard). This will give a clear understanding of what threshold needs to be passed before applying this new methodology contained within the Concept paper. FERC Order 706, section 234 states that CIP-002 is the cornerstone of the CIP Reliability Standards because it acts as a "filter", determining whether a responsible entity must comply with the remaining CIP requirements. Suggest that the SDT have defined limits (filters) for all BES Subsystems, this will help all entities in ensuring that compliance with CIP-002 and be able to complete any following required CIP Standards.
WE	Wisconsin Electric does not feel there should be any additional functions to address. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	This is difficult to answer because it is not clear what the criteria for the BES Functions are, and the Functions are not clearly articulated. However, it appears that there are functions that are not truly critical to the reliability of the BES in Table 1, such as Contingency Reserve/Peakers (it is very unclear what this is referring to, as Contingency Reserves and Peakers are different things) and Load Management (seems only the part related to Load Balancing should be included). The methodology should recognize the diversity of contingency reserves (multiple units, purchases). Additionally, Constrain Management should not be in the table unless it is restricted to IROL management. Frequency Control (which is different than Frequency Response) should be added. If this methodology is to be used, more effort needs to be expended in developing industry consensus on what BES Functions should be included, working through established NERC committees and their subcommittees.

Question 2

SOCO	No and perhaps some of the functions can be combined.
E-ON	E ON U.S. suggests BES Reliability Functions are only those functions which 1) operate to prevent instability, uncontrolled separation, or cascading failures of the BES and 2) enable restoration of BES operation – rather than the comprehensive list provided in Table 1.
ATC	ATC believes that this table needs to focus on essential functions critical to preventing cascading outages / large blackouts and should not include protecting for an "Adequate Level of Reliability".
OMPA	Will a comprehensive list of BES functions be provided in the final concept paper based on the comments received?
TAPS	For the reasons described in response to Question 1, TAPS believes that creation of a BES Reliability Function list that departs from the Functional Model, may add needless complication. We also think that developing the list based on an ALR criterion is unduly broad. In contrast, defining the relevant BES Functions and Subsystems using a security focus (as opposed to an ALR focus), *i.e.*, limiting them to BES Functions and Subsystems critical to avoiding instability, uncontrolled separation, and cascading outages, would allow for streamlining the applicability of the functions for the intended purpose, thereby appropriately narrowing the BES assets and cyber systems that warrant cyber protection. For example, the "situational awareness" function may be appropriate for RCs/TOPs/BAs, but is not relevant from a security viewpoint to others, such as a DP, LSE or GO. Again, unduly broadening the functions would inappropriately sweep into cyber security compliance unnecessary BES subsystems and cyber systems that support them.
GWA	It is not necessary for the list of functions to be exhaustive. The last row of Table 1 allows for other functions to be included. However, to prevent "Other" from becoming a catchall and potentially diluting security resources for functions with significant reliability impacts, it would be helpful to develop a description for "Other" that defines criteria for determining when a function should be included in consideration. The sentence, "Other Specific use systems whose loss or compromise may impact the reliable BES operation…" should be modified to "Other Specific use systems whose loss or compromise ~~may~~ would reasonably be expected to impact the reliable BES operation…"
MISO	If the list was not meant to be comprehensive, why are you asking if additional functions need to be included? Is the plan to have an exhaustive list at some point? We would discourage the drafting team from developing a standard that is so prescriptive that it would attempt to cover every conceivable situation. The drafting team should remember that this is not a specification but a reliability standard that should describe the "what" and not the "how" of protecting appropriate cyber

	systems.
SCEG	Not to our knowledge. However it should be noted that if any functions are added these functions should only be those which support an adequate level of reliability (6 characteristics of the BES with an ALR)
RFC-CIP	Due to technological changes that will occur over time (e.g. smart grid technology), will entities have the flexibility to include additional functions that may be introduced after this version of CIP Standards becomes effective?
GEEI	No, but see the table below for clarifications needed.
LES	Yes, Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	This concept paper is confusing as well as this question. The concept paper indicates Table 1 only gives illustrative examples (see Section C) then in Section D this same table is suppose to indentify all BES Subsystems. Then this question here is looking for more illustrative examples. Perhaps the methodology should be reviewed to determine what is an essential BES function. MRO NSRS believes that Table 1 needs to focus on essential functions critical to preventing cascading outages / large blackouts and should not include protecting for an "Adequate Level of Reliability". However, the proposed approach does not provide more clarity than providing more specific criteria for asset selection under the current approach in the standards. More specific details would be required under any approach. MRO NSRS believes spending time adding clarity and specificity to the current standard is more productive.
MEC	No. MidAmerican is not aware of any additional functions that need to be addressed. MidAmerican is concerned with the complexity and overlap in the functions proposed. Providing more specific criteria for asset selection under the current approach in the standards would provide more clarity than the proposed approach. More specific details would be required under any approach. Spending time adding clarity and specificity to the current standard is more productive. The concept paper requires 14 pages to present just the concept of functions and still leaves many questions. The functions are not defined and would have to be synchronized with existing enforceable industry requirements that are already defined for BES operations. Without definition, functional categorization has the potential to expand the scope of Cyber Assets to be protected so significantly that the value of the cyber security investment is not maximized in mitigating risk.

Question 2

SCE	N/A – see comment to question 1.
APPA	See discussion of the Functional Model above under Q1. The SDT should consider whether BES Functions and BES Subsystems can instead be derived from the purpose sections and associated Requirements of NERC's other Reliability Standards.
PAC	No. PacifiCorp is not aware of any additional functions that need to be addressed. PacifiCorp recommends that the drafting team focus on providing clarity and specificity to the current standard by adding additional BES functions to the current evaluation criteria without abandoning an approach that has now been accepted and implemented by the industry.
USBR	Pages 10 through 14. The inclusion of Protective Relays used throughout the table as Cyber System Examples must be clarified to only include those relays that are addressable or programmable and would result in an impact to the BES. The inclusion of Plant Control Room(s) needs to be clarified as well. The inclusion of the under frequency scenario needs to be clarified as a system under frequency condition under a specific contingency condition as determined by studies. A Control Room is not a Cyber subsystem but may contain cyber equipment that may have an impact on the BES. The BES Subsystem criteria for "unacceptable system voltages" needs to be clarified as how that is determined and what the parameters are. The "Not meeting Nuclear Plant Interface Requirements" needs a caveat "if applicable". Constraint Management BES Subsystems examples Generation Unit(s) and Synchronous Condensers are not elements that meet the Glossary of Terms Definition for Constrained Facilities. These should be removed. The BES Subsystem Criteria for Control and Operation includes all Primary and Backup Control Centers used by Generator Operators "that have been registered in the NERC Registry. Since Registry is by function and not asset this automatically includes all control centers irrespective the size of the generation stations controlled. The selection of control centers would be by the role the control center plays in managing the BES. The BES Subsystem Criteria for Restoration includes all Generating units involved in restoration. Currently the selection of restoration units in many plans is not supported by study or test. The limitation should be those generating units essential to restoration as determined by system studies. The reference to Load (distribution feeders) needs to be clarified. The BES Subsystem Criteria for system stability indicates that Generation Resources need to be identified if they may compromise a number of events listed. This needs to be clarified how that would be determined to remove the best guess condition or needless conservatism.
FPL	We believe that most of the functions have been addressed and we agree that the list does not have to be fully comprehensive. We believe each entity needs to have some degree of discretion on what they think should be included in that list based on its specific system requirements. Although the list does not have to be comprehensive since any other system

	that impacts reliability will be reviewed in other standards and thus included as needed.
TECO	We would encourage the SDT to map these functions back to the NERC defined BES Reliability Functions. It is important that the subsystem criteria and subsystem examples be thoroughly vetted within the industry.

Question 3

3. Does the methodology presented in Section D, Identification of BES Subsystems and Section F, Identification of BES Cyber Systems capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

Name	Comment
CLPUD	Yes, but see comment 1 above.
TNSK	All of the systems appear to be adequately captured. The reliability impact will have to be determined by the Regional Coordinator.
XCEL	Seems correct.
DOM	Again as mentioned above, the identification discussed in Section D is useful, but overemphasizes BES functions versus the cyber functions which should be the target of this approach. Also, applying the functions in Table 1 referenced by Section D with Section F seems to require that every device on our system will be evaluated at least once, and that that many devices will be assessed multiple times.
FMPA	See FMPA's responses to Questions 1 and 2, which describe why FMPA believes that the FPA Section 215 definition of reliability is more appropriate than ALR, and that categorizing threats is more appropriate than categorizing BES Reliability Functions or BES Subsystems.
SWPA	Yes, in fact it is too comprehensive and goes beyond the scope of the BES into distribution level equipment such as water heaters listed in the Load Management Function.
GTC	GTC believes that by tying the identification to reliability functions, all systems appropriate for protection are identified.
DYONYX	See comment in Question #1.

BPA	This team felt that subsystems and cyber systems need to ultimately be defined by each utility on an individual basis. It is helpful that NERC lists specific examples for each subsystem. However, each utility may have exceptions or additions to the NERC list of subsystems and cyber systems. This may actually increase TFEs not decrease them.
SDGE	I don't see that a methodology is really presented in Section D for Identifying BES Subsystems. There is mention of application of "pre-defined criteria" for mapping, but I've read the paragraphs several times and can't really identify a clear methodology. Section F, however, does a better job of listing a fairly clear methodology to identify BES Cyber Systems. It's hard to say if Section F captures ALL of the systems that will need to be protected, but the examples listed represent a good start.
GSOC	See some of the examples listed in the answer to question 2 above for additional BES Subsystems to be considered. As far as the BES Cyber Systems, the focus has been and should be the specific BES Cyber System such as RTU, Electronic Relays, etc, Cyber systems associated with the communication needs to be considered. If the communication to or from Cyber Systems were compromised then it will definitely affect the operability of the BES. It would affect 'Situational Awareness', 'Control Center Operation', etc. Communications is out of scope in the NERC CIP Standards but these facilities should be factored in some capacity. These are the telecomm cyber systems that are located at the control centers, generating plants and substations that interface to the ESP.
BGE	Line 25: "centralized, automated, programmable area load shedding system": We can achieve this function using Advanced Meter Disconnect function and also using Demand Response devices such as Smart Thermostats controlling Air Conditioners. 1. Does this mean both AMI and Demand Response systems are automatically considered as a Critical Cyber System? 2. Any provision/controls such as maximum load that can be shed, and the time period in which the load is shed gradually instead of instantaneously, make these systems non-CIP or at least low Cyber Impact systems? 3. For AMI / Demand Response Systems it will be very helpful if the identification criteria is explained with a specific example with load, time parameters etc. If amount of load does not matter, please state this explicitly. 4. If safeguards have been put in place to keep a subsystem within Adequate Level of Reliability, does that system then fall under the CIP guidelines?
CUSMO	Yes, in fact it is too comprehensive and goes beyond the scope of the BES into distribution level equipment such as water heaters listed in the Load Management Function.

MH	Under “Control and Operation” AGC should also be listed as a BES Subsystem Example in addition to Cyber System Example. Cyber system components could be AGC (as part of EMS or separate), station controllers and unit controls. Where do Special Protection Systems fit into the reliability functions? They could be added as a reliability function which would be in keeping with CIP-002-1 or they should at least be added as a BES Subsystem Example under “Other” reliability function. Under “Other” reliability function the following two BES Subsystem Examples should be removed as they are targets of protection (support subsystems) and not BES Subsystems: “Support systems used to modify cyber systems “and “Physical Security System”. All components in a BES Subsystem should not automatically inherit the categorization of the overall BES subsystem. If many units are part of the BES subsystem, then the assessed impact could be Minimal (very low) for an individual unit. Redundancy (often mandatory requirements in other reliability standards) should be considered by individual Responsible Entities as part of their consideration as it may reduce the impact of an individual BES asset. Master ends of BES subsystems may be categorized higher than individual remote end BES Subsystems. Responsible Entities should be allowed flexibility to properly determine the range of impacts and the resulting categorization of the BES assets. Provision for this flexibility should be provided in the overall procedure for BES subsystem categorization. Any impacts for any common mode failure of cyber subsystems should be addressed in the categorization of cyber systems. Consideration should be given for a categorization level where no mandated security controls are required (Level for None).
NST	Regarding the identification of BES Subsystems, we recommend that the SDT clarify whether or not it anticipates that all BES Subsystems would be considered and characterized (High, Medium, Low) using the proposed methodology. If not, we recommend the SDT discuss what types of systems would typically be excluded (i.e., what type of BES elements or facilities perform or support functions that do not support the characteristics of ALR). Regarding the identification of BES Cyber Systems, we recommend that the SDT consider carrying forward CIP-002-1’s concept of identifying cyber systems that are essential to the operation of one or more BES Subsystems or to the performance of BES reliability or operability functions. We believe this qualifier is presently and would in the future be useful to help distinguish BES Cyber Systems that directly perform or support BES functions from cyber systems that play a supporting but not a direct role (referred to as “Interconnected Cyber Systems” in Section I, “Defining The Target of Protection”). Cyber systems that could, if compromised, be used to directly disable or impair BES Subsystems and/or BES functions should also be identified as “BES Cyber Systems” even if those cyber systems are not deemed “essential.”
NPCC	Yes, the methodology in Sections D and F capture all of the systems that will need to be protected to achieve an acceptable level of reliability. No other issues need be considered.

Question 3

RFC	Yes
IRC	Generally Yes. The concepts proposed within this section create valid selection criteria for the identification of BES Subsystems that have the capability for impact to the reliability of the BES from a regional or multi-regional approach. Reliability Coordinators, Balancing Authorities and/or Transmission Operators (RC/BA/TOPs) currently do not have the necessary Authority or "Safe Harbor" to determine what Registered Entity assets within their areas may be a risk to reliability of the BES. Although these Registered Entities are interconnected via interweaving cyber communications and data processing systems, the RC/BA/TOPs currently have little say in what the Registered Entities declare as CCAs. Additionally the RC/BA/TOPs do NOT have sufficient staff with the required skills and knowledge to perform the needed security risk assessments necessary to make these key determinations. While absolutely essential for success of the risk assessment process, the current skill sets of Electrical Power System Engineers currently found in most operations and planning groups do not include sufficient abilities to perform the cyber system and network security risk assessments needed to successfully support this type of regional oversight program. The costs associated with establishing this initial capability and sustaining the ongoing studies and assessments annually required to meet compliance may be significant as the security analysts, architects and risk managers with backgrounds in Electrical Power Systems are a scarce resource nationwide. It has been said that the North American Grid is the most complicated machine ever built but the regions are the second-most complicated machines. Any standard requiring the RC/BA/TOPs to perform the analysis proposed in these sections, must also address funding to pay for that support which may be far above their current operational budgets today.
AEP	The paper talks of Adequate Level of Reliability (ALR) but then continues to include issues just impacting reliability. Every outage, or every system that is unavailable 'impacts' reliability, but the loss of that system does not necessarily reduce reliability to below 'adequate' levels. Situational Awareness is another term used, but not really defined. All data, even the current temperature and the temperature forecast, provides "Situational Awareness," but loss of a thermometer does not degrade the transmission system to a level below the ALR. The utilization of an open model, such as described in this concept paper, may produce unintended or onerous results.
MGE	In Section D, it appears that BES Subsystem(s) are captured and that is what the industry appreciates, a clear cut, defined area that will help entities comply with the Standard. Perhaps the SDT should allow the Applicable Entities to use this as a minimum level and afford entities the ability to establish other BES Subsystems that are equally effective and efficient and unique to their system.

	Section F, Due to the wide assortment of technology that is used within the Eastern, Western interconnections, and ERCOT the SDT should allow the Applicable Entities to use this as an example or allow them to establish other BES Subsystems that are equally effective and efficient.
WE	Wisconsin Electric's opinion is that all BES cyber systems have been captured in Section D. We do encourage the continued use of probability of occurrence of a cyber attack to limit protection of systems that have little or no impact to the BES. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	The methodology will not only capture all of the systems that need to be protected, it will capture too much. The methodology is not selective enough. Additional guidance may be necessary to limit the scope of BES cyber systems. For example, it may need to be stated that only real time monitoring and alerting systems are in the scope since those can affect Grid operability. Also, following the logic in sections D and F, the steps for determining cyber systems in scope appear to be: 1) identify BES Essential Functions; 2) derive BES Subsystems (including BES **cyber** subsystems) using the list from step 1; 3) derive BES cyber systems from the step 2 list; 4) derive a list of Cyber systems supporting BES cyber systems. The proposed BES Cyber systems and supporting BES Cyber systems identification process significantly expands the number of cyber systems that may be affected by this guideline and hence by the NERC CIP requirements. Consideration should be given to using the TPL standards to identify what equipment is essential to supporting the BES Functions specified in this methodology and whose supporting systems should be considered BES Subsystems.
SOCO	Yes. It appears to cover them all. We understand the drafting team will next consider the degree to which these systems and subsystems will need to be protected.
E-ON	The methodology presented in Sections D and F is overly inclusive and appears to capture far more than those systems essential to insuring BES reliability
ATC	A cyber attack should not be tied to the NERC definition of an ALR. A cyber attack is a high impact low probability event and would be less probable than a NERC category D event. A category D event would not provide an ALR.
TAPS	See response to Questions 1 and 2.
GWA	Given the evolution of the industry it seems reasonable to assume that the list is not comprehensive, and that should be stated. One example of an omission is a Wide Area Measurement System (a BES Subsystem) that may evolve with the

	deployment of more synchrophasors in the Bulk Electric System. The document should be as comprehensive as possible, with an understanding that not every BES System and Subsystem can be included. The systems listed should serve as examples to allow other types of Subsystems and Cyber Systems to be identified by Registered Entities.
MISO	The methodologies are not clear what is being protected against and appear to assume because a cyber system supports a BES asset that it will need to be protected automatically. The purpose of a reliability standard is protect the BES not the associated cyber systems. Protecting the cyber systems often supports the main purpose but is not always necessary to protect the asset. As an example, most generators require a manual operator intervention to re-synchronize to the grid and startup once they have tripped off-line. Does the need for manual intervention, thus, obviate the need for protecting some of the associated cyber systems? Thus, these methodologies will likely identify more BES Subsystems and BES Cyber Systems that need to be protected than necessary to maintain a reliable grid. The drafting team should solicit for industry experts with field operation experience to assess to what level the actual BES asset could be compromised.
SCEG	Yes
RFC-CIP	Same as comment for Q2. Will entities have the flexibility to add Subsystems and Cyber Systems not already included in the Standard's lists as technology changes?
GEEI	The issue to be considered is if you have a small generating station but is Interconnected power system how do you identify BES Cyber systems even for a small system
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	The methodologies presented in Sections D and F do not capture all of the systems that will need to be protected since the Adequate Level Reliability criteria was not applied correctly. In Section F, the MRO NSRS agrees the full target of protection should be identified especially before considering other cyber system components; it's unclear what these other cyber system components would be since Section F introduces them but does not explain what these systems are.
MEC	Section D does not provide a clear methodology and creates a new concept of subsystem without subsystems definition or clarity. Section D points out there may be cyber systems that may perform or support the BES on a wide-area basis that may or may not be associated with any specific BES asset. The concept paper proposes categorizing these as both a BES

	Subsystem and a Cyber System creating confusion. A more direct, achievable methodology is to build on CIP-002 R3 where Cyber Assets essential to the operation of the Critical Assets are identified. Requirement 3's list of examples already include some cyber systems that are not associated with any specific BES asset alone but do support the BES on a broader scale. Refining these examples would achieve the objective of capturing the systems that need to be protected.
PSEG	Table One, Other section (Line 46-50) identifies "Support systems used to modify cyber systems" as BES subsystem and cyber system examples. This type of broad definition will again lead to the confusion and ambiguity currently associated with CIP-002, Version 1. The drafting team must be must more specific with descriptions such as these.
SCE	N/A – see comment to question 1.
AWEA	A more important question is "How will the BES reliability impact of a specific Subsystem be assessed?" Insufficient information of the assessment methodology is provided to judge any aspect of the process.
APPA	See discussion of the Functional Model above under Q1. The SDT should consider whether BES Functions can instead be derived from the purpose sections and associated Requirements of NERC's other Reliability Standards. Identification of BES Subsystems and Cyber systems could take place through the same process. The step that is new appears to be the reverse engineering to track the reliance of many diverse BES Systems on common use Cyber systems. It would appear that registered entities may need to perform this mapping of BES and Cyber systems in both directions, top-down and bottom-up.
PAC	Section D does not provide a clear methodology and creates a new concept of subsystem without definition or clarity of what subsystems are. Section D points out that there may be cyber systems that may perform or support the BES on a wide-area basis that may or may not be associated with any specific BES asset. The concept paper proposes categorizing these as both a BES Subsystem and a Cyber System. This creates confusion. A more direct, achievable methodology is to build on CIP-002 R3 where Cyber Assets that are essential to the operation of the Critical Assets are identified. Requirement 3's list of examples already include some cyber systems that are not associated with any specific BES asset alone but do support the BES on a broader scale. Refining these examples would achieve the objective of capturing the systems that need to be protected.
USBR	Page 15. No. The methodology would indentify elements that would not or may not have an impact on the BES. The list does not clarify that the impact the BES must be based on a factual assessment. Section F also now includes Alarm functions and

	Feeder Rating systems.
PGE	This methodology could inadvertently capture more than what is required to maintain BES ALR. It is unclear how the Regional Entity or NERC will hold entities accountable for the scope of BES Subsystems or Cyber Systems identified.
FPL	As stated in responses 1 and 2, we believe this methodology should provide guidelines and does need to capture all of the systems since this will be done in other standards such as the TPLs. Table 1 and the flow chart in figure 2 are very helpful. Section D is confusing in that it mixes topics i.e. subject heading is identification of BES subsystems yet also talks about cyber systems.
TECO	We would encourage the SDT to map these functions back to the NERC defined BES Reliability Functions and include operating staff in the review of these. Table 1 does seem to address all the systems we are aware of. Q1 and Q2 deal with functions. Our staff is not comfortable with the definitions of the functions and would like them to map back to the NERC definitions.

