Individual or group. (137 Responses)
Name (97 Responses)
Organization (97 Responses)
Group Name (40 Responses)
Lead Contact (40 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (35 Responses)
Comments (137 Responses)
Question 1 (94 Responses)
Question 1 Comments (102 Responses)
Question 2 (96 Responses)
Question 2 Comments (102 Responses)
Question 3 (93 Responses)
Question 3 Comments (102 Responses)
Question 4 (95 Responses)
Question 4 Comments (102 Responses)

Individual
Jennifer Wright
San Diego Gas & Electric
Yes
San Diego Gas & Electric (SDG&E) agrees that it is appropriate to start with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a “medium impact” rating. However, SDG&E believes that it would be prudent to simply refer to the CIP-002-5.1 Impact Rating Criteria rather than restating it in CIP-014 Standard. Being more specific that this Standard is applicable to Transmission Owners that have any facilities identified as “medium impact” facilities under CIP-002-5.1 Attachment 1, Inpact Rating Criteria 2.4, 2.5, 2.6 and 2.7, would be clearer and more consistent with the general way that CIP-003-5 through CIP-011-5 are built upon the identification of “critical” facilities made in CIP-002-5.1. Linking the two explicitly, rather than simply restating the same language, would prevent the possibility that differences could creep into the rules over time as each Standard is modified.
Yes
SDG&E agrees with this approach. A facility’s identification as “medium impact” does not necessarily mean that the facility, if rendered inoperable or damaged could result in widespread instability, uncontrolled separation or Cascading within an Interconnection. Application of a risk assessment will ensure that CIP-014-1 is focused on the facilities that are most critical to the system.
Yes

SDG&E agrees that an evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified in R1 through R3 of the Standard is appropriate. Security threats and vulnerabilities can, and will vary from location to location and such differences must be accounted for in a robust security plan. It is appropriate and necessary that the Standard not mandate a one-size-fits-all approach, but requires entities to take into account the unique characteristics of each facility. SDG&E understands the Federal Energy Regulatory Commission's concern addressed by its Paragraph 11 directive that the Standard must have the analysis verified by an independent third party. While SDG&E believes it has in-house experts capable of performing such an analysis (as required by R4) and developing a Physical Security plan (as required by R5) adequately, SDG&E appreciates that verification by a third party, essentially a "second opinion," can serve to ensure a robust analysis of the physical security threats and vulnerabilities of facilities identified in Requirements R1 through R3. SDG&E appreciates the broad definition under R6.1 of what qualifies as a "unaffiliated third party reviewer." A list that unnecessarily limits possible reviewers could: 1) result in a bottleneck as too few potential reviewers are available for the industry to use; and 2) result in increased costs and a tight market for reviewers results in higher prices for their services.
No
Individual
Debra Horvath
Portland General Electric
Yes
Yes
The following comments relate to suggested modifications for Requirements 1-3 – PGE believes the 90-day period to ensure verification of the risk assessment is too short. It will be difficult for every Transmission Owner to establish a contract with an unaffiliated verifying entity during the implementation time period. In addition, the current wording of the standard puts the obligation on the Transmission Owner to make sure that the assessment is done within 90 days, even though by definition they cannot have control over that timeline. Therefore, PGE proposes replacing the R2.2 language, "[t]he Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment," with the language, "[t]he Transmission Owner shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from the completion of the Requirement R1 risk assessment." In addition, Requirement R3 provides no mechanism for the Transmission Operator who operates a primary control center identified by a different Transmission Owner to disagree with that identification. PGE proposes including similar language to that in R2.3 to allow for the Transmission Operator to document the technical basis for not identifying its primary control center as an asset to be protected.
Yes

In Requirement R4 the phrase “owns or operates” is used for the first time. If Transmission Owner Entity A is also a Transmission Operator of a line it does not own, and that line was identified by Transmission Owner Entity B in Requirement R1 and verified according to Requirement R2, Entity A could be responsible for evaluating and protecting that line under this wording. However, there is no mechanism built into the standard to communicate this information or to allow the Transmission Operator to dispute the decision. In addition, Requirement R4.2 should be changed to “[p]rior history of attack.” In addition, in Requirement R4.3, the current wording places an unrealistic and unclear burden on every Transmission Owner to monitor intelligence or threat warnings from an open-ended list of sources. We recommend changing the wording from “[i]intelligence or threat warnings from sources” to “[i]intelligence or threat warnings received from sources” to narrow the obligation to information that the Transmission Owner actually received from its monitoring activities. In addition, in Requirement R5, the phrase “owns or has operational control over” is used for the first time. It’s not clear why this needs to be different from the “owns or operates” in Requirement R4. Consistent terms should be used to decrease potential confusion. In addition, as above, PGE believes that the 90-day period to review each entity’s evaluation and security plan is too short. Again, we propose replacing the R6.2 language, “[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5,” with the language, “[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from completing the security plan(s) developed in Requirement R5.”
No
Group
Tennessee Valley Authority
Brian Millard
Yes
Yes
No
Comment: Proposed language to be added to the end on Requirement 6: This Requirement shall not apply to any Federal corporation or agency that meets any of the criteria in Requirement 6.1 and that has an Inspector General, pursuant to the Inspector General Act Amendments of 1988, appointed by the President of the United States and charged with oversight responsibility for such Federal corporation or agency. Comment: Recommend adding “with electric utility experience” as a reviewer qualification to 6.1.3 and 6.1.4.