Question 4

4. Section E, Impact Mapping of BES Subsystems proposes that all identified BES subsystems be mapped into categories based on pre-defined criteria that reflect their impact on the reliability and operability of the BES. This mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach, and if not, what alternative suggestion do you have?

Name	Comment
CLPUD	Yes.
TNSK	As a Generator Owner and a Generator Operator we do not have the information required to classify events based on the proposed graduated impact scale. We would like to work with the Regional Coordinator to perform this impact analysis to support the goal of ALR.
XCEL	Yes
DOM	The Operating Reliability Event Categories cited as an example are based more on loss of entire BES systems (e.g., lines, generators, networks) and not necessarily subsystems. It is difficult to predict how this concept could then be used to prioritize the cyber systems that support critical BES subsystem infrastructure. Furthermore, as the categories increase in severity, the criteria are based more on the simultaneous loss of several components or systems. The existing CIP standards were not adequately designed to address multiple contingencies. If addressing multiple contingencies is now desired, the paper should address contingency levels for cyber component directly, rather than tying these to a BES subsystem ranking. It would be difficult to apply the mapping described to components that could be operating in several completely different time frames. An RTU, which has been used in several examples as an example of a critical cyber system, can operate to supply real time data acquisition and control and, at the same time, supply accumulator data for other functions. Furthermore the criticality of a component such as this will also vary from day to day, if not hour to hour, as load and exact system configurations change. Simply put, a mapping of high on a component one day could be seen as low on another day. It is not clear how this concept will be useful in establishing criteria for cyber system reliability
FMPA	See FMPA's responses to Questions 1 and 2. FMPA believes categorizing threats is a more appropriate approach than defining new terms such as BES Reliability Functions and BES Subsystems. However, FMPA does agree that the threats ought to be measured against pre-defined criteria that measures the possibility of malicious control of a cyber system causing

	"instability, uncontrolled separation, or cascading failure". For instance, the threat of loss of supply could be measured against the Contingency Reserves of the Reserve Sharing Group, or against the largest single loss of source in a region, as a measure of the threat of "instability, uncontrolled separation, or cascading failure".
SWPA	Yes, at a high level we agree with this approach. However, we need to know what the "pre-defined criteria" are. The NERC Guideline for the Electric Sector - Identifying Critical Assets has already given us "pre-defined" criteria to follow when identifying assets that are critical to BES reliability. Let's first prove that the current efforts are not effective or NERC should simply tell us what systems are critical and take the guess work out of it. The industry is spending a lot of valuable resources chasing this moving target. Without any details it appears that this approach will force all registered entities regardless of size or location to identify all of their BES systems and then be responsible for documenting a certain level of protection on all of these systems again. While we do agree that it is in our own best interest to secure all of our cyber systems, we do not agree that they all should be monitored for compliance to mandatory standards and financial penalties. This approach is not consistent with other reliability standards such as FAC-003 Transmission Vegetation Management Program and PRC-023 Transmission Relay Loadability. These standards only apply to facilities above 200 kV or those that are identified as critical to BES reliability. They don't require a minimum level of requirements on all facilities and these standards are assigned "High" VRFs, while most of the CIPs are all "Low" to "Medium" VRFs. If the CIP Standards are allowed to reach into low-voltage systems that control water heaters, how can we ignore vegetation management on distribution lines where local reliability issues are proven?
GTC	GTC agrees with this approach and believes that mapping using pre-defined criteria should significantly reduce the effort and controversy involved in categorizing BES subsystems over a "define-it-yourself" methodology. However, gaining consensus on the pre-defined criteria will be a considerable undertaking.
DYONYX	We are very concerned by the "to be defined" "pre-defined criteria" in assessing the level of impact.
BPA	For the most part we agree with this approach. Our suggestion is to add to the existing options of High, Medium and Low impact a 4th option – <u>Non-applicable</u>. There needs to be a way to identify systems that have zero impact on the BES and a Non-applicable option would meet that need. – Bulk power system event classification? – What is the local impact – High med low are subjective. What do these mean to us? – Regions should figure out what is high impact for their areas. Page 16, lines 10-20, what are they trying to say here?

SDGE	It seems like a good approach, but will ultimately depend on the pre-defined criteria and the categorization levels that are identified.
GSOC	The approach is realistic but reaching agreement on pre-defined criteria may take some time and considerable discussion. The big concern is how some of the entities will be able to determine the mapping for their facilities. For example some of the IPPs and smaller Utilities do not have the capability to determine the impact of their facility on the BES, other than some of the obvious items, such as they are a blackstart facility included in the regional blackstart plan or the facility is greater than the BA Contingency Reserve allocation. They do not have the ability to conduct power flow and contingency analysis studies. The RC should be the responsible entity to determine the impact of the assets within their RC footprint and categorize them into high, medium and low. It is the RC who has overall responsibility for reliability. In some regions the RC conducts the studies and informs the registered entity which of their facilities is a Critical Asset. Under this new suggested BES mapping the RC should determine the asset mapping into high, medium or low.
CUSMO	Yes, at a high level we agree with this approach. However, we need to know what the "pre-defined criteria" are. The NERC Guideline for the Electric Sector - Identifying Critical Assets has already given us "pre-defined" criteria to follow when identifying assets that are critical to BES reliability. Let's first prove that the current efforts are not effective or NERC should simply tell us what systems are critical and take the guess work out of it. The industry is spending a lot of valuable resources chasing this moving target. Without any details it appears that this approach will force all registered entities regardless of size or location to identify all of their BES systems and then be responsible for documenting a certain level of protection on all of these systems again. While we do agree that it is in our own best interest to secure all of our cyber systems, we do not agree that they all should be monitored for compliance to mandatory standards and financial penalties. This approach is not consistent with other reliability standards such as FAC-003 Transmission Vegetation Management Program and PRC-023 Transmission Relay Loadability. These standards only apply to facilities above 200 kV or those that are identified as critical to BES reliability. They don't require a minimum level of requirements on all facilities and these standards are assigned "High" VRFs, while most of the CIPs are all "Low" to "Medium" VRFs. If the CIP Standards are allowed to reach into low-voltage systems that control water heaters, how can we ignore vegetation management on distribution lines where local reliability issues are proven?
MH	Alternative 1: If the impact mapping of BES Subsystems is based on very prescriptive criteria which provides minimal flexibility for the individual entity to categorize their BES assets then the revised CIP Standard should not include the procedure outlined in the concept paper; rather the revised CIP Standard should just document the criteria table for industry to use to assign the BES impact. The concept for categorizing cyber assets would be used by the team to develop the appropriate table(s). This simple approach would avoid industry investing effort in low value activities such as documentation.

	Alternative 2: If the impact mapping of BES Subsystems provides sufficient flexibility for individual Responsible Entities to properly evaluate the impact of their BES assets, then they can determine the appropriate BES Subsystem categorization. Responsible Entities would need to document their processes, assumptions and considerations. Examples: Redundant assets might be categorized lower due to redundancy than if only a single asset exists, or for AGC, the master end might be evaluated higher than the plant controllers or individual unit controllers based on MW impact. Manitoba Hydro favours this approach provided that there is value in more appropriate application of security controls by having performed the additional analysis. For either alternative, consideration should be given for the followings issues: – All components in a BES Subsystem should not automatically inherit the categorization of the overall BES subsystem. If many units are part of the BES subsystem, then the assessed impact could be Minimal (very low) for an individual unit. Redundancy (often mandated by other reliability standards) should be considered by individual Responsible Entities as part of their consideration and it may reduce the impact of an individual BES asset. Master ends of BES subsystems may be categorized higher than individual remote ends of BES Subsystems. – Responsible Entities should be allowed flexibility to properly determine the range of impacts and the resulting categorization of the BES assets. Provision for this flexibility should be provided in the overall procedure for BES subsystem categorization. – Any impacts for any common mode failure of cyber subsystems should be addressed in the categorization of cyber systems. Consideration should be given for a BES subsystem categorization level where no mandated security controls are required (Level for None).
NST	We are concerned that both defining and applying a comprehensive set of pre-defined criteria intended to facilitate a lookup-based categorization of BES Subsystems could prove a daunting and time-consuming task. Further, we believe it may not be either appropriate or desirable to essentially remove local entities' engineering expertise and judgment from the process of evaluating a given BES Subsystem's impact on BES reliability or operability. However, at the same time we support the goal of defining and applying an industry-wide set of metrics for BES Subsystem categorization, as it should result in a more consistent set of results with fewer regional and entity-specific differences in how BES assets are assessed for criticality than seems to be the case under the current version of CIP-002. Our recommendation is to conduct several trials of the proposed function and criteria-based categorization of BES Subsystems once an initial draft set of criteria has been completed. Trials should be conducted among different size companies, in multiple regions, with non-binding results, to gain a sense of whether the proposed methodology yields the type of results anticipated by the SDT.

Question 4

NPCC	Agree with this approach.
RFC	We agree.
IRC	Agree with approach. Comments for Section D above are also applicable here.
AEP	Performing pre-mapping and applying generic predetermined "risk assessment" can be inefficient and may result in undesired outcomes. This could contribute to either over or under securing individual systems. We would be better served by enhancing the current base of cyber security standards in order to increase clarity.
MGE	No. The "pre-defined criteria" has not been defined by the SDT and this question cannot be answered. The BES Subsystem is a subset of all programmable electronic devices (to include communication networks) that has had a process applied to it (methodology) and has been determined to require additional electronic protection against a possible malicious attack that could disrupt that programmable device that effects the BES.
WE	Wisconsin Electric does not agree with this approach based on the removal of a risk based analysis of the asset/system using probability of occurrence. We also feel this approach would add more interpretation issues as well as audit complexity. We would prefer to utilize current methodology as defined in CIP 002-1 with further refinement of the risk based methodology. If the proposed approach is used, there should be a reduced set of standard requirements for CIP that need to be complied with. As an example, Wisconsin Electric would not agree with an approach to require full compliance to all CIP standard requirements but have a lower violation severity level for non compliance due to the lower impact on reliability of the subsystem. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	As long as the scope is clear, the differentiation between the controls on the different levels are significant, the criteria are clear and correct and the number of levels are appropriate, the concept itself is sound. However, it is difficult with the information provided to assess whether this can be implemented correctly.
SOCO	No. As noted by FERC in Order 706 (Paragraph 111), "flexibility and discretion are essential in implementing the CIP Reliability Standards" and "implementing those Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand." FERC further noted in the same paragraph that "[c]yber security problems do not lend themselves to one-size-fits-all solutions." Based on these same principles set forth by FERC, NERC should consider not adopting pre-defined static criteria for mapping the impact of BES subsystems. Rather, NERC should

	provide criteria that would be applied unless the responsible entity documents through a sound engineering study that such BES subsystem should be placed within another category.
E-ON	E.ON U.S. does not agree. E. ON U.S. suggests BES subsystems be defined as systems the failure of which would lead to instability, uncontrolled separation, or cascading failures of the BES or impede restoration of BES operation
ATC	ATC does not agree with this approach because the team has removed the ability to determine the probability and severity of an event's occurrence. We agree that entities need to understand the impact of an event but that the likelihood of that event needs to be included in the equation. The failure to include the probability of the event will result in a drastic increase in cost with no meaningful benefits to the reliability of the BES. ATC also believes that the paper needs to provide more information as to why this approach is being proposed and the improvements over the existing process. We believe that these changes were not directed by FERC nor are they needed to address other aspects of Order 706.
TAPS	See response to Questions 1 and 2.
GWA	GWA members support an approach that considers reliability impacts of BES subsystems, pending review of the actual criteria once they have been defined. (see p. 16)
MISO	A BES subsystem either supports reliability or it does not. It seems that the current Critical Asset and non-Critical Asset approach would still be fitting.
SCEG	Yes
RFC-CIP	It seems to be consistent with the approach used for determining the degree of impact applied to Cyber Systems. Section E suggests categorizing event impact as High, Medium, and Low. It also suggests using criteria similar to NERC's Bulk Power Event Classification Scale which for Operating Reliability Events uses five categories. The drafting team should consider mapping the five categories to High, Medium, and Low. Implementing five impact categories would be unmanageable and not provide an improved security model.

Question 4

GEEI	Yes, in theory. In practice, a similar function does not imply the same level of impact. Whether due to other mitigating automatic or manual controls, the loss of a function in one BES subsystem at one facility may not have the same level of impact on reliability as the loss of the same function in a similar BES subsystem at another facility.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	No. It is unclear what value would be added by having multiple classifications. FERC Order 672 says that standards should be clear and unambiguous.
MEC	No. MidAmerican is concerned with the complexity in mapping to the categories proposed. The proposed concept does not provide more clarity than providing more specific criteria for Critical Asset selection under the current approach in the standards. More specific details would be required under any approach. It will be more productive to add clarity and specificity to the current standard.
MMPA	The approach is good as long as the "pre-defined criteria" is appropriately gauged. If the criteria is set too low it will encompasses assets that do not impact the BES. If it is set too high, than it may miss assets that could impact the BES.
SCE	N/A – see comment to question 1.
AWEA	The "pre-defined criteria that reflect their impact on the reliability and operability of the BES" are critical. Without knowing what the criteria will be, it is of limited use to judge the process. One concern is that the comprehensive/bottom-up process outlined in the paper may devote too much attention to smaller-scale components of the power system that, due in part to their small size, would be extremely unlikely to affect the reliability of the bulk power system. Some type of initial screening process that excludes generators and other grid components that fall below a certain size/importance threshold and thus are unlikely to affect grid reliability would be a useful step to ensure that the scarce resources available for securing the grid are devoted to steps that will yield the most benefits. Variable generators may also merit exclusion since they are typically treated as providing little or no capacity value to the power system. Taken literally, the guidance in this document would require that virtually all generating units, even small, variable resources like wind and run-of-river hydro, etc., be designated as "critical assets." Since these units, no matter how small or non-dispatchable, can be started in 15 minutes or less and can result in some amount of underfrequency if they are taken out of service unexpectedly, they would fall under the criteria specified under the reliability functions "Contingency Reserve/Peakers" and "Load Balancing, Frequency Response/Support." But these criteria are not consistent with power industry practice or

	needs. During a generation shortfall, what is needed is firm dispatchable capacity. An intermittent resource, like wind, that provides only energy and is incapable of being dispatched or committed at any specific output level, should not be considered a critical resource. With respect to generation, we think the characterization of "critical asset" should be based principally on committable and dispatchable capacity that can be exercised by the generation asset. A reasonable lower limit (e.g. a certain and relatively high number of MW of committable dispatchable capacity) should be used to make that designation. Wind assets obviously should be put in a different category than a dispatchable combined cycle or coal unit of similar maximum output.
APPA	See response to Q3.
PAC	No. PacifiCorp is concerned that the process of applying the pre-defined criteria to the BES subsystems will only add additional confusion to the industry and may introduce opportunity for a number of different interpretations by responsible entities. PacifiCorp also feels that finding agreement between the industry and the drafting team on acceptable criteria will be difficult and may delay needed revisions to the current standards. PacifiCorp feels it would be more productive to add clarity and specificity to the current standards. It should be noted that a similar impact mapping process could be used within the current methodology by first identifying the BES critical facilities, identifying the critical cyber systems supporting that facility, and then accessing the impact of that system based upon the impact to that facility and the probability of an occurrence of a security event.
USBR	No, the mapping is already needed as part of the existing version of the CIP standards. An alternative is not needed.
PGE	It is difficult to comment on the impact of this approach without knowing anything about the "pre-defined criteria." The specificity and clarity of those criteria will be critical to this approach.
FPL	Although we agree with the general approach, we believe additional language should be provided regarding risk assessments and definitions of threat basis. It is important that any pre-defined criteria are not overly restrictive since it will depend on the different systems of each company and varying situations across the regions.
TECO	We are concerned that the criteria for the definitions must be clear, simple, and not subject to interpretation.

Question 5

5. Section E, Impact Mapping of BES Subsystems provides an example of three impact levels: High, Medium, and Low. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems, and why?

Name	Comment
CLPUD	No opinion.
TNSK	I would recommend 2 levels, especially if these translate to different hardening requirements to keep the implementation less confusing and manageable. Potential constraints or remedies for unregulated Generator Owner and Generator Operator non-utility entities should be considered.
Xcel	Additional level of "None" should be added as a fourth.
DOM	Based on having to evaluate every piece of equipment, 2 levels perhaps (high or low), is more appropriate.
FMPA	See FMPA's responses to Questions 1, 2 and 4. As FMPA explains in those responses, FMPA believes that "threats" ought to be mapped instead of BES Subsystems. FMPA also believes that only two levels are needed: 1) critical, and 2) non-critical, as was the original intent of the standard. FMPA believes that the FPA Section 215 definition of reliability ought to be used as the "yard-stick" to determine if a system is critical or non-critical. FMPA believes that a critical cyber system should be regulated by the standards and the measure for whether a system is critical or not is to determine through threat analysis if a cyber system can be maliciously used to cause "instability, uncontrolled separation, or cascading failure". All other cyber assets would be non-critical and not regulated by the standards.
SWPA	There needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current approach will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.
GTC	GTC believes that 3 levels are appropriate.

Question 5

DYONYX	We believe only two levels are needed as currently defined, Critical or Not-Critical.
BPA	4 Levels – High, Medium, Low and Non-applicable. See Comment #4
SDGE	I believe that 3-4 levels would be best for impact mapping. Any larger number of impact levels would probably be too confusing to implement.
GSOC	The main objective is to determine the impact the asset has on the reliability and operability of the BES, therefore, the three levels of impact is a good starting point. We do not see having any more levels, either the asset has an impact or it doesn't and having the three levels helps to establish the degree of the impact the asset has on the reliability and operability of the BES.
CUSMO	There needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current approach will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.
MH	Manitoba Hydro suggests a minimum of three (3) and a maximum of five (5) impact levels. Impact levels: High, Medium, and Low may not be sufficient for BES Subsystem impact categorization; however, too many levels could be confusing and difficult to implement. All components of a BES Subsystem should not necessarily inherit the BES subsystem impact level. Individual components of the BES Subsystem may require a lower impact level; therefore, an additional impact level may be required (four (4) levels). Consideration should be given for a BES subsystem categorization level where no mandated security controls are required (Level 5 Negligible, Minimal or Very Low). If this additional level is not available for BES components, then all BES Subsystem components will inherit the higher impact which may lead to inappropriate application of security controls. All common mode impact introduced by interconnecting cyber assets should be addressed by the target of protection and cyber impact analysis.
NST	We believe three impact levels is an appropriate number, as it reflects a recognition there are differences among BES Subsystems in terms of their relative importance to reliability and/or operability, and that it is appropriate to then account for these relative differences when establishing a set of required security controls for associated Cyber Systems.