Rationale: There should be a common standardizing qualification such as PSP, CPP, or electric utility experience that applies across the sub requirements of R6 that entities and the ERO can use as criteria to qualify unaffiliated third party reviewers.
No
Individual
Guy Zito
Northeast Power Coordinating Council
No
The applicability of the draft standard should be expanded to incude Planning Coordinators in addition to Transmission Owners and Transmission Operators. While NPCC agrees that TOs and TOPs simple application of the screening criteria to determine which facilities need analysis, they may not be able to conduct a complete analysis. The SDT should consider that Transmission Owners in some cases do not have the ability to conduct an analysis with a "wide area" view of consequences. Smaller TOs or TOPs only have an outside equivalent representation of the BES and could need help conducting their analyses. Consideration should be given to allow them to conduct the studies in conjunction with PCs.
No
The Rationale Box for Requirement R2 stipulates that "'unaffiliated' means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission o(O)wner)." This conflicts with Requirement R2 Part 2.1 which lists "A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or An entity that has transmission planning or analysis experience" as those qualifications for an unaffiliated verifying entity. Clarification is needed that an Independent System Operator that has operating authority over an entity is eligible to be the unaffiliated verifying entity.
No
Regarding Part 5.1, the requirement states that the security measures should be designed to deter, detect, delay, assess, communicate and respond to potential physical threats. NPCC suggests removing the obligation to 'deter' from this Part and establish a separate Part that addresses deterrence and very basic specifics regarding what constitutes deterrence. The new Part could describe how an entity should implement deterrence and consider some minimum auditable criteria; for example, Consider and Implement measures designed to deter potential physical threats including 1) perimeter control 2) motion detection 3) lighting 4) access control. In this manner the ambiguity surrounding the term 'deter' is eliminated. Part 5.3 should allow flexibility to modify the time line. Suggest that Entities should 1) have a master Physical Security Plan; 2) have the flexibility to accomplish mitigation activities associated with the results of the vulnerability assessment, and 3) capture those mitigation plans under a separate mitigation plan (similar to the action plans for Cyber Assets vulnerability assessments) or include "associated modifications to the time line".

Yes
It is NPCC's expectation that RAI concepts will be applied to the operating and enforcement of this standard.
Individual
Greg Froehling
Rayburn Country Electric Cooperative
No
Overall comment is this is too complicated of a draft standard for a 90 day consensus! Keep it simple. I agree with the functional entitiy that is identified however, I would add GO to address any "critical" switchyards that may exist that are not owned by a TO. I also agree with the scoping of the facilities similar to the CIP V5 criteria with the following exception, apparently a list already exists for the substations that should be considered "high" do they deserve an alternative approach to what is within this standard? Altering the existing basic approach as follows: Since the FERC order allowed for "One or More Reliability Standards", it would be appropriate to address the "High " facilities separate from the "Medium Facilities". This approach would make it an easier task to file the "high standard" within the 90 days then follow with the "medium later". Thus giving more time, latitude and maneuverability to address issues that arise specific to those facilities.
No
I agree with the risk assessment in concept, the standard has far too many requirements and sub requirements to accomplish the task. Since initial analysis apparently this has already been done for the "High Risk" stations, a more efficient approach would be for the RC to perform the analysis based on the criteria mentioned to validate findings and find any second contingency facilities that may not have been identified. Since the RC is the "Reliability Coordinator", this is your third party identifying facilities without bias… Determinations will be based on an engineering basis utilizing standard uniform criteria across North America. The same analysis occurs for all entities within all regions, no variations this would yield consistency! Then the RC notify the entities that they have facilities that have been identified. (much like other NERC standards) Thus the information on which facilities have been identified would disseminated and controlled in a much more secure and better controlled environment while still maintaining the quality and consistency of the study needed.
No
Once the in scope facilities have been identified, it would be best for the entites to use the same resources for the evaluation of "Potential Threats" since this language has endless possibilities. i.e. Aerial attack, induced seismic events to name a few to illustrate "Potential". I favor the wording of "reasonable risks" The FBI, DOE or DHS should be involved in the discussion with the entities in lieu of a third party who is only subject to confidentiality agreements and also has interests beyond mitigating the true risks.
Yes