	We also consider three to be an appropriate number of levels by virtue of the fact that FIPS Pub 199 the NIST risk management framework, both referenced by the concept paper, are based on the use of three-level information and information system categorizations. At the same time, we believe three is the maximum number of levels that should be defined, as using more levels would in our opinion add considerable complexity to the categorization process without a commensurate improvement in cyber security.
NPCC	We suggest a fourth level, which addresses the highest of the High. We suggest "Critical" for this fourth level.
RFC	We agree with three levels.
IRC	Support the current concept of High/Med/Low as depicted in the concept paper.
AEP	Without the benefit of seeing how the impact levels affect the controls, it is difficult to determine how the granularity would be applied. Application of cyber controls on graduated levels may result in increased uncertainty as to what controls apply; what will an auditor judge vs. our opinion? This is difficult enough currently with basically a binary decision system. However, a graduated approach is a good concept if the scope was focused on "essential" systems and not every system directly or indirectly associated with the BES operations. If a graduated approach is utilized, there should be a choice for "no impact."
MGE	The BES Subsystem is a subset of all programmable electronic devices (to include communication networks) that has had a process applied to it (methodology) and has been determined to require additional electronic protection against a possible malicious attack that could disrupt that programmable device that effects the BES. There should be two levels, critical and non critical. The SDT assumes that all BES Subsystems have an impact on the BES. As in the presently written CIP-002-1 methodology, a system is set up to see if an item is critical or not. This is not present in this concept paper. An example might be a 15MVA generator connected at the Distribution level, connected to SCADA/EMS and not blackstart capable. This concept paper would probably say it is in the "Low" impact category. Why? Because the Concept Paper (SDT) assumes it should be. There may be items that don't fall within this BES Subset and would be placed in the "non critical" category.
WE	Wisconsin Electric feels an additional level of "no impact to the BES" should be defined. Wisconsin Electric also supports comments submitted by EEI on this subject.

Question 5

DUKE	No. Another level is needed for subsystems that would have a negligible impact on the reliability or operability of the BES. While these subsystems would need to be reviewed and evaluated, and may theoretically have an impact on the BES, that impact and the probability may be so small that the resources should be applied elsewhere.
SOCO	A fourth level of none or not-applicable is needed for cyber items that are in the Target of Protection but have an insignificant impact on the operability of BES Cyber Systems or the reliability of the Bulk Electric System. As an alternative, because the definitions for medium and low levels are very similar, NERC should consider combining the medium and low levels and having the following three levels: High, Low, Not Applicable.
E-ON	One. Medium and low risks are irrelevant. Only cyber systems the loss of which could lead to instability, uncontrolled separation, or cascading failures of the BES, or impair the ability to restore BES operation, are relevant
ATC	ATC does not object to the categorization of "High", "Medium" and "Low" but that entities must be allowed to consider the probability of an event. In addition entities must be able to consider their security practices along with their current cyber and physical protection investments. If this approach is to be implemented then we believe that either a fourth category should be added that would represent "no" impact on the BES or that the group follows the five event categories currently used by NERC. (Event categories 1-5) ATC also believes that the SDT should identify the potential cyber and physical protection that will be assigned to each category ("High, "Medium" and "Low").
OMPA	OMPA agrees there should be the availability of levels or degrees of impact rather than a one-size fits all; however, OMPA believes that an option of "no impact" should be identified in the impact mapping process. Is this assumed that if the process, equipment or facility has no impact that it is simply not listed? Risk is typically determined by looking at both probability and impact. OMPA recommends the addition of "probability" in the process vs. looking only at the "impact" or severity of the event or occurrence. This assists an entity with prioritizing the processes, equipment, facilities, systems that resources will be assigned such that they are consistent with the overall risk to the BES.
TAPS	The Concept Paper's proposed mapping of BES subsystems for high, medium, and low impacts incorrectly assumes that the cyber systems supporting each such BES subsystem has an impact on reliable operation of the BES that merits some (albeit low n the case of low impact systems) level of regulation of cyber security protection. TAPS believes a fourth category of minimal impact, *not* meriting regulation by mandatory cyber protection standards, should be added. Alternatively, in light of the

Concept Paper's acknowledgement that "low impact" means that "the loss of confidentiality, integrity, or availability would not be expected to affect the BES Functions it supports" (page 19, lines 31-32), it should be clarified that BES subsystems with a "low" impact should not be subjected to regulation of cyber protection. Imposition of even limited regulation of cyber protection would impose unjustified burdens from a registered entity compliance and Regional Entity monitoring perspective.

As described at page 15 of the Concept Paper, this assessment "is based on their impact on the reliability or operability of the BES, as defined by the characteristics of an ALR." As demonstrated in response to Question 1, this ALR-based test is over-inclusive and goes far beyond Section 215's purpose for reliability standards, including those for cyber security, as necessary for "reliable operations" –avoiding instability, uncontrolled separation, and cascading outages. See FPA Section 215(a)(3) and (4). Thus, TAPS' comments (in response to Question 1) about narrowing the focus consistent with the statutory security-focused directive apply to assessing impacts. There are many BES facilities and supporting cyber systems the sudden disturbance (due to cyber attack or otherwise) of which would have little or no impact on avoiding instability, uncontrolled separation, and cascading outages, and which should therefore be excluded from the scope of cyber-security protection requirements. Therefore, TAPS alternatively proposes a simpler two-tiered approach focused on the definition of reliability in FPA Section 215, based not on BES Subsystems, but on cyber systems themselves. Tier 1 would be regulated by the standards and would be directed at fortifying the cyber systems that, if maliciously used, could cause instability, uncontrolled separation, and cascading outages. Tier 2 would be all other cyber systems which would not be regulated by the standard, because their malicious use could not result in instability, uncontrolled separation, or cascading outages. This, we believe, was the original intent of the standard, to regulate the cyber security of "critical" cyber systems.

Especially if NERC adheres to the inappropriate use of the ALR test for identification of BES Functions and BES Subsystems, it will be sweeping in nearly all BES facilities and the cyber systems that support them, even if they have minimal or no impact on BES reliability or security—*i.e.*, avoiding instability, uncontrolled separation, and cascading outages—if subject to a cyber attack. An additional category of "minimal" should be added to capture those cyber security assets that do not need to be covered by any NERC cyber standard, *e.g.*, the RTU communicating between a 20 MW gas turbine generator and a small utility that operates it. In particular, a cyber system that receives information but does not communicate information to those controlling the grid and does not control the operation of BES generation or transmission certainly does not need to be regulated by NERC cyber standards. Treating such a cyber system as "low impact" and apparently meriting some regulation of cyber protection would needlessly saddle consumers with unnecessary costs of regulation of cyber protection systems, and burden Regional Entities with unnecessary compliance monitoring, without in any way advancing the objective of making our grid better protected against cyber attacks, much less those that could cause the instability, uncontrolled separation, and cascading outages at which Section 215 expressly intended reliability standards to be directed.

Further, cyber security assets supporting BES assets that have a minimal, if any, impact on security should not be deemed to have even a low impact for cyber purposes just because they communicate with cyber systems that *are* important to protect the grid against cascading outage, separation, or instability in the event of a cyber attack. As discussed above, with reference to the online banking example, what is key is protecting from cyber attack the systems that matter from a system security perspective, rather than putting armor on every computer that interfaces with such cyber systems or otherwise has any contribution to keeping the lights on anywhere. The Concept Paper seems to recognize that issue (Page 29, line 25) without

	defining the "Alpha" and "Beta" companies and thereby clearly making it the responsibility of the utilities with cyber systems critical to maintaining system security (*i.e.*, avoiding instability, uncontrolled separation, and cascading outages) to mitigate the impact of interconnection with others.
GWA	Three levels of impact may be sufficient. It is important to have a well-documented process and criteria for determining whether impact is High, Medium, of Low. Otherwise, this approach will lead to confusion and inconsistent application. (See further comments in next question.)
MISO	From the wording of the Medium and Low impact descriptions, it appears these categories have little or no impact on BES reliability. Thus, two categories seem appropriate: critical and non-critical.
SCEG	We believe the concept of three levels is sufficient with the push towards NIST standards the HIGH, MEDIUM, and LOW levels would be easily integrated. SP-800-53 and FIPS 199
RFC-CIP	An Impact Level designation should be considered for the impact potential that is introduced when Subsystems and Cyber Systems used for testing, trouble shooting, and maintenance are used.
GEEI	Three is sufficient, assuming that there is not an exponential increase in cost/complexity when moving form Medium to High. Based on the reading of this document, there are more opportunities for a BES subsystem to be classified as "High" than any other ratings. If the application of security controls does not follow a roughly linear progression through Low to Medium to High, then there is little value. This will depend on what the required controls from the library of controls looks like when they are applied to each impact level. If every impact level results in the application of the same set of controls, then there is little value having the impact levels determine the controls. For example, if when mapping, it starts to look like this: Low: Password Protected, Logging, Periodic Audits Medium: Password Protected, Logging, Periodic Audits High: Password Protected, Logging, Periodic Audits, Intrusion Detection If the controls are the same, there is no need to define the different levels. It devolves into the same binary "critical/not critical" that exists today.

LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	There is not enough description for the impact levels ("high", "medium", or "low") for the MRO NSRS to make a judgment on whether it's appropriate or not. No matter what categories are developed there should be a category with a clear distinction between assets that are considered critical or not. With the implication that the facilities deemed critical will receive a prescribed level of security. MRO NSRS believes the existing two classifications are sufficient - critical or non-critical.
MEC	Two classifications, critical and non-critical, are adequate. Additional levels would only add complexity. If an additional level is necessary, it would be to add a "no impact" level.
PSEG	High, Medium, and Low are appropriate levels
MMPA	As written the level of impact appears to assume that everything has the potential to impact the BES. Either the "pre-defined criteria" needs to ensure that systems which would not impact the BES are exempt from unnecessary security measures or the levels of impact need to include a level below "low" such as minimal.
SCE	N/A – see comment to question 1.
APPA	There should be an additional "de minimus" category for BES Subsystems that are so small or localized in impact that they effectively cannot contribute to a cascading outage unless there is a common mode fault affecting hundreds of such facilities. See discussion under Q6.
PAC	While PacifiCorp has concerns with the drafting team's concept of Impact Mapping it does feel that three impact levels are sufficient. Additional levels would only add confusion.
USBR	No. The text does provide sufficient clarity on the exact determination of the level. The mapping must be clear in order to be measurable. The impact determination needs to also be repeatable. It is not clear what value grading the impacts will have other than for creating severity levels.
BRAZOS	The impact levels should also include a Critical level (above High) and a None level (below Low).

Question 5

FPL	We believe that it's not the number of impact levels that's important, but rather how they are defined. In the example provided, high, medium, and low impact levels should be clearly defined. Once the definitions are provided, each entity will be able to consistently apply it in their risk assessment.

Question 6

6. Section E, Impact Mapping of BES Subsystems: Do you prefer discrete thresholds or performance based criteria for mapping the BES subsystems (e.g. MW values as opposed to percentage of total generation)?. Please explain.

Name	Comment
CLPUD	Discrete thresholds.
TNSK	Whichever method best supports the reliability of the BES is preferred. We could use percentage of total generation, but the total generation data would have to come real time from the Regional Coordinator to the Generator Owner / Generator Operator.
XCEL	Performance-based metrics are preferred as they will allow entities to evaluate assets with respect to their regional control areas
DOM	It needs to be more performance based to allow for operational differences within the regions. (Percentage of total generation is also a discrete threshold.)
FMPA	See FMPA's responses to Questions 1, 2, 4 and 5. FMPA believes that discrete thresholds are appropriate, and not percentages. The purpose of the standards as laid out in FPA Section 215 is to avoid "instability, uncontrolled separation, or cascading failure". Therefore, threats (which as described previously, FMPA believes is a more appropriate concept than BES subsystems) ought to be measured against the ability to cause "instability, uncontrolled separation, or cascading failure". Using a loss of demand threat as an example, loss of 20% of a 20,000 MW utility is a serious threat, loss of 20% of a 50 MW utility is not; hence, a discrete number such as loss of demand equal to the Contingency Reserve or equal to the largest loss of source may be appropriate.
SWPA	We prefer a combination of both. Due to the complex nature of the BES it will be difficult to apply a threshold on a continent wide basis. This is not a "one size fits all" approach; it depends on how it is configured. Each region should already have engineering based planning and operational processes in place to identify how the loss of a BES facility impacts the region. So let the regions use their information and experience to decide what the criteria should be.

Question 6

GTC	GTC prefers discrete thresholds for mapping BES subsystems. This method places the resources and investment in meeting the CIP standards on the protection of the systems rather than on the justification of the impact of the asset itself. This method is also straightforward to audit and reduces confusion. Another benefit of discrete thresholds is that assets do not dynamically change impact levels and entities can plan for the protection of systems based on their design.
DYONYX	This approach will create a mountain of clarifications, exceptions, and a complex array of decision making criteria that will be extremely difficult to resolve, design, implement and audit. Why are we creating this complex process, scales, etc. just to come down to a Low, Medium, and High concept based on a "business systems" perspective? The categorization process will become so complex that it will be difficult to determine and audit.
BPA	More clarification needed, especially on what is meant by performance based criteria. Because BPA deals more with transmission than generation, we would like clarification on how this question would apply. BPA prefers performance based criteria because discrete thresholds don't work for all conditions. For example the BES definition of everything 100kV and above. There may be some 100kV systems that are very important to the interconnected system but they are few and far between, so having a performance based criteria that allowed for indentifying the important ones instead of a blanket threshold would actually increase reliability because we could focus on a subset instead of everything. Casting a larger net only catches more fish if you are fishing where there are fish. Page 16, lines 20-25, "work in defining the detailed criteria and categorization levels for mapping of BES subsystems is underway by another Standards Drafting Team subgroup with expertise in BES planning and operating areas" feels important to what the concepts paper is discussing, yet it is being developed separately REFERENCE page 17, line 40 "BES mapping process is required to determine the impact on the BES". How will the information be re-aligned with the separate development?
SDGE	I prefer discrete thresholds for mapping the BES system, because I think it is simpler in the long run. Wording such as 1) any generator over xxx MW, 2) if the frequency dips to xx.x Hz, or voltage drops to x.xx pu are easier to understand without having to go through calculations or a conversion process.
GSOC	We feel that discrete thresholds are better than performance based criteria for mapping the BES subsystems. When conducting contingency analysis studies to determine the impact of an asset, the contingency analysis will establish the amount of MWs, if lost that would affect the reliability of the BES for various system conditions (Loading levels, network configuration, etc). Therefore, discrete thresholds are a better measure to determine the impact than performance based criteria. Another example a of discrete threshold is a generating asset exceeding the established BA Contingency Reserve allocation. Using performance based criteria could result in the asset flip flopping between being categorized as having a high

	impact under certain conditions and then not being categorized as a high impact but rather as a medium or low impact.
CUSMO	We prefer a combination of both. Due to the complex nature of the BES it will be difficult to apply a threshold on a continent wide basis. This is not a "one size fits all" approach; it depends on how it is configured. Each region should already have engineering based planning and operational processes in place to identify how the loss of a BES facility impacts the region. So let the regions use their information and experience to decide what the criteria should be.
MH	MW highly preferred. If using percentages, users will always be converting to MW for clarification. With MW, each user can more easily determine priority importance of concerns competing for time and/or resources for mitigation. However, performance based criteria would assist to compensate for significant variation between regions. Any performance based criteria must be readily available to the individual Responsible Entity.
NST	We are not power engineers and therefore have no specific preference. However, our experience with industry clients suggests it might be appropriate to build some flexibility into defined criteria by defining multiple sets of metrics in some cases (e.g., "If MW" ≥ 'X' – or – "Pct Total Generation" ≥ 'Y' Then,…).
NPCC	We prefer performance based because an impact based mapping of BES subsystems is superior to that of a threshold based because of a cost benefit reliability ratio. Protecting cyber assets in these BES subsystems based on MW value or some other threshold will potentially lead to unnecessary expenditures and little if any incremental benefit to securing some of these systems. The effect of compromising all BES subsystems should be assessed and documented and understood. Then an appropriate level of protection should be applied depending on the impact of the failure or compromise of that subsystem. To protect "everything" above some arbitrary threshold is not cost effective.
RFC	We prefer discrete MW values. Percentages, such as percentage of total generation could miss assets for smaller companies. Also, if percentages are based on dynamic numbers such as seasonal peak or actual generation, the determination of criticality becomes a constantly changing situation.
IRC	The criteria and thresholds should be based upon percentage values (%), not discrete values, to preclude changes necessary when the discrete values may no longer apply. There is also danger in specifying detailed technical security requirement specifications within Reliability Standards since the technology along with threats, vulnerabilities and risk are constantly moving and dynamic entities.

Question 6

AEP	Each company's assets, functions and cyber systems are different and arbitrarily setting generic thresholds or criteria may not be appropriate in all cases.
MGE	Examples of both would need to be given to the industry. Why not use both and allow the Applicable Entity to make that determination as part of the Version 3 CIP Standard. This would add to the paradigm shift that is upon us now. The Standard should not be so descriptive that we have one way to determine the Impact Mapping of BES Subsystems. The complexity of this methodology will give too much opportunity for interpretation by an Auditor. This would also allow presently identified Facilities that fall below the established criteria (sub-transmission) that do impact the BES to remain having additional protection to ensure the reliability of the BES.
WE	Depending on how the discrete thresholds or performance criteria are determined, Wisconsin Electric could work with either measurement. If thresholds are used, they should NOT be implemented on a unit basis. The responsible entity should define a fleet threshold based upon State Estimator Analysis, to ensure BES stability and reliability. Then let the responsible entity select what assets need to be selected as critical to meet this threshold. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	Performance based criteria – there are too many variables to define discrete thresholds.
SOCO	As noted in our response to Question 4, we believe that adopting pre-defined, one-size-fits-all criteria is inconsistent with FERC's recognition of the need for flexibility, which is necessary to allow for meaningful implementation. As a result, pre-defined static criteria should not be adopted for mapping BES subsystems. Provisions should be allowed for entities to make rational engineering evaluations in order to identify which facilities truly have a high, medium, or low impact on BES reliability. Failure to do so will result in significant increase in compliance costs to protect arbitrary systems and no actual improvement in reliability.
E-ON	Any thresholds should be based on impact upon BES reliability
ATC	We believe that any threshold developed by the SDT needs to be flexible enough to capture both the impact of the attack on that entity's assets along with the impact on the Bulk Electric System (BES). A small entity may not have any assets that impact the BES outside of its control but does have assets that if compromised have a severe consequence on their system. Knowing this will help any entity determine how to protect its system but only those that impact (Cause cascading or large area blackouts) the BES outside of its area should rise to the NERC compliance level.

	Any threshold developed has to identify the outage that needs to be studied. Does an entity have to look at single element outages, multiple outages or a single event that opens all breakers in an entity's system? ATC does not support a one size fits all approach if it sets predetermined levels based on a perceived impact. We suggest that the team look at the planning standards in order to get a better understanding of a study structure.
TAPS	See responses to Questions 1, 2 and 5. TAPS believes that there is a relatively simple threshold for mapping threats that can be caused by malicious use of cyber systems, and that is whether malicious control of the cyber system can cause "instability, uncontrolled separation, and cascading outages" as reliability is defined in the FPA Section 215. Making it more complicated is burdensome to registered entities and the Regional Entities. Additionally, making it more complicated and including non-critical cyber assets would distract attention from the truly critical cyber assets and extend the time required to conduct analyses to resolve problems that could actually impact BES reliability.
GWA	GWA believes that performance-based criteria would provide a more sound approach. The diversity of the asset makeup, load requirements, and system engineering in different parts of North America would mean that discreet thresholds, while easier to apply, would potentially have different consequences for different parts of the BES. Performance-based requirements should provide for a more consistent application across the BES.
MISO	Performance based criteria is always superior. Thresholds usually are selected arbitrarily and oftentimes are set low enough to include all impacting systems but as a result include many non-impacting systems. If an engineering analysis was performed and revealed an appropriate threshold that solved the issues above, this would be satisfactory.
SCEG	Performance based criteria better encompasses the entire BES and sets the same standard for all utilities regardless of their size. A percentage also better reflects each individual company's overall impact on the BES and will result in a more comprehensive impact mapping system-wide.
RFC-CIP	The example "percentage of total generation" could mean that the same BES Subsystem could have a different level of impact on any given day. This would make compliance and auditing extremely difficult therefore discrete levels are preferred. Note that NERC's Bulk Power Event Classification Scale uses discrete levels.
GEEI	Discrete thresholds are easier to manage, but will not scale over time or with facility changes. We would suggest using performance-based criteria. A minimum MW value can indicate a normal/abnormal system rather than percent base value as it can mean anything.

LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	It would appear to be appropriate to use a discrete level to be consistent with the existing NERC Operating Reliability Events Categories and the Statement of Compliance Registry Criteria Revision 5.0.
MEC	In general, discrete thresholds would be preferred since they are easier to apply and less prone to error.
MMPA	Discreet thresholds are more easily definable. Performance based thresholds would be overly difficult in identification, compliance, and auditing.
SCE	N/A – see comment to question 1.
AWEA	Clarity in criteria is important. Characteristics need to include more than just MW size or % of total generation. Capacity value or contribution to LOLE are important generator characteristics.
APPA	I would need to see a more concrete proposal before providing a single answer. Note that percentage of total generation should be a regional or large area-based criterion, since a small BA of 300 MW could lose a major percentage of its generation, e.g., 20% or 60 MW, with no measureable impact on reliable operation of the interconnection or the region. Conversely, loss of 10% of a large BA's generation due to a cyber-security event is much more likely to have a severe impact on reliable operations. There are other criteria that could be used as well, such as a. DHS Tier I, II, and III critical assets b. Current NERC standards and Requirements with high, medium and low Violation Risk Factors c. Standards associated with emergency versus normal operations or system operations versus planning d. IROLS and SOLS e. Facility Voltage (>300 kV, >200 kV, >100 kV, plus RE identified critical facilities) f. Entity or cyber-system span of control or impact (wide area versus local) The criteria above are illustrative and should not be read as a recommendation that the SDT adopt any one of them.

Question 6

PAC	While PacifiCorp has concerns with the drafting team's concept of Impact Mapping, PacifiCorp would prefer discreet thresholds versus performance based criteria as the later is very often open to interpretation. Discreet thresholds would reduce the confusion and debates within responsible entities over impact levels.
USBR	If specific threshold are needed then they need to be absolute and repeatable. Such a threshold would be specific to the system configuration rather than loading of any one resource or asset.
PGE	PGE believes that discrete thresholds that are developed by the Regional Entity and apply across the Interconnection would provide the most clarity and direction to individual registered entities.
BRAZOS	The discrete threshold approach may initially be a good starting point realizing some form of performance based criteria can be developed after some experience with the overall process.
FPL	Neither approach works perfectly. Discrete thresholds are difficult to determine with diverse areas yet strictly looking at percentage is not correct either. Determination should be by impact i.e. Causes loss of x amount of load, causes system instability, causes voltage collapse, etc. Otherwise, we believe that a performance-based criterion more clearly addresses threats to the system and ties better with other operational and planning standards. It is important to make a distinction of whether this is more cyber-focused rather than related to power systems.
TECO	Regardless of the two approaches (discrete thresholds or performance based criteria), this needs to take into consideration of the regional differences and overall regional impact within which an entity operations. The MW values, for example, need to be based on the regional area versus the entire country.

Question 7

7. Section G, Categorization of Cyber Systems describes how an entity determines the impact a specific cyber system has on its assigned BES reliability functions. Do you agree with this process as described in the concept paper? Please explain.

Name	Comment
CLPUD	No opinion.
TNSK	Yes I agree with this. The Regional Coordinator would have to explain the use and impact of the data exchange between the Generator Owners and Generator Operators as they relate to the BES Functions to determine the impact the systems have on BES reliability functions.
XCEL	We agree with the process, but there needs to be more definition on how cyber systems are mapped to BES reliability functions (the proposed functional impact that correlates to each BES subsystem). There will need to be some standardization for the meaning of each impact category (HIGH, MEDIUM LOW) so that entities will have a uniform approach to categorizing systems.
DOM	The concept is acceptable but its implementation could be difficult. For example, a state estimator ("SE") is required for situational awareness. Inputs to the SE are from SCADA RTUs. An abnormal network topology and loading could exist where the loss of a normally inconsequential RTU could cause the SE to not solve. What testing will be required to determine if the RTU is low, medium or high impact?
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6. As described in these responses, FMPA believes that a threat analysis ought to be done for each cyber asset to evaluate the magnitude of the threat.
SWPA	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of protection on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.

GTC	GTC agrees with this process with one caveat. Loss of confidentiality, integrity, and availability does not affect BES cyber systems in the same way that it affects information systems. For BES cyber systems, loss of availability and integrity are much more important than a loss of confidentiality. The categorization should reflect an appropriate weighting to these characteristics that are unique to the BES.
DYONYX	We agree that if one system has a "High" impact on one function and "Low" on another, the "High" classification should be applied. The problem is the broad level of definitions for the ALR, functions, and potentially the "to be defined" criteria. See comments for Question #1.
BPA	No. For example, even though the Asset Impact is High a supporting system may not have a high level of criticality. There needs to be options to assess the cyber impact based on high, medium, low and non-applicable no matter what the asset impact level is. Also, more clarification is needed on Figure 3. There needs to be more flexibility in assessing the cyber system's impact level. May conflict with current NERC functional model and reliability functions that we are registered for. Page 19, lines 15-25, how does this apply to cyber systems, how do Entities determine how many real-time energy controls lost or unavailable will result in a "loss or compromise to the function of the BES Subsystem it supports"? Page 19, line 40, how is security categorization being defined under this concept?
SDGE	The three categories of impact (high, medium, and low) as described seem like a good process. As mentioned above, I don't think you'd want much more than three or four different categories of impact, as it would get confusing and potentially difficult to implement due to the subtle differences between a large number of categories.
GSOC	The process as described is acceptable
CUSMO	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of protection on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.

MH	The categorization of cyber systems as written mixes impact (high and low impact) and probability (medium impact). This leads to a very confusing analysis. If the team continues to use a mix of impact and probability then more levels and better descriptions are required. Manitoba Hydro suggests that only impact be assessed using 3-4 levels. A 4 level may be required for "No Impact". Manitoba Hydro suggests that the same scale as BES subsystem and levels of impact be used for the cyber systems impact analysis. This method would make the any analysis and documentation much simpler. It would also readily accommodate integrating any common mode failures for cyber systems. Confidentiality should be removed from the impact categories or handled separately under the Target of Protection. Availability and integrity (compromise) can directly result in impact to the BES Subsystem; however, confidentiality of BES cyber systems data is normally not a concern and information about BES cyber assets on separate (collateral) cyber assets do not always require the same categorization as the BES cyber asset or subsystem. The current process would require that cyber assets used to protect confidentiality would be categorized the same as the BES Subsystem which may not lead to appropriate security controls.
NST	We do not agree with the proposal to require an entity to attempt to predict the degree of impact a BES Cyber System's loss or compromise might have on the BES reliability functions it performs or supports. We believe doing so would in many instances require the application of highly subjective judgments, thus introducing to the overall analysis a significant qualitative component that we believe the SDT is striving to avoid. Moreover, we believe that following the proposed approach would, when combined with the categorization of BES Subsystems, result in a methodology that is more complex than the one defined in the referenced FIPS-199 Standard. Under that standard, the categorization of an information system is tied directly to a previously performed categorization of the information it stores and/or processes (e.g., {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}). There is no requirement to, for example, predict the severity of impact on *information* integrity of a loss of information *system* integrity. As an alternative, we recommend that identified BES Cyber Systems be categorized based on the highest level categorization of BES Subsystems whose functions they perform or directly support. BES Cyber Systems would thus be categorized as High, Medium, or Low Impact, depending on whether their associated BES Subsystems were categorized as High, Medium, or Low. We believe this modification would simplify the overall Cyber System categorization process (it would eliminate the need for the "Final Categorization" step described in Section H) and would reduce the amount of subjective judgment required while still serving the overarching objective of protecting BES reliability and operability from cyber threats.
NPCC	Agree with section G in principle, but feel that more explanation on the use of Confidentiality – Integrity – Availability security concepts is needed.

RFC	We agree with the process in general, but have the following suggestions: a. The language must be consistent between the levels. For example, High says "...compromise of the integrity…" while Medium uses "operational integrity". b. No mention is made of misuse of a compromised system. While the CIA principles are a good basis for this discussion, they do not go far enough in considering impact of a compromised system. The impact of misuse, whether deliberate or accidental, should be a major factor in the determination of the impact of the cyber asset on reliable operation of the BES.
IRC	Yes. This section describes the activities as that of the Responsible Entity but the focus of this paper, itself, is that the interconnection between various systems and with other entities presents significant security risk. This is as true for the cyber assets as it is for the power lines. The very words listed in the Introduction support this view: "The Bulk Electric System is controlled (not the wires, transformers, relays, meters, etc…) but the highly interconnected, integrated into a single multi-state spanning machine, as vulnerable as its weakest component." The focus of the current CIP Standards is hardware focused—virtually all Critical Assets within the BES are pieces of hardware, generators and substation components and essential supporting cyber assets which are focused on specific hardware devices and components of the BES, not systems. The essential control systems needed for RC/BA/TOP functions are implied by the current CIP Standards but not specifically addressed other than from the hardware perspective. An Electric Sector organization, such as an ISO, which functions as RC/BA/TOP but which has no real hardware-based Critical Facilities or Assets has only the Control Center and it's supporting Data Center as CAs, which do not easily conform to the current risk-based approach for identifying Critical Assets. The updated standards must continue to meet the needs for owner/operators as well as for other entities such as the ISO/RTOs who have Control Centers and very large Data Centers (1500+ servers) along with the trained IT staff and system operators. As a natural corollary, our primary cyber assets are the software systems that support the Control Center operators; therefore, much of the requirements in the current CIP Standards do not apply or are distorted when applied to a fully functional data centric model. Since the subset of software centric Control Centers is a very small portion of the BES, it is recommended that an alternative approach would break out these security controls and use standard security models (ISO-27002, NIST SP 800-53 R3 or ISO pubs) to develop a security organization framework. In some instances these documents are insufficiently comprehensive to meet the ISO's needs (for example there is no NIST guideline for Windows 2003 or 2008) which could present gap in security management within the framework of the BES.
AEP	In Section G, the categorization of cyber system impacts identifies a categorization of 'low' if the loss ... 'would not be expected

	to affect the BES functions it supports.' We interpret this to mean that regardless of the BES functions supported, there is no concern with the loss of the supporting cyber systems. Yet in Section H, Table 2 shows in the bottom row, which corresponds to a cyber system impact of 'low', but with 'final categorizations' of H (high), M (medium), or L (low), depending on the impact mapping of the BES Subsystem. It seems logical that this bottom row would be all L (low). Otherwise, more extensive and costly cyber controls than necessary may be applied. AEP contends that this categorization process will be a significant administrative burden that will not yield corresponding benefits, and could divert staff from meaningful reliability and/or security duties.
MGE	No. Once again the BES Reliability Functions have yet to be determined.
WE	Wisconsin Electric could support the categorization process. There should be additional information or examples of what loss of confidentiality, integrity and availability is and how it impacts the BES subsystem for each category of impact. This concept can be confusing to the regional entity applying the matrix. There could be cyber systems that by themselves are critical to a process but not to the overall viability of the BES or systems supporting them. These systems should not be elevated to a high status because of this fact. Again, an asset based approach would make more sense. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	We do agree with the approach, but believe the process is not clearly enough defined. Section G does not explain how definitions of Asset Impact levels (High, Medium, Low) differ from definitions of Cyber Impact Levels of High, Medium and Low. It is not clear if Asset Impact is meant to represent a likelihood of occurrence (of availability and integrity loss) or actual impact of such occurrence. It is not clear what the difference between High and Medium is other than the word "unlikely", which is very subjective. It should also take into consideration an additional "negligible" category that was proposed in question 5. In addition, loss of confidentiality should not be included in the consideration of the impact – it should be limited to loss of integrity and availability.
SOCO	Yes, we agree with the concept along with the changes described herein.
E-ON	Medium and low risks are irrelevant. Only cyber systems the loss of which could lead to instability, uncontrolled separation, or cascading failures of the BES, or impair the ability to restore BES operation, matter. Introducing gradations of risk does nothing to lessen the compliance uncertainty that exists today and invites further uncertainty as to which set of requirements app

Question 7

ATC	ATC believes that this section needs some additional clarity. It's our understanding that entities will have to first identify the "High", "Medium" and "Low" Cyber Systems which form the center of protection in the Target of Protection figure (See Figure 6 Yellow area). Along side the center of protection are three different cyber system identifiers: "Interconnected Cyber Systems", "Infrastructure Cyber Systems" and Collateral Cyber Systems" (See Figure 6). So is the team proposing additional cyber and physical protection for each of the three different cyber systems and will they be the same no matter what the center of protection category? (Example: If you have a BES Cyber System that is "High" will the different cyber systems (aka: "Interconnected Cyber Systems", "Infrastructure Cyber Systems" and Collateral Cyber Systems") have the same compliance obligations as a BES Cyber System identified as "Low"?)
TAPS	See responses to Questions 1, 2 and 5.
GWA	In general, yes, but this is associated with question 5. If there are further gradations (more than 3), consider including as part of the impact criteria, factors such as recovery time (short, medium, long – with long being 24 hours or longer, medium being a range of hours, and short being minutes to ??); and availability of alternative approaches to support reliability if a system were compromised (e.g., manual controls).
MISO	We do not agree with the assessment. Medium and Low categories appear to describe impacts that may not impact the BES. If the BES is not impacted, the CIP standards should not apply to the Cyber System.
SCEG	General Comment: Nowhere in the document is a requirement for a Cyber Security Assessment Team? Level of knowledge to perform a valid assessment/analysis would require input from various disciplines for determination of the remaining Sections.
RFC-CIP	See comment for Q5. Impact category for equipment used on an intermittent bases (i.e. test equipment) should be considered.
GEEI	The process is agreed with, but in practical application this will not be a simple determination. Systems are dependent on each other, share data, and rely on the integrity of the overall data stream. If a downstream system is classified as "Low", but that downstream system feeds data to a system that is classified as "High", then the system has been inadequately protected. The paper recognizes this, and says that the downstream system must be classified as "High". To continue that reasoning, with system interdependence constantly increasing, this will eventually lead to all systems providing some piece of data that is fed to a "High" classified system, leading all downstream systems to inherit the "High" classification, which again, devolves into the same binary "critical/not-critical" that exists today.

Question 7

LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	There is not enough description for the impact levels ("high", "medium", or "low") for the MRO NSRS to make a judgment on whether it's appropriate or not. No matter what categories are developed there should be a category with a clear distinction between assets that are considered critical or not. With the implication that the facilities deemed critical will receive a prescribed level of security. MRO NSRS believes the existing two classifications are sufficient - critical or non-critical.
MEC	No. It is unclear what value is added by having multiple classifications versus a "critical" or "non-critical" approach. The standard should be kept as simple as possible to achieve the desired goal. CIP-002 R3.1 through R3.3 list the characteristics that qualify a Cyber Asset for identification as a Critical Cyber Asset. These characteristics address a threat based on the asset's cyber accessibility (routable protocol or dial up). The characteristics of routable protocol and dial up accessibility are missing in the concept paper. They are essential to determining the impact of a specific cyber asset or system on the BES and should be included.
SCE	N/A – see comment to question 1.
APPA	The approach appears to be conceptually sound, although the definitions appear without much prior discussion of the terms used in the definitions of High, Medium or Low, e.g., "High if the loss of confidentiality, integrity, or availability directly causes or contributes to the loss or compromise of the integrity or availability of the BES Function it supports." See discussion above and consider adding a de minimus impact category.
PAC	No. It is unclear what value is added by having multiple classifications versus a "critical" or "non-critical" approach. The standard should be kept as simple as possible to achieve the desired goal. CIP-002 R3.1 through R3.3 lists the characteristics that qualify a Cyber Asset for identification as a Critical Cyber Asset. These characteristics address if there is a threat based on the asset's cyber accessibility (routable protocol or dial up). The characteristics of routable protocol and dial up accessibility are missing in the concept paper. They are essential to determining the impact of a specific cyber asset or system on the BES and should be included.
USBR	No. The impacts described are very subjective. Most of the definitions as written can only be described through statistical analysis. Language such as "contribute" or "compromise" does not lend itself to factual assessment rather to judgment. The impact on the BES is best determined by the Registered entity based on function of the critical asset and its relation to the

	BES.
PGE	The categorization of cyber assets based on the impact of the system that they are involved in could lead to confusion if multiple assets of different impact levels are included within the same environment. Instead of having a clear line of demarcation for what is and is not under CIP control, as in the current framework, this approach presents an additional compliance and security risk as assets that are housed in the same physical environment are subject to very different sets of controls. This mixed environment could lead to avoidable human error because someone mishandles a system.
FPL	We agree with the methodology as it is based on impact, however, we believe that the process as described is not as well defined and can cause confusion resulting in unnecessary systems as being identified as critical when they do not have significant impact to the BES.
TECO	We agree in principle with the approach; however, we believe that the process to develop and maintain this list is going to be very complex and will take significant education, knowledge, and awareness to complete/maintain.

Question 8

8. Section H, Final Categorization of Cyber Systems Based on Overall Impact on the BES describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a cyber system has on the BES. Do you agree with this process described in the concept paper? Please explain.

Name	Comment
CLPUD	Central Lincoln sees no way a low impact asset could correspond to a high cyber impact on the related cyber asset. The reverse, however, might occur. Suggest removing the elements above the diagonal on Table 2.
TNSK	Yes, this is a good process.
XCEL	We agree with the overall approach, but there needs to be additional detail on the final categorization output (again, a standard approach to evaluating the overlap of asset and cyber impact) as well as allowances for a fourth category for cyber systems that have no impact ("NONE" or "N/A").
DOM	No. As another way to do an assessment, if the impact of a cyber system is high (that is, it supports a critical BES function), but the cyber risk is low (based on a probability of failure caused by an outside source), then we would propose the overall rating of the cyber system should be low. Low cyber system ratings would then require less constraints or less support. This follows what is understood to be one of the goals discussed on the 8/25/09 Webinar – put your resources and time on those cyber systems that have more of a chance of leading to failure. In Table 2, is the Asset Impact actually referring to the BES Subsystem Impact?
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6.
SWPA	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.

<table>
<tr><td>GTC</td><td>GTC agrees with this process, but does not concur with the sample categorization table included in Table 2 of section H. A high water mark of BES subsystem impact and cyber system impact does not accurately reflect the impact on reliability of the BES. A more appropriate table might look like the following:

<table>
<tr><td>Asset Impact →</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Cyber Impact:</td><td></td><td></td><td></td></tr>
<tr><td>High</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Medium</td><td>Medium</td><td>Medium</td><td>Low</td></tr>
<tr><td>Low</td><td>Low</td><td>Low</td><td>Low</td></tr>
</table>

If by definition, a Low Impact Cyber System is not expected to affect the BES Function it supports (p. 19 line 31), then it should not be required to be protected at a High due to its relation to a subsystem that may in fact have impact on the BES.</td></tr>
<tr><td>DYONYX</td><td>We do not believe the deterministic methodology defined in this document will provide a consistent approach. First, the basic broad definition of ALR is not applicable to the objective herein which leads to even more confusion in the defined functions and BES Subsystems. Can we not come up with a more definitive front end process when we are looking at categorization of systems associated with impacting the operation of the BES?</td></tr>
<tr><td>BPA</td><td>Not entirely. There needs to be more clarification on the high, medium and low classifications. What is a low example? Also, a Non-applicable option needs to be added that covers systems where no action is needed. As an example, how would a utility handle a high subsystem, with a high cyber system supporting it which has no interconnectivity whatsoever?

BPA does not agree with the examples in Table 2 of section H showing a high impact for all high cyber impacts. We think the asset impact should be the overriding categorization. Thus, a low asset impact would have a low impact even if the cyber impact was high.</td></tr>
<tr><td>SDGE</td><td>At first glance, the process described in the concept paper for Final Categorization seems okay. It's difficult to comment substantively on the process, however, because the example shown doesn't have any details behind it. You know what they say, the devil's in the details. Since Table 2 is not an actual table (per the note included), it does leave me a little confused as</td></tr>
</table>

	to what an actual table would look like.
GSOC	The process as described is acceptable
CUSMO	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.
MH	Manitoba Hydro does not agree with the example of overall impact on the BES. The table indicates that most cyber assets will require the same security controls associated with the HIGH category and few cyber assets will receive the LOW categorization. A mapping between impact categorization and security controls should be developed by first identifying all the necessary security control levels; then sample cyber assets should be mapped into the security controls and finally a representative table or mapping list should be documented. The security controls should provide for additional criteria such as layers of security protection including those outside the ESP or PSP, use of private communications or other private facilities with restricted access. All layers should not need to be as described in the current CIP Standards (i.e. 6 wall perimeter, etc.). Responsible Entities may have a significant investment in private communications and other security layers to improve reliability. Private communications and other layers of security should be allowed to provide part of the mandatory security; otherwise unintended consequences could result by discouraging private communications and additional layers of security controls.
NST	We believe this step can and should be eliminated by simplifying the Cyber System categorization process (see our response to Question 7, above).
NPCC	Agree with this process.
RFC	We agree. This approach would achieve the goal stated in section H of providing a more consistent approach than application of a risk-based methodology as presently required in CIP-002-1 and CIP-002-2.

IRC	Concur that pre-determined categorization of the cyber system should be based on both the impact mapping of the supported BES Subsystem and the impact of the cyber system on the BES function it supports. Some may argue that categorization should be exclusive, i.e., that High be only selected when both functions are high, not when either of the functions is high as proposed in the concept paper; however, we disagree and concur with the approach outlined in the concept paper.
AEP	Please refer to our comments in item 7.
MGE	There should be two levels, critical and non critical. The SDT assumes that all BES Subsystems have an impact on the BES. As in the presently written CIP-002-1 methodology, a system is set up to see if an item is critical or not. This is not present in this concept paper. An example might be a 15MVA generator connected at the Distribution level, connected to SCADA/EMS and not blackstart capable. This concept paper would probably say it is in the "Low" impact category. Why? Because the Concept Paper (SDT) assumes it should be. There may be items that don't fall within this BES Subset and would be placed in the "non critical" category.
WE	Wisconsin Electric feels that additional information around standards required for compliance based on categorization level (impact mapping) along with the type of cyber system considered should be provided before answering this question in the positive. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	There needs to be a more nuanced approach to assessing the impact – any high should not automatically be high. If asset impact is high and cyber impact is low, or asset impact is low and cyber impact is high, the categorization should be medium.
SOCO	Yes, we agree with the concept along with the changes described herein.
E-ON	This deterministic methodology in comparison to the risk methodology in place today appears to radically increase the number of facilities that will be subject to NERC CIP standards. This methodology will, at minimum, necessitate more time for affected entities to verify and, if necessary, implement CIP compliance verification at far more facilities than has been the case in the past. The current 6 to 12 month period is insufficient to accomplish this undertaking.
ATC	Table 2: Page 21 ATC does not agree with the table as proposed. We believe that if this table is to be used the lower of the Asset Impact and Cyber Impact ranking should be used to determine the BES Function. (Example: If a BES Subsystem has a "Low" Asset Impact, or no impact, event then there is no benefit to treat it exactly the same a BES Subsystem that has a "High" Asset

<table>
<tr><td></td><td>Impact just because of the Cyber Impact ranking. We believe that entities should not be expected to treat BES Functions that have little or no impact on the BES the same as BES Functions having a "High" impact because the cyber impact on the BES function. ATC does not see a reliability benefit in protecting BES Function the same if their impact on the BES is not identical. In addition if you have a BES Subsystem that is "High" but it has a cyber Impact of "Low" it should be rated "Low". The reason is that the cyber system identified as "Low" would have no affect on the BES Function so why expect the same level of protection on these different BES Functions.)

The SDT should adopt the following table if this effort is going to be pursued further:

<table>
<tr><td>Asset Impact ></td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Cyber Impact:</td><td></td><td></td><td></td></tr>
<tr><td>High</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Medium</td><td>Medium</td><td>Medium</td><td>Low</td></tr>
<tr><td>Low</td><td>Low</td><td>Low</td><td>Low</td></tr>
</table>

ATC believes that the designation of "High", "Medium" and "Low" could be replaced with a system more like the Categorization of Events (1-5) (Page 16 of the concept paper). Since the Categorization of Events was suggested as a possible input into the impact assessment if the 1-5 is not adopted, then how will the SDT place the events into the "High", "Medium" and "Low" categories. (What would be the process to move the 5 Categories of Events into the three categories suggested by the SDT?)

The SDT needs to present their thoughts on the compliance obligations for whatever categories they determine are appropriate. The determination of the compliance obligations for each category is the cornerstone to this whole effort and if not supported by the industry could result in a drastic delay in addressing actual FERC directives.

ATC believes that if this table is used additional compliance obligations should only be placed on BES Functions that fall into the "High" box. Medium and Low BES Functions could be identified but should not be subject to additional compliance obligations.</td></tr>
<tr><td>TAPS</td><td>See responses to Questions 1, 2 and 5.</td></tr>
<tr><td>GWA</td><td>Yes.</td></tr>
</table>

Question 8

MISO	The impact on the asset is all that matters. The purpose is to protect the BES. If a cyber system is compromised but has no impact on the BES that cyber system is not even relevant to reliability. If a cyber system has a high impact on a BES element but the BES element has a low impact, the BES is not likely to be compromised because the actual BES element has a low impact.
SCEG	Consideration should be given as to how the newly classified "cyber systems" will fall under CIP-003-CIP-009 since these standards currently address a more narrow scope of cyber assets. This new apporach will result in many more cyber systems (and targets of protection) being identified, and the result may bring undue burden on utilities and/or require infeasible application of the additional CIP-003 through CIP-009 standards. Consideration of each category of cyber systems should be analyzed to determine the feasibility of implementing the remaining CIP standards. In other words, the applicability of the remaining CIP standards should be based on the "type" of Target of Protection or various exemptions should be allowed.
GEEI	Agreed, this is generally no different than the current risk-based assessment, except that two of the key variables that are inputs to the overall risk assessment have been defined by a fixed process through the impact mappings. The matrix should show the 3 characteristics, availability, integrity and confidentiality as variables for asset impact and cyber impact.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	No. It will result in a mis-allocation of resources to highly improbable or impossible events. The approach adds complexity without providing a reliability benefit. Misallocation of resources will decrease the reliability and safety of the BES creditable threats both cyber or non-cyber will not receive sufficient resources given that there are finite resources to allocate.
MEC	No. The overall approach adds several layers of complexity and it is unclear if it would produce improved results. MidAmerican is concerned with the complexity in the process proposed, questions if the process is repeatable on an annual basis and challenges the resulting security categorizations. As defined by ISO/IEC Guide 73, risk is the combination of the probability of an event and its consequence. The proposed categorization addresses only impacts (consequences) but does not address probability. As a result, how can the final security categorizations accurately reflect the risk posed by the Cyber Asset and what security measures should be applied? The proposed approach does not provide more clarity than providing more specific criteria for asset selection under the current approach in the standards. More specific details would be required under any approach. Adding clarity and specificity to the current standard is more productive. MidAmerican's methodology yielded rational results within the standard's current framework without multiple classification levels

Question 8

SCE	N/A – see comment to question 1.
AWEA	Based on Table 2 the process is either unclear or flawed. If a cyber system has a Low impact ("not expected to affect the BES Function it supports") why would the Final Categorization ever be rated as High regardless of the Asset Impact? Iron clad cyber protection of that cyber system would still have no impact on BES reliability.
APPA	Yes, but with all of the misgivings identified above. My primary concern is that the resulting deterministic matrix implies a level of categorical precision that does not exist in practice. This concern is not obviated by the statement that the evaluation matrix in Table 2 on page 21 is illustrative. That being said, current CIP-002 implicitly has a four cell matrix.
PAC	No. PacifiCorp feels the same results could be realized using only two categories of critical and non-critical. The overall approach adds several layers of complexity and it is unclear if it would produce improved results. An example is provided below:

	Asset Impact		
Cyber Impact	High	Medium	Low
High	Critical	Critical	Non-Critical
Medium	Critical	Non-Critical	Non-Critical
Low	Non-Critical	Non-Critical	Non-Critical

USBR	No. If the original thesis is examined under which we are trying to protect our cyber assets categorizing something low still results in an impact and may reveal a exploitable vulnerability.
PGE	PGE does agree with this process and believes that it would produce consistent results.
FPL	We agree with the process as described, but believe there is still a need for risk-based assessment to be performed.
TECO	We agree in principle with the approach; however, we believe that the process to develop and maintain this list is going to be very complex and will take significant education, knowledge, and awareness to complete/maintain.

Question 9

9. Section I, Defining the Target of Protection describes how an entity determines the set of cyber assets necessary to provide security assurance in the BES functions the cyber system performs. Do you agree with this process described in the concept paper? Please explain.

Name	Comment
CLPUD	It is unclear what the goal is here. Will the non-BES cyber assets be required to meet CIP-003-009?
TNSK	This is flexible, but is silent on the risk of attack, for example whether or not the protocol is routable or non-routable protocol, or if the system is properly isolated.
XCEL	We agree with the overall approach, but the paper's definitions require additional clarification. There also needs to be agreement on how 3rd party systems are addressed and who is responsible for communications links between systems and assets.
DOM	In general, this concept is agreeable. The flexibility for the owner to define a Target of Protection is appreciated. The concept of Collateral Cyber Systems is also agreeable, but it may not always be practical to move it out of the Interconnected or Infrastructure network segments. There are concerns about the inclusion of communication links within a Target of Protection. Specifically, communication links have always been excluded because there may not be a practical way (or identified need) to protect them. It is also appreciated that Section I uses the Target of Protection concept to identify more standard cyber components. On line 32 of page 23 it identifies devices such as routers, switches, firewalls, etc., as the actual components supporting cyber systems. It would have been better to develop this concept more in the beginning of the paper rather than emphasizing BES components, because this would seem to be the ultimate targets to be analyzed and protected. Also, the paper never seems to fully develop how the Target of Protection will be linked with the rest of the concepts presented in the paper or with the existing CIP standards themselves. This subject needs to be more fully developed.
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6. While FMPA agrees that cyber systems ought to be separated by where security is administered, e.g., unsecured connections between components of a system are part of the same system, we do not think that we need to define a new term "Target of Protection" but rather more succinctly define cyber systems as those systems whose boundaries are determined by where cyber and/or physical security is administered. If neither is administered, then there is no boundary. For instance, a substation automation scheme that interconnects all of the digital relays in a

	substation without cyber (e.g., firewalls) and/or physical (e.g., the relays are not connected together in a system – air gap) security would be one system. Alternatively, if there is a substation automation scheme where the relays are only connected through cyber security protocols in a "star" arrangement, then each relay would be a separate cyber system, and the central processing of the substation automation would be a separate cyber system. If loss of the substation could cause "instability, uncontrolled separation, or cascading failure", then the central processing of the substation automation could be a critical cyber asset regulated by the standards – including the cyber security protecting the connection between the relays and the substation automation processing; whereas individual relays may not be critical cyber assets depending on whether control of a relay could cause "instability, uncontrolled separation, or cascading failure".
SWPA	Yes, it appears to give us more flexibility than the current approach.
GTC	This section needs significant clarification. The approach appears acceptable from a theoretical viewpoint, but actually implementing this process is not practical.
DYONYX	Our understanding is that BES Cyber Systems would be protected in the same manner as Critical Cyber Assets in the current paradigm. However, protecting BES and non-BES Cyber Systems that in turn protect BES Cyber Systems, and including the same in the Target of Protection perimeter, is quite an extension to the original intent and scope of the Standard. Adding an additional layer of systems, utilizing different controls, is going to just mindboggling. In addition, nothing has been said about routable versus non-routable protocols. Section J notes that "external party dependencies cannot be ignored". This technically sounds good but, in our opinion, this will be a monster to design, implement, and sustain.
BPA	We felt that this assumes the utility has a combined IT and field network, which BPA does not. The figures in this section may not apply directly to cases where there is operational system isolation. Also, clarification is needed on the term Collateral – proximity in terms of physical location or network? No option to exclude a system that may touch the BES. Need ability to assign "N/A" Note, there are many terms not well defined to be able to adequately answer this question. Page 23, lines 15-20, what is "target of protection? Page 23, lines 20-25, discuss historical data collectors (think PI), "ICCP nodes, operations support workstations, etc" appears we must now consider that which we had already excluded from our critical cyber assets lists Page 24, figure 5, no workstations are listed in the "BES Cyber Systems" circle

	Page 25, figure 6, HMI (human machine interface) listed in the "BES Cyber Systems" circle; appears contradictory to figure 5 on page 24 Page 27, lines 5-10, what is the definition of "network proximity"?
SDGE	This section is a little easier to understand because there some additional real-world examples shown. I'm agreeable with the process as shown. One comment gathered from others in the company regarding the Target of Protection: It's obvious that the Target of Protection as defined will consist of a much wider footprint than what the current CIP Standards require, especially in the area of substations. Aside from the increased cost to implement these new protections, colleagues are concerned about the potential implementation schedule for these requirements imposed by the wider Target of Protection. To be realistic, these will probably double the size of our current CIP efforts, which is a substantial amount of additional work. We're all for Cyber Security and are supportive of the CIP Standards, there are just some internal concerns about the implementation schedule and how we manage the increased requirements.
GSOC	Section I, is confusing making it difficult to agree or disagree. Rewording and adding more clarity might help eliminate confusion. May consider adding a table or incorporate into Table 1 General comment: In the circle diagram for Control Centers the Interconnected Cyber Systems section has a PI Server, this should be changed to Data Historian Server since PI is an actual product name and this document should be product neutral.
BGE	This section indirectly redefines the Electronic Perimeter for CIP, by broadening the scope of the perimeter. The too broad definition of "Target of Protection" is making almost all of the enterprise IT systems (if they are on same corporate network) Critical Cyber assets. The concept described in this section can be applied to pure electric systems such as SCADA easily, but it is very difficult (or almost impractical) to implement this to AMI Systems which connect to corporate IT Systems (e.g. Meter Data Management System, Single sign-on Servers), electric devices such as advanced meters and AMI communication network which could be built on a public network. This concept is also difficult to implement on a Load Management system where it too connects to corporate IT systems such as the Customer Information System, GIS, Load Settlement and Customer Self Serve. In addition many load management systems are built on public paging systems utilizing one way communications.
CUSMO	Yes, it appears to give us more flexibility than the current approach.
MH	The Target of Protection to determine the cyber assets necessary for security is quite extensive and complete.

	Identifying the target of protection should be performed prior to categorization of the cyber assets. In this manner, the impact of these other cyber systems can be individually identified including their loss or compromise. This should lead to a more thorough analysis and better mapping to the appropriate security controls. The interconnectedness and inter-dependencies can also be included in the analysis. Technologies which provide effective air gaps should be permitted to reduce the impact of interconnected cyber systems.
NST	We agree with the basic concept of defining a "Target of Protection" that considers both identified BES Cyber Systems and cyber systems with which they interact or on which they depend. However, we also suggest the following changes: • We recommend renaming "Interconnected Cyber Systems" to something that (1) more clearly indicates their indirect involvement in or support of BES functions and (2) distinguishes them from other types of cyber systems within a "Target of Protection," many or all of which may be logically interconnected with BES Cyber Systems. Suggested examples are "Ancillary BES Cyber Systems" or "Secondary BES Cyber Systems." Were the SDT to adopt this recommendation, it might then also consider renaming, "BES Cyber Systems" to "Primary BES Cyber Systems," thereby indicating their direct performance or support of BES functions. • We recognize that a given Responsible Entity's BES Cyber Systems may very well interact with and/or depend on "Interconnected Cyber Systems" that are owned and/or operated by third-parties. However, we believe that assuring such third-party systems have appropriate security controls is a very different problem than assuring one's own cyber systems are properly secure,* so we recommend that third-party Interconnected Cyber Systems be identified separately from Entity-owned Interconnected Systems. * We believe, in fact, that unless Entities are given the means to exert some degree of control over how third-party cyber systems are protected, they will consistently define Targets of Protection that do not include any third-party systems. See our comments on Section J ("External Cyber Systems") below. • We recommend the SDT identify cyber systems described on Page 23 Lines 29-33 (routers, switches, etc.) as "Infrastructure Cyber Systems," as is done in Figures 5 and 6. • We suggest revising the paragraph defining "Collateral Cyber Systems" to either (1) remove implementation recommendations or (2) allow the *option* of applying the same or possibly a modified set of security controls to Collateral Cyber Systems as those applied to BES Cyber Systems instead of moving Collateral systems to a different network segment (which might be difficult and/or costly in some cases). This would be consistent with how non-critical Cyber Assets within an Electronic Security Perimeter are handled under the current version of CIP-007. • The paragraphs and figures on Pages 27 and 28 seem to suggest a one-to-one equivalence between "Target of Protection" and "Electronic Security Perimeter" but are somewhat unclear. We recommend that the SDT concentrate for now on identifying Targets of Protection and defer discussions of what various approaches to grouping Cyber Systems

	within one or more Targets of Protection might mean from a logical and/or physical security standpoint, lest such discussions become a distraction.
NPCC	Agree with this process, but struggled understanding the correlation between the text and diagrams.
RFC	We agree. The approach described in Section I provides a better approach to identifying the additional cyber systems that need to be protected, as well as those non-critical or collateral systems that a entity may wish to remove from the target of protection.
IRC	Yes. We especially appreciate the breakdown in the TOP that demonstrates how this might work for Control Centers, as well as Gen/Transmission facilities. We look forward to reviewing the next level as the SDT moves forward
AEP	The inclusion of supporting systems (i.e. environmental controls and monitoring systems) and the "Collateral Cyber Systems" could exponentially increase the assets in scope and complexity without any commensurate gain to security or reliability of the BES. In addition, Section J describes the interconnection of external cyber systems. It is unclear how an entity can assume all of the risks associated with an external entity's systems and the data connection (which might be a leased communication line from an independent provider).
WE	While Wisconsin Electric can agree in concept to this process, we feel additional definition should be presented around how various cyber systems would be treated based on high, medium and low categorizations. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	This is difficult to answer because the concept is not clearly defined. The systems suggested to be part of the *Target of Protection* population would seem to considerably expand the existing regulatory compliance scope of the affected utilities thus residing in higher compliance costs for the industry.
SOCO	Additional information is necessary to adequately access the impact.
E-ON	The concept paper's "Target of Protection" appears a roundabout way of stating that equipment connected with a BES cyber system so as to create the potential for communications access to the BES cyber system requires protection. The concept

	paper also does not limit this concern to networks employing a routable protocol as is the case today and as is appropriate
ATC	The concept paper is not clear if the other categories "Interconnected Cyber System", "Infrastructure Cyber System" and "Collateral Cyber System" will be treated the same for each of the three categories (High, Medium and Low) for BES Cyber System.
TAPS	See responses to Questions 1, 2 and 5.
GWA	The description in Section I is helpful.
SCEG	The Concept looks good in paper, but the reality would be many of the Collateral Cyber Systems will be more integrated. This will make the removal of the systems a greater challenge
GEEI	The *concept* isn't disagreed with, but security is not generally as simple as: "choose system/function from column A, impact from column B, and security requirements show up in column C". It is a laudable goal to pursue this table, but far too often the answer depends on factors that are not easily quantified. Collateral systems which have impact on other regulations i.e EPA, need to be considered.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	No – MRO NSRS believes the concepts presented in the paper could cause significant scope creep resulting in the addition of components that previously were not required to be included, or were deemed non-critical given their limited or no impact onto the reliability of the BES.
MEC	No. MidAmerican agrees with a Responsible Entity having flexibility in defining a Target of Protection to maximize efficiency in secure operations. MidAmerican accomplished this by analyzing the Cyber Assets without the additional proposed layers of complexity of cyber system grouping and labeling. Additional specificity would be needed for all entities to achieve consistency. Section I introductions potential significant scope expansion by adding "non-BES Cyber Systems." MidAmerican agrees with Section I's conclusion that unnecessary Cyber Assets should be moved out of the other protected network segment. This can be accomplished within the existing standards' framework and without additional layers of process complexity. MidAmerican generally agrees with figures 5 through 7. Figure 8 and figure 9 are unclear and could be construed to expand

	scope to include communication links that are explicitly out of scope in the current standard. Section J discusses interconnections and information exchanges across multiple organizations. It is unclear what is meant by "a third party data connection outside of the traditional Electronic Security Perimeter" or what is intended (beyond what is already achievable in the existing standards) by "the responsibility to mitigate the risk" of an external interconnection.
PSEG	The term Target of Protection is capitalized but not defined in the NERC glossary, nor is there a current SAR to have the term defined and added. PSEG recommends the drafting team consider developing a clear definition of the term and take the necessary actions to have the definition added to the Glossary, or, eliminating the term altogether.
SCE	N/A – see comment to question 1.
APPA	The framework appears to be conceptually sound. Delineating the differences between BES, Interconnected, Infrastructure and Collateral Cyber Systems would appear difficult to this cyber non-expert. On page 23 at lines 29-34, an italicized definition of "Infrastructure Cyber Systems" appears to be missing.
PAC	No. While PacifiCorp agrees that a Responsible Entity should have flexibility in defining a Target of Protection to maximize efficiency in secure operations, we feel that Section I introductions potential significant scope expansion by adding "non-BES Cyber Systems." PacifiCorp agrees with Section I's conclusion that unnecessary cyber assets should be moved out the other protected network segment. This can be accomplished within the existing standards' framework without additional layers of process complexity. PacifiCorp generally agrees with figures 5 through 7. Figure 8 and figure 9 are unclear and could be construed to expand scope to include communication links that explicitly out of scope in the current standard. Section J discusses interconnections and information exchanges across multiple organizations. It is unclear what is meant by "a third party data connection outside of the traditional Electronic Security Perimeter" or what is intended (beyond what is already achievable in the existing standards) by "the responsibility to mitigate the risk" of an external interconnection.
USBR	No. The concept does not provide security assurances. The premise expounded in the concept is that any subsystem can result in a BES impact. The flaw is in the determination of the impact. A Cyber subsystem of a BES Cyber Asset may fail, however, that does necessarily mean the BES is at risk. The overall complexity of the defense against a cyber failure cannot compromise the functionality or maintainability of the cyber asset. This Target of Protection moves in that direction.

Question 9

PGE	PGE is not able to provide meaningful comment on this approach without greater understanding of the pre-defined criteria that are used to categorize Cyber Assets.
FPL	Agree with the process and find it helpful. Although its application must be left to the individual utilities, the process is still too broad and should provide clarification. In addition, clearer expectations of the systems in Figure 8 should be provided.
TECO	Section I provides a good representation of what a Registered Entity must do in order to separate the non-critical cyber assets (collateral cyber systems) from its critical cyber systems in order to improve cyber security controls in the most cost effective manner.

Question 10

10. Provide your company's thoughts on applying different levels of protection (i.e., security controls) based on characteristics and impact categories of specific BES cyber systems (e.g., transmissions substations, generating plants, control centers) as discussed in Section K, Applying Security Controls to the Target of Protection, of the concept paper.

Name	Comment
CLPUD	Seems to go well beyond the scope of CIP-002. Is this the intent?
TNSK	The impact category to a Cyber System and determination of Target of Protection for Generator Owner and Generator Operators will need to be completed with the assistance of the appropriate Regional Coordinator.
XCEL	We support the overall approach of developing different levels of protection based on characteristics and impact. However, more detail needs to be provided on what the security controls catalog contains and what will be required for implementation.
DOM	Other than basing it on having evaluated every piece of equipment, Dominion fully supports the ideas expressed in Section K. A flexible approach that "mitigate[s] risk while maximizing the value of the associated cyber security investment… without unduly requiring entities to invoke exception processes in the standards" is exactly what these standards should be about. Also, while it is understood that the ultimate goal of the standards to be developed is to protect the BES, this standard itself should concentrate on cyber components only. Referring to a substation as a BES component is confusing. A substation is not a cyber system. It is a system comprised of many components, both mechanical devices, electrical devices and cyber devices. In this paper, the Target of Protection concept needs to be concentrated on cyber systems first.
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6. FMPA believes there ought to be only one level of protection regulated by the standards, and only on "critical" cyber systems that can cause "instability, uncontrolled separation, or cascading failure". While entities can and will use cyber security measures on non-critical cyber systems, there is no need to regulate these security measures.
SWPA	The process is good in that it allows for different levels of protection based on impact. However, there needs to be acknowledgment that not all cyber systems necessarily impact the BES. There needs to be an exception for subsystems that have little or no impact to BES reliability.

Question 10

GTC	It is absolutely crucial to have controls appropriate to the characteristics of the environment (substation, generating plants, control centers). An unmanned substation in a rural area has different vulnerabilities than that of a data center in an office park. Controls should be applied that are appropriate to the risk profile of the system being protected.
DYONYX	We believe a two tiered set off levels is adequate. Why make it complicated and very difficult to implement and sustain? See comments to question # 1.
BPA	See answer in Comment #11 Would like clarification of terminology comment. Page 29, lines 25-30, implies that utilizes that identify a cyber system as "high", but their external interconnected partner does not take full responsibility to mitigate any risk associated with the cyber system; What does full responsibility mean here?
SDGE	The idea of applying security controls to the Cyber Systems within the Target of Protection seems reasonable. It stands to reason that different levels of protection would be proper, given the new impact categories. In our internal discussions, we talked about the library of controls that the drafting team will develop. Those seem key in determining what actual steps must be taken in the protection of our Cyber Systems. As mentioned above, the general concept presented seems okay, but there are a lot of missing details that make it difficult to comment substantively. For the limited amount of information presented, it seems workable.
GSOC	Our company agrees that different levels of protection are definitely needed and this approach will achieve that. The different environments, a Control Center, a Plant DCS or a Transmission substation will require different security controls, therefore developing a library of controls appropriate to the cyber subsystem is a good approach.
BGE	It is likely that the CIP compliance management (i.e. the paperwork) for substation cyber assets is likely to increase dramatically and encompass most BES stations, probable unnecessarily if the primary intent is to provide Adequate Levels of Reliability to the BES. Substations typically exist in more numerous, simpler, more effectively isolated, and very different cyber environments than federal government IT systems. The continued march toward increased reliance on IT- centric security standards in use by the government will be a confusing impediment to effective and easily understood implementation of cyber security measures in most substations. We ought to be able to talk in the standards about cyber security for protective relays, RTU's and other common substation equipment without obscuring that discussion with lot of language intended to apply to large data processing systems with confidential information on a WAN connected to the Internet.

CUSMO	The process is good in that it allows for different levels of protection based on impact. However, there needs to be acknowledgment that not all cyber systems necessarily impact the BES. There needs to be an exception for subsystems that have little or no impact to BES reliability.
MH	All the categorization of BES Subsystems and Cyber Subsystems should be as simple as possible to map to the appropriate security control level. The overall process and documentation should be kept to a minimum. Flexibility for Responsible Entities to choose the appropriate impact levels will optimize the process. If the final process does not allow for flexibility then the overall process should be simplified to a chart of impacts versus required security controls.
NST	We strongly endorse the concept of developing requirements that take into account the sometimes significant differences among built-in security capabilities of various types of BES cyber systems. At the same time, however, we believe there will be instances, for example in the case of "High Impact" cyber systems, where the Standards should continue to require the application of equivalent protections using alternative controls, if necessary. We also recommend that the SDT consider allowing for different or customized levels of protection to be applied to some cyber systems and/or their constituent elements within a single Target of Protection (Section F concludes with a statement suggesting to us that all cyber systems within a Target of Protection will require the same level of protection as BES Cyber Systems within). For example, the Availability requirement for a SCADA/EMS system server might be High, while the "real-world" Availability requirement for any one of its operator workstations might be only Medium, or perhaps even Low. We believe this recommendation supports the SDT's goal of maximizing the return on industry investment in cyber security.
NPCC	We agree with applying different levels of protection if you remove from this question "(e.g., transmissions substations, generating plants, control centers)" because those are not cyber systems.
RFC	Different levels of protection based on net impact of the cyber system is an excellent idea. It tracks with most major IT governance solutions in use.
IRC	We are supportive of the approach used in NIST SP 800-53 R3 which uses a building block approach of some controls for low level risks and then increases the controls if the higher risk levels is Medium or High. We do not see the need to re-invent basics for Control Centers and supporting Data Centers. However, the Generation and Transmission organizations may be challenged by this approach, given the differences and more complexity of the security tasks facing those entities.
AEP	Any methodology for securing essential cyber systems should allow a degree of flexibility and discretion by the responsible

	entity. The methodology should provide a framework to allow the flexibility without pre-determining the set of controls that should be used.
WE	This has merit. Transmission substation control systems, generation control systems and control centers have evolved at different rates regarding internetworking technology. Relay controls do not have the same protective capabilities as more traditional windows based architectures as seen in the control center areas. This makes it difficult or impossible to deploy malware protection (antivirus) on a solid state network connected relay resulting in creation of a TFE under the current standards. This is just one example of problems we are presently encountering applying the current standards across all critical cyber assets. The protection levels should take into account the probability of occurrence (risk) as currently used in CIP 002-1. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	Needs to be coordinated with other groups that are trying to do the same thing, such as groups developing Smart Grid standards. We do support varying controls, similar to the NIST model - NIST standards can be applied to the *Target of Protection* to ensure industry wide consistency in adoption of existing standards.
SOCO	Different levels of protection are needed to appropriately address the variance of risks between BES cyber systems. Moreover, the connectivity and/or other vulnerabilities to outside the electronic security perimeter should be considered in determining the appropriate level of protection.
E-ON	Medium and low risks are irrelevant. Only cyber systems the loss of which would lead to instability, uncontrolled separation, or cascading failures of the BES are relevant. Introducing gradations of risk does nothing to lessen the uncertainty over compliance that exists today and invites further uncertainty as to which set of requirements apply. It should not be an undertaking of the drafting team to develop security controls or control "specifications." The drafting team should develop minimal requirements that when adhered to insure BES reliability. Affected registered entities then implement security controls that meet or exceed these requirements, and therefore further BES reliability, while maximizing the value of their own cyber systems investments
ATC	Applying different levels of protection based on asset characteristics and BES impact is a step in the right direction. However, the type and scope of the threat needs to be known. For example, if the threat is assumed to be a coordinated physical and cyber attack on multiple assets, systems and facilities, the level of protection would be vastly different then protection against vandalism from a single individual. In addition we do not believe that all categories ("High, "Medium" and "Low") need to be subject to NERC compliance.

Question 10

TAPS	See responses to Questions 1, 2 and 5.
GWA	The diverse environments in which assets that make up and support the BES, and the different impacts of individual assets and systems suggest a library of controls with discretion to select those best suited to the environment and impact of an individual system. This will provide a better overall level of security than the "two-bucket" (critical or not critical) approach embodied in CIP 002 V2, by ensuring a comprehensive review of assets, impacts, and allocating security resources to address relative impacts.
MISO	It is not clear what problem the CIP drafting team is trying to solve. Is the CIP drafting team trying to prevent cascading outages and blackouts caused by cyber attacks or are they trying to prevent the BES from ever experiencing any level of impact from a cyber attack. It appears the drafting team is attempting to develop standards based on the latter approach when it would be more appropriate to develop standards designed to prevent cascading outages and blackouts. The standards should not be focusing on a small scale cyber attack on cyber systems that might prevent operational challenges but would not cause a blackout.
SCEG	We agree with this approach. A smart instrument in a remote area requires a very minimum set of controls for Cyber Security, where as a Router connecting a DCS/SCADA to a Control Center would require a much more protective posture
RFC-CIP	Cyber Systems at transmission substations generally operate on specialized programming and processing hardware, have not been developed to accommodate additional security applications, and utilize communications requiring a modem interface. Therefore, security measures would be practically limited to the electronic perimeter, or modem, boundary. However, Cyber Systems at Control Centers are based on a distributed system of client/server hardware and software that communicate over a much wider network system and require careful security posture monitoring at every node.
GEEI	This is an admirable goal, but as a systems manufacturer, it still leaves a great deal of potential variability, when considered on an implementation-by-implementation basis, in the security requirements for any cyber system.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	The MRO NSRS agrees that there needs to be protection but not enough information is provided to apply security controls.

MEC	MidAmerican agrees with different levels of protection. However, the levels of protection should be determined based on risk characteristics for the type of cyber asset. As stated earlier, risk includes consideration of probability of an event. For example, assets that are not vulnerable to viruses have no need for antivirus solutions, but the current standards do not provide that flexibility. The protections defined in CIP-005 and CIP-007 should be revised to acknowledge the differences in risk characteristics between relays, controllers, servers, firewalls, etc. This will also significantly reduce the number of technical feasibility exceptions without creating risks to the BES. MidAmerican does not support differentiating based on impact alone. This would add further complexity and not reflect the true risk to the BES.
PSEG	PSEG appreciates that the drafting team recognizes a key objective of the next version of CIP 002 is to develop controls "in such a way as to mitigate risk while maximizing the value of the associated cyber security investment for the industry." PSEG strongly supports hardening of cyber control systems, and applying appropriate security controls. PSEG does not support allocating resources to file and maintain Technical Feasibility Exceptions for systems that are simply not capable of running specific controls. PSEG recommends that the drafting team consider the applicability of each control to various types of devices, rather than forcing a "one size fits all" control than may actually fit none.
MMPA	Different level of protection is a more reasonable approach then the current system where assets either are CCA's or are not. Not all CCA's require the same level of protection and some require TFE's that may fall into a lower level of a multi-tiered approach where a TFE would not be required. Conversely, a non-CCA may require more stringent protection than standard business practices.
SCE	N/A – see comment to question 1.
APPA	If a useful library of security controls can be developed and be appropriately targeted to different types of BES systems and to differentiate between systems based on their importance (e.g., high thresholds for RCs and large multi-state BA/TOP control centers, with low thresholds for small BAs and TOPs, etc.), then the concept paper will be a major advance. However, appropriate balance must be struck between standardization and registered entity discretion.
PAC	PacifiCorp agrees with applying different levels of protection based upon characteristics and categories of specific BES cyber assets. The levels of protection should be commensurate with the risk characteristics for the type of cyber asset.
USBR	Impacts on the BES as the result of Critical BES Assets monitored by or controlled by Cyber Assets is not acceptable irrespective the relative probability of the impact however developed. The existing requirements describe specific criteria and processes which my company must either develop or have documented and implemented to be compliant with the standards.

Question 10

	There has been no demonstrated reason that these requirements are inadequate. The definition proposed by the team in this question (BES Cyber systems are transmission substations, generating plants or control centers) is not realistic or consistent with other reliability standards.
PGE	PGE is not certain how NERC and the Regional Entities will be able to apply their enforcement processes to a flexible system of controls. While a level of flexibility may be appropriate for each entity's implementation, this needs to be weighed against the enforceability of the controls.
FPL	This is a good approach and is similar to what most companies do today. The level of protection i.e. card access, passwords, etc are proportional to the impact that the system could have. One item one clarification should be made regarding external connections as part of a company's Target of Protection. For instance, does this mean a company that relies on data from a foreign company to maintain situational awareness must develop an alternate source of data or require the foreign company to meet the standards.
TECO	We agree with this and strongly encourage the SDT to engage security vendors and SCADA/DCS vendors in the development of this library of controls to ensure that the required controls can be implemented on equipment in the field today as well as equipment developed in the future.

Question 11

11. Section K, Applying Security Controls to the Target of Protection, of the paper introduces the concept of a library of security controls. What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems? What specific challenges would you anticipate in implementing controls from among a library of security controls?

Name	Comment
CLPUD	No opinion. But since this form has no room for general comments, Central Lincoln would like to comment on the applicability of CIP-002. Per the functional model, load serving entities do not own physical assets, and so do not own the BES subsystems and BES cyber systems described. LSEs should be removed from the applicability section.
TNSK	The library of Controls should be based in the implementation best practices of the existing standards.
XCEL	Recommended sources: NIST framework documents (specifically 800-53 and 800-82), ISA-99 The main challenge is translating the security controls designated for information systems and the general information security components of confidentiality, integrity, and availability for the control system environment (where availability has been traditionally stressed as primary, but the other components still need to be addressed).
DOM	It is anticipated there are very few standards that are written to cover real-time data acquisition and control systems using the wide variety of software, hardware, ages, and configurations found throughout the industry. If the Target of Protection was defined more specifically to be aimed at standard cyber devices as mentioned above (firewalls, routers, switches, etc.) it would seem that the library could be based at least partially on standard Information Technology ("IT") protection standards already in place. In fact, standard IT procedures such as user logins, password protection, patch management and malware prevention were examined in the requirements and implementation of Version 1 CIP standards. These are areas of cyber protection that are already well understood and were verified in the current implementation of CIP. This should be used as the basis for any future changes including the development of a library of security controls.
SWPA	We recommend researching all current industry standards and creating a "library of controls" based on those that are most applicable to the systems used to support the BES. We do not agree with adopting another organization's standards verbatim, if they were developed for systems outside of those commonly applied to the BES, without close scrutiny from registered entities. We are also concerned about standards that are also developing and we may or may not have input into their change

	process.
GTC	Vendors should be consulted as a source in developing the library of security controls.
DYONYX	As we read this section, “the drafting team will consider approaches to provide flexibility while ensuring adequate protection from dynamic and evolving threats and vulnerabilities…along with different levels of protection, etc.”, in our opinion this whole level of detail is **unsustainable**.
BPA	The utility needs to be able to tailor fit their own library of controls. A predefined library of controls will never be all encompassing – it needs to have options and be flexible. If the library of controls includes a limited list of choices and none actually work for the utility, then the work falls on the utility to try to make something fit where it naturally doesn’t fit. Clarification comments. Page 30, lines 15-30, what does "develop a library of controls (requirements) appropriate to the degree and type of protection needed" mean here? Page 30, lines 25-30, specifically note that "operating environments" will be taken into consideration when entities evaluate their approach to protection Page 31, lines 15-20, "all cyber systems related to reliability or operability of the BES are required to implement a security posture commensurate to the level of criticality of the BES Subsystems they are supporting" does this mean if a system supports a critical asset it needs to be covered the with the same controls?
SDGE	As mentioned above, we feel that the library of security controls is key to Section K. They need to be vetted by power system industry experts for practicality, reasonableness, and effectiveness. A library of security controls for a financial institution would be much different that what would be applicable to the power industry. Especially in our field locations, we deal with many inhospitable environments and special challenges related to distance, temperature, etc. If possible, we’d like to have some choices available when implementing an appropriate security control. Please don’t lock us in to a small number of controls that may be difficult to implement in our power system environments.
GSOC	The drafting team should consider the following industry standards that exist such as: the NIST framework, ISO/IEC 27002, etc. Another thing that the drafting team should consider is getting input from the vendors of the various cyber systems that they supply, EMS/SCADA, RTUs, Electronic Relays, etc. The vendors should be involved up front to help define the types of

	security controls that should be implemented. If the vendors are not involved up front to help establish security controls that support their products, then it could be difficult and costly for entities to implement the security controls. This could result in the entity having to implement costly workarounds or having to take exception to the standards as stated in Section K.
CUSMO	We recommend researching all current industry standards and creating a "library of controls" based on those that are most applicable to the systems used to support the BES. We do not agree with adopting another organization's standards verbatim, if they were developed for systems outside of those commonly applied to the BES, without close scrutiny from registered entities. We are also concerned about standards that are also developing and we may or may not have input into their change process.
MH	The library of security controls must include provision for layers of protection both inside and outside the ESP and PSP. Protection afforded by isolation, use of private communications and private facilities must be included in this library of security controls. If the library does not accommodate these security provisions then inappropriate security controls may be required. The design of the security controls must provide for flexibility and broad application, so that technically creative solutions, which meet the intent of the standard requirements, are still permitted and they are not excluded by narrow interpretations of the standard requirements. A draft list of security controls should be made available at the same time or before the industry considers any revised CIP-002 standard. Without any information on the security controls the industry will not be able to understand the overall approach and impact to their entity.
NST	We consider the newest revision (Rev 3) of NIST Special Publication 800-53 to be an excellent resource for the development of such a library of security controls. In particular, we note that Appendix D of that document ("Security Control Baselines – Summary") provides a set of recommended controls for High, Moderate, and Low impact information systems that might be useful as a starting point for the creation of comparable baseline profiles for High, Medium, and Low impact BES Cyber Systems. Challenges we see include: • Developing a set of baseline control profiles for BES Cyber Systems that are properly tailored to BES operational environments, address the right sets of identified cyber threats and vulnerabilities (we recognize that reaching consensus on what is "right" may require no small effort), are achievable, and leverage industry investment in compliance with the existing, "-1" set of CIP Standards. • Maintaining and updating a controls library to reflect both emerging technologies and new and evolving threats. • Striking a reasonable balance between allowing for flexibility in selecting and applying controls and requiring, for the sake

	of consistency and overall BES protection, that all BES entities comply with some minimum set of requirements for High, Medium, and Low impact cyber systems. A revised set of CIP Standards based on a "catalog of controls" could, depending on the amount of customization permitted, greatly complicate the tasks of verifying and enforcing compliance.
NPCC	We agree with the concept of a library of minimum requirements, but do not support the concept of a library of controls since requirements are implemented by controls. We suggest one library of requirements for control centers, another for substations and a third for generation. We are concerned about how much time and effort will be needed to create those libraries. We are concerned that existing sources will need so much modification to work with the BES that it is probably more efficient to use industry expertise.
RFC	NIST SP800-53 Appendix F "Security Control Catalog", CoBiT, FISCAM. There is probably an ISO standard as well. The challenges will revolve around achieving a balance of good control with ease of implementation. It is easy to go too far when implementing controls and require more than is necessary to achieve the ultimate purpose
IRC	No comments—We would like to see more details of proposed controls and would support controls similar to how they are currently structured in NIST SP 800-53 Rev 3 and similar ISA publications. The Concept presented in the paper appears sound with respect that those assets listed as HIGH should receive the most stringent controls. NERC/FERC audits should focus on the HIGHS and MEDIUM controls and use self reporting (and spot checks) to address compliance with systems rated as LOW. The level of documentation required for Compliance should be consistent with the level of Risk—HIGH Risk components should have detailed documentation available for review, while Low risk components should comply with basic requirements but not be subject to the same level of documentation required for HIGH systems. Let's not further expand the documentation requirements beyond that currently specified.
AEP	NERC reliability standards focus on the outcomes rather than solutions to achieve those outcomes. Having a menu of controls could inadvertently shift the focus from what to secure and protect to how it should be done which can reduce efficiency and innovation.
WE	Wisconsin Electric recommends starting with current standards (NIST 800-53, ISO 17799) and research current vendor equipment capabilities for relays and control systems around cyber security and internetworking requirements. ANSI standards for specific control systems and relays would be another point of research. The library should be based on what can be accomplished today with a future state direction. Some of these systems have long service lives, so the library of acceptable protective measures will need to allow for older technology that cannot be protected in a certain way without creating a TFE.

Question 11

DUKE	NIST Special Publications SP800-53, 800-32. It may be difficult to determine how to adapt business controls to process computing systems. Another challenge is that technology is constantly changing.
SOCO	As noted in our response to Question 4, cyber security problems do not lend themselves to one-size-fits-all solutions. For example, flexibility is needed to avoid unnecessary duplication which may result based on previously implemented or alternate security protections, or higher level controls.
E-ON	The drafting team should not be developing security controls. The drafting team should be developing standard requirements. Pursuant to FPA Section 215, cyber security standards exist to insure BES reliability by visiting sizable penalties upon relevant entities who fail to secure facilities essential to BES reliability in a manner that complies with the applicable minimal standards. This requires the drafting team to develop requirements that are clear and concise so registered entities readily understand the steps they need to take, or refrain from taking, in order to avoid penalty. The major challenge in implementing controls from a library arises when the methodology currently employed, although perhaps fully adequate in protecting BES reliability, is not part of that library. That is why the drafting team should focus on clear and concise performance requirements rather than prescribing the use of one or more pre-approved security control methodologies
ATC	We are not aware of any source documents but believe that the SDT needs to work with various technical teams that can catalog existing utility practices. ATC does not believe that there is a one size fits all approach that can encompass all entities. The SDT needs to justify the amount of work needed to develop a library of security controls over addressing actual FERC directives.
GWA	NIST Special Publication 800 series, ISA security standards, SANS, and IEEE are all resources. The challenge with implementing security controls from a variety of sources is that the overall approach to each set of controls is somewhat different. The important goal, however, is to provide each asset owner discretion to select a set of controls that provide effective security that are cost-effective, are easily administered and maintained, and are appropriate to the type of asset and its associated reliability impacts. This will ultimately lead to an improved security posture for the BES.
SCEG	The Nuclear Industry has put forth tremendous effort to develop a minimum set of Security Controls to Achieve High Assurance of Adequate Protection. [RG 5.71 (Draft) and NEI 08-09 Rev 2] The list was developed using NIST. Many Controls were modified to take advantage of the Utilities Physical Protection Posture. With different levels of expertise at the various Utilities a Control could have different meanings. Training on the Controls that

	are selected as a baseline for High, Medium, and Low Levels of protection would be beneficial to the Industry.
RFC-CIP	The "Library of Security Controls" could be patterned after NIST 800-53 Appendix F " Security Control Catalog" which maps levels of control to the levels of impact of the system being protected. Consider the comment to item 10 above that many security controls would not be able to be applied to a High impact asset. The Library approach could therefore generate an excessive amount of technical feasibility exceptions if such a provision was incorporated into the standard.
GEEI	One of the challenges when selecting from a "library" is that there is always variability in an implementation. Being forced to choose from a particular set of solutions may under-engineer or over-engineer the solution giving no cost or additional risk mitigation benefit. There is no generally accepted / authoritative library of "security controls".
LES	IEEE, EPRI, or ISA. The main challenge would be implementing controls on systems that are not designed for the application, or require utilities to establish a remote connection to update the security control applications on an otherwise isolated networked.
MRO	Inadequate information has been provided in regards to the library of security controls. The library of security controls needs to be developed before a recommendation can be formed. The library of controls might be appropriate in a case-by-case application but a global application should not be made mandatory since every company has unique methodologies.
MEC	MidAmerican would support a library identifying security controls by type of asset. As noted in MidAmerican's response to question 10, standards CIP-005 and CIP-007 need to be revised from a one-size fits all approach. The drafting team should first revise existing controls in the standards by matching controls to the various Cyber Asset types. This foundation is necessary before a gap analysis against other sources can be effective in producing a list of controls by asset types. Risk is the combination of the probability of an event and its consequence. For a control to lower or eliminate risk, it needs to have an impact on lowering probability of an event or lessening the consequence of the event. Only controls that materially lower probability and/or consequence of a significant event for a specific Cyber Asset type should be on the library list for that asset type. Controls that do not materially lessen probability or consequence of a significant event jeopardize the drafting team's crucial undertaking of mitigating risk while maximizing the value of the associated cyber security investment for the industry.

	The recommended approach leverages existing progress made under standards 003-009 without completely rewriting or abandoning them and can deliver effective results quicker. To the extent that the security controls in the library are supported in other information technology industry standards, vendors would have greater encouragement to provide information technology that delivers the security controls.
SCE	N/A – see comment to question 1.
APPA	No comments.
PAC	NIST Publication 80-53 - Recommended Security Controls for Federal Information Systems and Organizations. PacifiCorp would support a library identifying security controls by type of cyber asset. As we have experienced in the current standards not all controls can be applied to every type of cyber asset utilized in the industry thus the reason for the introduction of Technical Feasibility Exceptions (TFEs). A library of security controls by cyber asset type would eliminate most TFEs and the administrative overhead associated with these exceptions. If the controls were specific to a category of cyber assets it would likely lessen the challenges of the industry in trying to apply controls to devices that cannot conform to the controls.
USBR	Vulnerability is determined by analysis and test not assumption. The greatest challenge for the team would be to find method that clearly demonstrates the security control solves a real vulnerability.
BRAZOS	ISA-99.
FPL	Although we agree that a library of security controls is helpful, we want to note that it is used as a guideline not as requirements as stated in lines 19-20 of Section K. If the security controls provided are required, it may reduce the flexibility to have vendor solutions implemented in a timely manner.
TECO	We agree with this and strongly encourage the SDT to engage security vendors and SCADA/DCS vendors in the development of this library of controls to ensure that the required controls can be implemented on equipment in the field today as well as equipment developed in the future. NIST and other standards issuing organizations should be consulted. To ensure success, the engagement of security and systems vendors is crucial. We want to also ensure that the controls are cost effective to minimize impact to rate payers who will ultimately be responsible for paying for these controls.

General and Editorial Comments:

Name	Page	Line	Section	Comment	Suggestion
AMER EN-1				This concept paper represents a fundamental shift from any concept that has been used to define critical assets. The concepts outlined in the paper seemingly remove the idea of Critical Assets in favor of a more broad approach. The driving force with reasons behind this concept paper should be stated.	
AMER EN-2				Categorizing cyber systems as described in this concept paper will encompass significantly more cyber assets with no consideration of cost, complexity, or resources needed to protect and remain compliant. There is no supporting information in the concept paper that gives any direction as to the scope of what protective and compliance documentation will be required to remain compliant. Without these boundary guidelines, it is hard to ascertain the value of these concepts as it relates to overall security and compliance burden and its relative value to the protection of the Bulk Electric System.	
AMER EN-3				A great improvement to the risk based methodology if you are going to be forced to apply cyber controls to several new devices is the use of different cyber security protections based on risk and type of cyber asset which is outlined in this concept paper.	
AMER				Many of the NIST controls make no sense for	

Name	Page	Line	Section	Comment	Suggestion
EN-4				control systems. They are written for Ethernet based networks. NIST controls require people intimately familiar with control systems, their configuration, and how they can be protected to develop a set of controls that can actually be implemented. The current criterion of the device needing to have a routable protocol is logical and valuable in determining what you need to protect. Introduction of a concept that envelopes all BES subsystems does little to protect over cyber security for systems that have an "air gap" or use non routable protocols. Including non-routable systems will only increase the compliance burden and provide little to no additional protection to the Bulk Electric System.	
AMER EN-5				Compressive inventory and categorization of BES Subsystems is a large and complex task that would be a significant undertaking if such a study were required annually. It is the intention of NERC and the drafting team to require annual inventory and classification of all assets that comprise the Bulk Electric System? Current CIP standards require 30 days to update any changes in network configuration. Are systems that are part of the BES subsystems that are not inside an electronic security perimeter going to be included in this 30 day window?	
AMER EN-6				The questions outlined can not be answered without an understanding as to what the security controls are going to be based on the categorization of the BES subsystems. This	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				concept could be beneficial if controls for low risk systems do not overwhelm the benefits of such systems being included within the scope of these regulations. Without such additional information, it is difficult to come to a consensus to answer the included questions in this survey.	
ATC-1a				General Comments: ATC appreciates the amount of work the Standards Drafting Team has already spent on the CIP standards and understands the number of challenges that still must be tackled, but we believe that the proposed *"Categorizing Cyber Systems an Approach Based on BES Reliability Functions"* concept paper does not represent the correct path to improvements. We do believe that the paper contains some good ideas but without fundamental changes the result of this effort may result in a drastic increase in cost and compliance with little or no benefit to the reliability of the Bulk Electric System.	Categorization is not bad but entities must be able to determine the likelihood and severity of an event when categorizing their BES Functions
ATC-1b				It is our understanding that the approach, presented in the concept paper, will result in the elimination of the identification of Critical Assets and the protection of its Critical Cyber Asset (Risk-based Assessment) and replaced with a system were all Cyber Systems will have to be categorized into "buckets" (High, Medium and Low) and then exposed to some level of compliance obligations. The "bucket" concept is critical because it dictates the level of cyber and physical security that entities will have to	Any additional compliance obligations should be limited to only those that have both "High" Asset Impact and Cyber Impact

Name	Page	Line	Section	Comment	Suggestion
				demonstrate compliance with and does not allow for any cyber system to be excluded from compliance. ATC believes that improvements to formalize the process for the identification of a facility's importance (use a Risk-based Assessment approach) is a step in the right direction, but that Reliability Standards should only focus on "High" (Critical/Essential) facilities.	
ATC-1c				ATC also feels that this concept paper fails to address some key questions:	We believe that the concept paper should address these key questions.
ATC-1d				How will this improve reliability? We acknowledge that this will greatly expand compliance obligations but this paper does not address how that alone will improve reliability.	
ATC-1e				What other alternatives were considered? The SDT should provide alternative approaches for the industry to discuss and consider. The SDT needs to provide additional justification for the selection of its proposal and why the alternatives were rejected. (The industry should be allowed to weigh in on the alternative approaches.)	
ATC-1f				What is the SDT attempting to protect against and from what type of event? The proposal seems to indicate that NERC wants to protect everything from everything even if its impact on BES reliability is "Medium", "Low" or	

Name	Page	Line	Section	Comment	Suggestion
				none.	
ATC-1g				Why is the SDT abandoning the "probabilistic" approach currently allowed in CIP-002 with a "deterministic" approach? How did the SDT conclude that low probabilistic events were going to be treated the same as high probabilistic events?	This is not done in the planning criteria for example. A lower probability event is not held to the same requirements as a high probability event. Clear criteria should be applied just like for planning criteria.
ATC-1h				What is the cost impact of this proposal? This should be looked at from the perspective of a small, medium and large entity. Based on our understanding it would seem that a small entity that does not have any Critical Assets will likely incur a large increase of cost. In contrast an entity that has Critical Assets may not see an increase in compliance for those elements but will see an increase in cost associated with "Medium" and "Low" facilities. Because of the possibility of increased cost, we believe that the SDT needs to perform a Beta Test.	
ATC-1i				Beta Test: (This was suggested as a possibility on the Webinar conducted on August 25th) ATC believes that the SDT should perform a beta test to help the SDT understand the impact and potential cost associated with this proposal. In addition, a beta test would help the SDT work through the undeveloped elements of the concept and learn about any significant weaknesses or flaws with the concepts before including them in	ATC believes that the SDT needs to perform a Beta test and publish the results. The publish document should address our concerns at a minimum.

Name	Page	Line	Section	Comment	Suggestion
				mandatory Reliability Standards. This will also aid the industry to understand the potential impact in moving to this type of Reliability Standard.	
ATC-1j				The beta test should reveal the following: Comparison of existing Critical Cyber Assets to Cyber System that are classified as "High", "Medium" and "Low".	
ATC-1k				Does the number of Critical Cyber Assets equal the number of "High" Cyber Systems? If so, are they the same assets? If not, what is the difference?	
ATC-1l				What would be the cost to protect the additional "High" Cyber Systems using existing CIP standards?	
ATC-1m				What is the potential cost to protect "Medium" and "Low" cyber systems? (NOTE: It's our understanding that the SDT has not started to document what are the compliance obligations for "Medium" and "Low" cyber systems which may make determining cost difficult but the SDT should make a good faith effort to understand those cost.)	
ATC-1n				Partial Picture: The concept paper provides only a partial picture of the impact associated with this type of	The concept paper needs to provide more of the picture in order for the industry to understand the totality of moving this effort forward.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				fundamental change to the CIP standards because it does not get into the compliance elements (Cyber and Physical security) associated with the three "buckets". We believe that the SDT must provide a more complete picture of the changes before moving ahead with this concept paper. When the paper refers to the loss of a BES subsystem or subsystem element, it should be more clear that this only applies to loss of the subsystem or element due to a cyber system attack (e.g. take control over, block control of, falsify monitoring, block monitoring, change settings, etc.)	
ATC-1o				FERC Direct Changes: Given that FERC did not direct these changes, it would be very helpful for the SDT to identify why they feel it is necessary. (What problems or issues are being addressed because of this new approach? and, who believes them to be problems or issues?) ATC believes that the proposed concept paper is not needed to address the remaining FERC directives contain within Order 706, and that it would be best for the SDT to address the remaining FERC directives contained within Order 706.	The Concept Paper needs to better identify the purpose of this change along with why the industry should be supportive of this new proposal. ATC believes that the SDT should focus its attention on actual FERC directed changes and then consider if it is prudent to make this paradigm shift.
BGE-1				In definitions - need to add BES Reliability Functions	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
PSEG-2				The paper mentions "Critical Cyber Assets" in very few places, instead focusing on the phrase "BES Cyber Systems". Under the new concept, will all systems under the Target of Protection be seen as equivalent to Critical Cyber Assets in Versions 1 and 2, or are only those systems classified as BES Cyber Systems equivalent to Critical Cyber Assets?	
SOCO-1				In general, there is a concern that if we modify the standard to encompass so many more components, systems and subsystems, how will anyone be able to make this standard compatible with the interoperability standards/technology?	
SOCO-2				If this paper is used to revise CIP-002 will other CIP Standards be revised at the same time? It appears that the changes described in this paper would be difficult to use if Standards CIP-002 through CIP-009 are not revised to complement each other. As a result, the revised CIP-002 should become effective along with the other applicable revised CIP Standards, guidelines and implementation plans.	
SOCO-3				To be consistent with NERC's authority under the Federal Power Act, references to "reliability or operability" should be replaced with "reliable operability."	
TECO-				TEC would like to recognize the effort and	

Name	Page	Line	Section	Comment	Suggestion
1a				creative thinking of the Standards Drafting Team in creating the concept paper for categorizing cyber systems. We agree with and support the comments of the Edison Electric Institute related to this draft. In addition we would like to stress the following points.	
TECO-1b				1. The Concept paper introduces potentially significant change to the current methodology to determine cyber systems to be protected. This has the potential to increase the scope of work as standards CIP-003 – 009 are applied to the new set of cyber assets. It will significantly increase the effort required by the industry in terms of resources and costs. While we support the concept of the new methodology, we strongly urge NERC and the SDT to allow for and build in adequate time for the industry to come into compliance when drafting the actual revision to CIP-002.	
TECO-1c				2. In order to address the Technical Feasibility Exception issues, we believe the SDT will need to modify or allow for more use of or methods for providing mitigating controls to provide regulatory compliance.	
TECO-1d				3. We strongly support the SDT concept of ensuring that the security controls and	

Name	Page	Line	Section	Comment	Suggestion
				requirements be commensurate with the BES reliability impact of a particular cyber system.	
TECO-1e				4. It is unclear from the concept paper where the SDT is going with the routable protocol. We believe the SDT should use caution in evaluating expansion of the scope beyond that due to the vast amount of equipment in the field which does not have the ability to comply with the technical controls of CIP-003 – 009.	
TECO-1f				5. We strongly encourage the SDT to engage the security and SCADA/DCS systems vendors in the process of developing controls for these systems.	
TECO-2				Are Cyber Systems equivalent to Cyber Assets? That may need to be explained/defined in the document as the industry has been considering cyber assets.	It would at first appear that Cyber Systems relate to software/hardware that work together to provide certain functionality. However, in your examples, you list things such as relays, front end processors, etc. What is the difference between cyber systems and cyber assets. Can systems be discrete pieces of hardware?
SOCO-4	Gene ral	-	-	The term BPS is used in the "Defining Critical Assets" & "Defining Critical Cyber Assets" standards rather than BES.	Use a common term for the "system" throughout the standards.
SOCO-	3	14		Editorial	Replace "*Based on BES Reliability*" with "Based on impact

Name	Page	Line	Section	Comment	Suggestion
5					on BES Reliability".
AWEA-1	3	15	Executive Summary	It is concerning that the approach to cyber security standards outlined in this paper seems to supersede existing NERC efforts to develop cyber security standards. In particular, the processes that have already been developed for identifying and protecting critical cyber assets based on risk-based analysis seem like a valuable basis from which to work in developing future processes. A large amount of effort has already been devoted to developing these processes, which seem to be very effective and enjoy stakeholder support, and this paper does not offer any reason why these processes are inadequate and need to be superseded. The abrupt transition from existing cyber security efforts to the approach offered in this paper also exposes the industry to significant uncertainty about what form cyber security standards will ultimately take, reducing industry's ability to comply with these standards in an efficient way.	Risk-based processes that have already been developed for identifying and protecting critical cyber assets should form the basis of any newly proposed approaches.
ATC-2	3	35	Executive Summary	ATC does not believe that the concept paper identifies the FERC directive that this paper hopes to address.	The paper needs to clearly identify the FERC directive that is being addressed. In addition, the paper needs to identify the alternative approaches that were considered along with why the SDT reject the alternate approach.
SOCO-6	3	41		Editorial	"drafting team" should be replaced with "Standards Drafting Team (SDT)".

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
SOCO-7	3	50		Editorial	Define first occurrence of SDT.
ATC-3	4	20	Introduction	The following sentence is not clear: "FERC's comments in its Order 706 approving the Cyber Security Standards as well as common perceptions…"	What are the common perceptions being considered and who do they represent? The purpose of this effort should be to address FERC directives.
DYON YX-1	4	27	B	We believe the ALR definition is too broad for use in categorizing systems that impact the reliability or operability of the BES. For example, just because a BES infrastructure is not designed with sufficient capacity to supply "the energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of the system components" does not mean certain elements of the infrastructure need to fall under the CIP Reliability Standard. The issue is with the design, not the additional protection required.	Develop a more definitive set of reliability criteria for use in determining Critical Assets / BES Sub-Systems. Eliminate ALR # 6.
ATC-4	4	30	Introduction	ALR definition is too vague to be an acceptable basis for the CIP standards. For example: Item 2 – the definition/criteria for "performs acceptably" are open to wide interpretation and may vary for different conditions [Is the loss of less than 1,000 MW of load acceptable for cyber system contingencies?]; the definition/criteria of "credible Contingencies" are open to wide interpretation (including probabilistic considerations) [What level of cyber security allows the associated cyber	This effort should focus solely on those things that are essential/critical to the BES.

Name	Page	Line	Section	Comment	Suggestion
				system contingencies to be deemed not credible?]; Item 5 – the timeframe/criteria for "restored promptly" are open to wide interpretation, is restoration within a week acceptable for cyber system contingencies; Item 6 – the "ability to supply . . . power and energy . . . at all times" for any contingency is impossible whether it is a cyber contingency or something else; besides adequate has the meaning of the supply continuity being good enough, not perfectly.	
ATC-5	4	30	Introduction	A key premise of the paper is that proper cyber system security categorization is based on the identification of Reliability Functions that are essential to achieving an Adequate Level of Reliability (ALR). However, compliance with the NERC Transmission Planning Standards of TPL-001-0, TPL-002-0, and TPL-003-0 assures an adequate level of reliability is achieved for BES subsystems based on meeting acceptable system performance levels for different categories of contingency events for an appropriate range of system conditions. Bulk Electric Systems that are built and planned to meet these Transmission Planning Standards should not have any BES subsystems that are essential to achieving the adequate level of reliability characteristics. On the other hand, cyber attacks are expected to produce events that fall into the TPL-004-0 (Extreme Event) category of contingencies, which are not subject to any set of adequate reliability limits. If a set of acceptable system performance limits/characteristics would be developed for	This effort should focus solely on those things that are essential/critical to the BES.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				cyber attack contingencies, which are extraordinary, then it would be reasonable to expect these limits/characteristics would different from (beyond) the adequate level of reliability limits/characteristics.	
MGE-1	4	31-44	B	This section states that the NERC Adequate Level of Reliability (ALR) will be used as a test to see if a cyber system is required to maintain a reliable BES thus, to ensure ALR. Entities are to use ALR as a measure while formulating their BES Subsystem components to see the BES Reliability impact. All NERC Standards have this as an imbedded intent, which produces a reliable BES.	Identification of BES Subsystems is required to avoid instability, uncontrolled separation, or cascading outages. (as stated in section 215 of the Energy Policy Act authorized by Congress).
E-ON-1	4	35	B	The second BES characteristic requires the BES perform acceptably after "credible" contingencies. The term "credible" is too subjective and leaves the identification of BES functions far too open-ended. After the fact, any series of events or combination of events, no matter how improbable, can be said to have been a credible contingency.	Replace the word "credible" with "pre-identified credible."
GEEI-1	4	35	B	"Credible Contingencies" is not clearly defined	Define the term versus leaving REs to interpret.
SOCO-8	4	35		Editorial	Replace "credible Contingencies" with "credible events".
XCEL-1	4	35	B	ALR Characteristic #2 - please clarify what defines a "credible contingency".	Define "credible contingency"

Name	Page	Line	Section	Comment	Suggestion
E-ON-2	4	42-44	B	The sixth BES characteristic reads: The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components. E ON U.S. believes that this is not a characteristic of BES reliability. BES reliability requires that generation and load be balanced, not that the BES has the ability to supply the energy requirements of electricity consumers at all times. The ability to meet the demand of electricity consumers at all times is a measure of system adequacy and a characteristic of service, not BES, reliability. Section 215 (a)(4) of the Federal Power Act provides that [t]he term 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements. Section 215 does not mention maintaining an ability to supply the energy requirements of all electricity customers at all times. Including all cyber systems that support all the functions required to supply electricity to end use customers will greatly, and needlessly, increase the number of cyber assets subject to CIP requirements.	Strike characteristic six from the list. Only the first five characteristics of the BES set forth in NERC's definition of Adequate Level of Reliability are relevant to identifying the BES functions and BES cyber systems/

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				Cyber systems that support an electric utility's ability to supply the aggregate electric power and energy requirements of its electricity consumers at all times should not, for that reason alone, be subject to Version 3 CIP cyber security standards.	
FPL-1	4	46-49	B	These sentences give the impression that the objective/goal is to achieve all of the characteristics of the NERC ALR. It is inconsistent with the heading over the Executive summary section that says "an approach based on impact. The overall approach and process are useful and helpful. These sentences create concern and are a distraction from the balance of the paper which allows categorization based on impact and varying levels of protection.	
FPL-2	5	9		Phrase " if it directly performs one or more of the identified functions" speaks to identified functions which are not previously mentioned	"if it directly performs one or more of the functions contained in Table 1 on page x"
SOCO-9	6	11		Editorial	Replace "credible Contingencies" with "credible events".
GEEI-2	6	30-40	Figure 1	No mention of Distributed Generation	Future widespread implementations of distributed generation capabilities are likely. Include distributed generation as a potential BES subsystem if NERC feels that there is potential for impact to the BES.
GEEI-3	6	30-	Figure 1	No mention of Demand Response or AMI	Recognizing that this is potentially an out-of-scope item, improperly managed and/or secured Demand Response

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
		40			and AMI systems have the potential to have an impact on the BES. Include Demand Response and AMI systems if NERC feels that there is potential for impact to the BES.
ATC-6	7	15	Introduction	ATC does not agree with using impact of an event as the only attribute for determining categorization. We believe that entities should also be allowed to consider the probability of an events occurrence.	The paper must allow for the consideration of or credit for existing cyber and physical security investments.
DUKE-8	7	23		The paper states that nuclear are excluded. Since FERC has ruled that nuclear plants should be considered under CIP, his statement of exclusion is confusing. Are nuclear plants part of the analysis – or not?	
FPL-3	7	31-34		This is redundant and just repeats which was stated above.	Recommend removing.
SOCO-10	7	44		Editorial	Replace" standards drafting team" with "SDT".
ATC-7	8	15	Introduction	Why is the SDT replacing a probability approach to cyber security with a deterministic approach?	The industry deserves a complete explanation as to why the SDT is moving to this approach. (See our earlier comments)
IRC-1	8	15	B	Statement says: "this methodology parallels general approaches to risk management practices." Concur with this approach. The general risk analysis considers not only	Since this concept paper greatly increases the scope of the systems that will be auditable by NERC, suggest that business impact be a factor in the analysis to be a truly holistic risk methodology and approach.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				technical impact but also business impact. We already know that version 2 of the standards will remove business impact factors for risk analysis.	
DYON YX-2	8	17	C	Table 1: Contingency Reserve / Peakers: The "Unit capable of starting in 15 minutes or less" is not appropriate for application to the CIP Reliability Standard. Application of this provision gets into the "reliability" of the "Contingency Reserve" itself, e.g., the "reliability" of the components used to provide "reliability".	Eliminate the "Unit capable of starting in 15 minutes or less provision".
MGE-2	8	25 and 26	B	Do not agree with the below statement; "but should be prepared to have their assumptions challenged, as this represents a paradigm shift for experienced operating personnel". The statement may be proof that no matter how an Entity maps and identifies BES Subsystem, the Entity will be challenged by an auditor on their methodology. This is why the SDT must give the industry clear guidance on BES Subsystem identification.	Remove the statement.
PGE-1	8	26	B.	PGE believes that the Standard Drafting Team's efforts to introduce a "paradigm shift" to the CIP Standards is premature and unwarranted. PGE has invested significant time and resources in complying with Version 1 of the CIP Standards. Shifting to a new paradigm could result in significant changes to PGE's cyber security program, in some areas potentially forcing PGE to greatly extend that program beyond what is	

Name	Page	Line	Section	Comment	Suggestion
				necessary to maintain reliability and security. The Standard Drafting Team has not presented sufficient rationale to justify this potentially burdensome and costly paradigm shift.	
ATC-8	8	35	Introduction	The SDT needs to provide a more complete picture of the impact of this change in CIP Standards. What is the compliance obligations associated with "High, "Medium" and "Low". (Cyber and Physical)	More detail is needed
BGE-2	10			Table 1 - Section C - need to be stronger and form the matrix as a requirement not a suggestion	
E-ON-3	10	10-15	Table 1	As E.ON U.S. understands it, any generating unit, or combination of units with common mode of failure, with output in excess of available Contingency Reserves would be identified as a BES subsystem. It is often the case that generating units reside within the boundaries of a contiguous piece of property, often sharing, for example, bus work, other electrical interconnections, or common fuel supply. Table 1 suggests that all facilities within these multi-unit generation campuses would be deemed BES subsystems and thus all associated cyber systems would be required to conform to NERC cyber security requirements. This approach will result in a considerable increase in the number of systems, down to and including protective relays, that must comply with the as yet undefined Version 3 requirements. E.ON U.S. questions	Blackstart generating units only should be deemed BES subsystems.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				how many of these facilities are in fact essential to maintaining BES reliability.	
DYON YX-6	10	17/ 32	C	Transmission "busses" are too low of level of detail for relevant analysis. The entire transmission substation or switchyard is more relevant for analysis.	Eliminate "busses" from the BES Subsystem examples.
DYON YX-3	10	18/ 38	C	It is difficult to understand how a single "protective relay" can be a "cyber system" by itself that impacts the BES. A group of protective relays could certainly impact the BES.	Eliminate "protective relay" as an example of a "cyber system".
AWEA-2	10	18	Contingency/ Peaker Reserves	In the Contingency Reserve/Peakers Category, the criteria of "Unit capable of starting in 15 minutes or less" is identified. Almost any unit, even nuclear units, can "start" in 15 minutes or less. Few can reliably get to some designated load level in 15 minutes or less. That is the real test.	The criteria should be modified to clarify that it specifies that the plant be able to be dispatched a certain load level in a certain amount of time.
XCEL-2	10	18	Table 1	It is unclear the relevancy of the bullet "15 minute or less" in the criteria - what is this?	Clarify what justifies the "15 minutes or less" criteria and how it applies
RFC-1	10	19	C	For the "Contingency Reserve" row, "Criteria" column – It says "Unit capable of starting in 15 minutes or less". Doesn't the unit actually have to ramp up within 15 minutes to the amount of reserve it is supposed to provide?	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
DYON YX-4	10	21	C	We do not agree with inclusion of the following: "Transmission facility or facilities whose loss or compromise may result in the loss of resources identified for Contingency Reserves". Again, the application of this provision gets into the "reliability" of the "Contingency Reserve" itself, e.g., the "reliability" of the components used to provide "reliability".	We cannot agree that transmission facility or facilities whose loss may impact the resources for "Contingency Reserves" are applicable for the CIP Reliability Standard. Theoretically, this could be ALL transmission substations, etc. However, we can envision the identification of a transmission facility or facilities whose loss may result in the loss of the single resources that by itself exceeds the "Contingency Reserve" similar to the loss of transmission facility or facilities that impact the availability of a black start unit.
DYON YX-5	10	25	C	Cyber System Examples: "Plant control room" is not a good example of a cyber system. The definition of "control room", along with "control centers", is a troubling set of terms. It is not the "control center" or "control room" that is a "cyber system", it is the underlying "system" within the control room or control center that is important.	Eliminate "plant control room" term as an example of a cyber system.
DYON YX-7	10	29	C	We question the relevance of analyzing the loss of a single resource (or combined resource sharing a common mode failure) and the impact on under-frequency conditions. It is simply not a condition which occurs. In this scenario, voltage or VAR analysis will supersede any need for under frequency condition analysis.	Eliminate this scenario
AWEA-3	10	30	Load Balancing	In the Load Balancing and Frequency Response/Support Category, the phrase "Single resource or combined resources (sharing a common mode failure) whose loss or compromise may result in under-frequency" is used to identify	The test should be whether the loss results in unacceptably low frequency or rate of change of frequency.

Name	Page	Line	Section	Comment	Suggestion
				critical resources. Any unit, even of very small size may result in under-frequency if lost.	
RFC-2	10	30	C	For the "Load Balancing" row, "Cyber" column – Should AGC be listed separately or is it assumed to be part of the EMS?	
XCEL-3	10	30	Table 1	We are concerned b/c frequency response and support are difficult to characterize.	Clarify what the specific criteria for frequency response and support are
WE-1	10	40	C, Table 1	We do not consider a plant control room to be a cyber system.	Remove plant control room from cyber system examples.
RFC-3	11	11	C	For the "Voltage Support" row, "Cyber" column – Should EMS and UVLS be listed?	
DUKE-1	11	25		If Constraint Management is retained as a BES Function that is in the scope of this method, BES Subsystems to support that should include constraint management tools that the industry provides such as the Interchange Distribution Calculator.	
DYON YX-8	12	10	C	Control Center not applicable	Eliminate the use of the term "control center"….source of much confusion whereby the "systems" concept should resolve; see comment for Question # 1.
WE-2	12	10	C, Table 1	Cyber system examples: We use the acronym DCS for generation "distributed control systems".	Consider adding "distributed control systems" for generation assets as a cyber system.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
SOCO-11	12	28		Editorial	Replace "centre" with "center".
RFC-4	12	29	C	For the "Control and Operation" row, "Criteria" column last line – "centre" should be spelled "center".	
E-ON-4	12	30-40	Table 1	Table 1 suggests that the collection of status and alarm points the monitoring of which is essential to BES reliability is both a BES subsystem and cyber system. Such a classification would potentially necessitate applying the full suite of cyber security requirements to, for example, field wiring from RTU to alarm/status contact.	Clarify the intent of this section.
DYON YX-9	12	49	C	The term "element" is not clear	Eliminate the term element; too low of level of detail.
DYON YX-10	12	50	C	We understand that load is important to have in the restoration process but load is typically available from multiple sources and specific loads cannot necessarily be relied on for use in the restoration process.	Eliminate "load distribution feeders" from list of possible BES Subsystems; otherwise, this would imply ALL load feeders should be available.
DUKE-2	12	51		Distribution feeders should not be included – this greatly expands the scope of the standard.	
WE-3	13	20	C Table 1	Protective relays may or may not be "cyber systems". An electro-mechanical relay should not	Modify "protective relay" with "solid state" or "microprocessor based".

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				be considered a cyber system.	
RFC-6	13	24	C	For the "System Stability" row, "Cyber" column – perhaps EMS, SCADA, and RTU should be added.	
RFC-5	13	31	C	For the "System Stability" row, "Criteria" column – "wide-area spread are" should be "widespread area".	
E-ON-5	13	35-45		Water heater and air conditioner loads are sometimes controlled by utilities to lower demand during peak usage periods. Such programs complement and improve the efficiency of utility operations and ought to be encouraged. While conceivable such systems may be essential to BES reliability, in practice these tools are complementary and often far down the list of reliability tools relied upon by operators. Subjecting utilities to the potential penalties that result from violation of NERC standards risks discouraging the implementation of programs that would otherwise provide operator optionality and economic benefits to ratepayers.	Remove apparent presumption that DSM and load management systems are essential to BES reliability.
DYON YX-11	13	40	C	We are concerned about how these terms (load management control systems, Smart Grid, etc.) and offered for consideration.	We agree the design of Smart Grid infrastructures should consider large (> 300MW) single point "control scenarios".
SDGE-	13	45	Table 1	A BES Subsystem example that could be in-	As you know, there are many different types of "Smart Grid" systems, involving different types of equipment and

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
1				scope is shown as "Smart Grid"	functions on both the Transmission and Distribution systems. The term "Smart Grid" really needs to be defined more fully so that the intended audience can understand exactly what functions are being called out as "in-scope".
DUKE-3	13	48		It is not clear what is meant by Dynamic Feeder Management System – does this include distribution assets?	
DYON YX-12	14	10	C	We are concerned about measures to protect available "remote relay setting" provisions from cyber attack. We agree it is important but other than protecting the network with which they are accessible,	
GEEI-4	14	15	C	"Physical Security System" is listed under Cyber System Examples. As worded, it is not clear what the cyber element of the example is.	Change "Physical Security System" to Electronic Access Control Systems, Electronic Asset Access Control Systems, or similar.
RFC-7	14	17	C	For the "Other" row, "Cyber" column – Consider adding, "cyber systems like Distribution Management System (DMS), Windows Active Directory Servers, etc."	
IRC-2	15	28-32	D	Statement indicates that:" Identical cyber systems may also be implemented in different environments, resulting in different impacts on the BES functions they support. …a control system in a small generating facility may have a different reliability impact on the BES than an identical	There needs to be a clear statement related to the security of the interconnectivity between the control systems of all entities with those of the RC/BA/TOPs.

Name	Page	Line	Section	Comment	Suggestion
				control system operating a larger or several generating facilities." Should go further.	
BGE-3	16			Section E - mapping needs to be clarified to tell us the entity-determined criteria for graduating the impact scale will meet all compliance requirements	
DYON YX-13	16	15	E	Again, why have three (3) levels (see comment to question # 1). The NERC Bulk Power System Event Classification Scale in its current form is totally insufficient for this purpose. This is way too much detail.	We recommend caution be applied when using other terms or parameters from other Standards for application to the CIP-002. Something as sensitive as CIP-002, which has significant impact on the application scope of the CIP Reliability Standard, should be quite clear in their use of terms and definitions.
IRC-3	16	`17	E	Not sure why "situational awareness and operational control" are mentioned in the last part of the sentence.	Delete the phrase "such as situational awareness or operational control" from the last sentence.
SOCO-12	16	21		Editorial	Replace" standards drafting team" with "SDT".
GEEI-5	17	15-30	F	The examples lack detail and therefore are still vague.	Provide more detailed examples that REs can apply.
GEEI-6	19	N/A	G	Lack of clarity.	Detailed case studies or examples would be helpful.
DYON YX-14	19	15	G	We believe this type of classification is too detailed and not relevant for use herein. We are also not sure if the fact that a cyber system that	See comments from Question #1

Name	Page	Line	Section	Comment	Suggestion
				impacts multiple non-BES Sub-Systems "together" of which impacts the reliability of the BES is taken into consideration here.	
GEEI-1	19	24-32	G	Confidentiality, Integrity, and Availability carry different meanings in different contexts, even within the same system.	Add definitions to Appendix A that clearly define what NERC believes Confidentiality, Integrity, and Availability to be given the diverse sets of scope that encompass the BES.
GEEI-7	19	24-32	G	Confidentiality, Integrity, and Availability are not independent variables to be measured. One cannot rate a systems Confidentiality without also rating its Integrity, etc.	Make the language clear, or define the terms more clearly. Alternately, remove the terms. The statements hold meaning even after the removal of the three terms and replacement with a more generic "compromise" adjective.
EAGLE-1	19	35	G.	"This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES Subsystems as shown in Figure 3." Question: Does the methodology recognize that a single Cyber System may support a single function for multiple Responsible Entities? As an example, a single control room provides SCADA for 5 separate GOPs. Each Responsible Entity could categorize the single Cyber System differently based upon the affect the loss of availability of its generation to the BES.	
DYONYX-15	21	11	H	This approach is a single system analysis approach which misses the point. We just do not believe this concept is applicable for control systems and issues associated with the reliability of the BES.	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
ATC-9	21		Table 2	The logic of the evaluation matrix is inverted. For example, if the impact of a BES Cyber System on an associated BES Subsystem is "High", but the impact of the associate BES Subsystem on an associate BES Function is "Low", then the Cyber System Category should be "Low" because the resultant impact on the associated BES Function is "Low". An appropriate title and different row and column labeling of the evaluation matrix would help clarify the meaning and usage of the table. A suitable title for the table might be, "BES Function Impact". The better heading for the first row would be, "Subsystem Impact on BES Function". The better heading for the first column would be, "Cyber System Impact on BES Subsystems. For the 3x3 table example in the paper, the revised table would have one "High" cell, three "Medium" cells and five "Low" cells.	
IRC-5	21	Table 2	H	Header should be changed from "Asset" Impact to "System" Impact as the focus of the concept paper is on critical systems and not critical assets.	
WE-4	23	20	I	Interconnected cyber systems are a concern and need to be accounted for when they use routable protocol.	Change "Interconnected Cyber Systems supporting…" to "Interconnected Cyber Systems using routable protocol supporting…"
GEEI-1	23	29-30	I	"Non-repudiation" is part of integrity - it seems redundant to list them both.	Remove non-repudiation, and include non-repudiation in the definition of Integrity in Appendix A.
DUKE-	23	30		This paragraph introduces the concept of non-	

Name	Page	Line	Section	Comment	Suggestion
4				repudiation requirements in addition to confidentiality, integrity and availability – this seems like a further expansion of scope.	
DUKE-9	23	41		Are the Infrastructure Cyber Systems referenced here the Infrastructure Support Cyber Systems defined on p 32, line 43? If not, a definition is needed.	
NST-1	29	11-33	J ("External Cyber Systems")	We believe that declaring Responsible Entities would own and be responsible for mitigating risks associated with Target of Protection elements they neither own nor control would provide Entities with a powerful incentive to ensure they never include third-party cyber systems and/or interconnections in their defined Targets of Protection.	We believe that solutions to the problem of having to depend on and/or trust input from outside a given company's zone of control will likely require the establishment of bilateral or multilateral service level and information security agreements among Responsible Entities, perhaps under the aegis of NERC and/or Regional Entities. We recognize such efforts could be hampered by existing antitrust regulations and FERC constraints on information sharing, but we are convinced the current proposed approach will not achieve the SDT's goal of protecting third-party cyber systems and interconnections that are important to overall BES reliability and operability.
WE-5	29	20	J	Responsible entity with operational responsibility should identify and manage risk of the BES cyber system- requires additional dialogue.	More clarification of roles and responsibilities for both the BES cyber system owner and operator would be good.
IRC-4	29	25-28	J	Many utilities have third-party vendors providing key control system maintenance and operational support. While the utility may specify what security controls the vendor must provide, it is difficult and almost impossible for the utility to	The new standards should address a new category for key electricity sector vendors and require their compliance with applicable security controls to support reliable operation of the BES. For example, vendor EMS components should be designed and developed to allow

Name	Page	Line	Section	Comment	Suggestion
				enforce those controls on vendors and their staff.	compliance with CIP stds. Additional, the ERO and REs should be able to audit those vendor Operations and Maintenance centers to ensure compliance with applicable sections of the CIP stds.
PSEG-1	29	25	J	The example states (lines 25-30) that Alpha "owns the risk and has the responsibility to mitigate the risk…" Does that give Alpha the right to force Beta to endure a compliance burden, or does the example require Alpha to cover the compliance burden at Beta themselves? If Alpha and Beta do not agree, what sort of process will arbitrate the situation?	
DUKE-5	29	27		It is not clear whether this means Utility Alpha is responsible for protecting the interface with Company Beta from unauthorized access or if it means Utility Alpha is responsible for mitigating the risk of Company Beta's system being compromised.	
BGE-4	30			Section K - need clearer direction in applying the controls	
DUKE-6	32	35 and 40		What differentiates operations support workstations from HMI Workstations?	
XCEL-4	33	6	Definitions	The definition of "Collateral Cyber Systems" needs to be clarified to ensure the scope is not	Revise definition of collateral cyber assets to narrow the scope to those assets specifically connected to BES cyber systems within the same network that will fall under the

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				wide open.	same target of protection because of connectivity.
DUKE-7	33	11		The use of "evaluates" in this sentence does not make sense, and this seems to be the first place that the concept of resiliency is introduced in this paper. It seems this concept should be explained in section I if it is going to be used here.	