I think the standard IF broken up into 2 standards (High, Med) should provide clearer guidance as to the expectations of the plans content. Similar to the issues that arose with the Low assets in CIP V5 . Give basic structure and content to be addressed to give FERC the assurance the specific concerns have been met.
Individual
William H. Chambliss, member Operating Committee
Virginia State Corporation Commission
Yes
Yes
There does not seem to be any timeframe within which the initial assessment is to be completed under R1, nor when the 30 and 60 month periods for subsequent reassessments under R1.1 are to begin and conclude.
No
R4.2 requires each Transmission Owner of an identified facility to "consider" and "Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events." Is such consideration to be given to other "similar facilities" of the specific Transmission Owner or of any Transmission Owner anywhere in North America? How will such "consideration" be possible if the scope of such consideration is intended to be the latter? R5 is fine, but R6 suffers from the same ambiguity as R4.
No
Group
None
Terry Volkmann
Yes
No
The SDT has not factored in the resiliency concerns stated in the FERC order. Many of the facilities selected by the initial screening process will have long lead time equipment that if damaged will be out of service for several months. The assessment process needs to consider the operational risks during the time that the TO is waiting for replacement equipment. R1 should be amended to include the following sub-requirement. If the facility being studied has long lead time items, i.e. 4 months or greater, the study must include an N-1 analysis for the widespread instability, uncontrolled separation, or Cascading within an Interconnection test. In addition, the premise for this standard is a physical attack resulting in faulted equipment. There is no mention of the assessment being conducted for the Facilities under fault

conditions and in many cases under delayed clearing. R1 should be amended to include the following sub-requirement. The analysis of the subject Facility must include dynamic simulation of faulted conditions with delay cleared for the most severe contingency within the Facility. The phrase "instability, uncontrolled separation, or Cascading" is core to the definition of Interconnected Reliability Operating Limit (IROL). Every RC and PC has an IROL methodology under the FAC standards. R1 should be amended to include the following sub-requirement. The test for instability, uncontrolled separation, or Cascading must be consistent with the IROL methodology established by PCs and RCs under FAC-010 and FAC-011.
No
It is recognized that a one–size–fits all approach is not practical. However the proposed directives as to what should be included in physical security plans are so general that little is likely to change from current practices that are insufficient to protect very critical high risk substations. The only language directive in CIP-01401 is listed on Pg. 10, R5 para 5.1. More definitive guidelines must be outlined if improvements are to really be achieved. The utility industry has used real-time remote monitoring of substation equipment for reliability purposes for decades. Similar technology is available for the very important physical security function. The following sentence needs to be added at the end of paragraph 5.1. “Security measures must include isolation zones of sufficient size covering approaches to substations, in addition to monitoring inside substation fenced areas, to detect both attempted and actual penetration of critical sites and the surrounding buffer areas. The areas must be patrolled with real time monitoring & assessment equipment designed to provide live and playback/recorded video that must be automatically presented to alarm station operators. Detection equipment must include gunshot detectors. Sufficient real-time surveillance must be provided to allow sufficient time to implement a tactical response plan to minimize and interrupt threats.”
No
Individual
Steve Hamburg
Encari
Historically, FERC and NERC have taken the position that redundancy is not an acceptable criterion to exempt a Critical Cyber Asset from mandated physical or cyber controls. Redundancy is not supposed to be a factor in the determination of the criticality; instead redundancy is used to improve reliability and availability. This principle should be extended to the protective measures applicable to control centers under CIP-014-1. So long as both the primary control center and backup control centers meet the bright line criteria for a medium impact rating under CIP-002-5.1, the protections under CIP-014-1 should apply equally to both the primary and backup control centers.
No

There should be a strong, rebuttable presumption that an applicable Transmission Facility requires physical protection owing to its classification under the bright-line "medium impact" rating criteria under CIP-002-5.1 (which is repeated in the Applicability section of CIP-014-1 for Transmission Facilities). The utility of a risk assessment could be recognized, however, as justification for rebutting the presumed need for a set of mandated physical security measures.
No
The approach taken by the Nuclear Regulatory Commission, which prescribes specific physical protections for nuclear plants and materials in 10 CFR Part 73, is instructive. Applicable Transmission Facilities, which are subject to common potential threats and vulnerabilities, warrant minimum physical security protective measures. Physical security plans should incorporate those prescribed protective measures unless a responsible entity can establish that its validated security plan provides a comparable level of protection required by the Standard.
Yes
CIP-014-1 should expressly permit one well-coordinated physical security plan for a Transmission Facility. As proposed, there could be a separate physical security plan under CIP-006-5 for BES Cyber Systems within an applicable Transmission Facility and potentially another physical security plan for the Transmission Facility as whole under CIP-014-1.
Individual
David Ramkalawan
OPG
No
In the applicability section of the proposed standard, does the exemption refer to the Nuclear Generation Facility or the Transmission facility to which the Nuclear Generation Facility is connected? In Canada the Canadian Nuclear Safety Commission has no jurisdiction over the Transmission Owner/Operator; therefore the intent of the standard has to be made clear on this point.
Yes
Yes
Yes
Individual
Ralph Meyer
The Empire District Electric Company
Yes

EDE feels this is the right approach on selecting a threashold for applicability to this standard.
Yes
Yes
No
Individual
Kalem Long
The Empire District Electric Company
Yes
Yes
Yes
Yes
Individual
Mike Kidwell
Empire District Electric Company
Yes
Yes
Yes
Yes
Individual
Candace Morakinyo
We Energies
Agree
Edison Electric Institute (EEI)
Individual
Ronnie C. Hoeinghaus

City of Garland
Yes
Yes
No
Clarification - R6.2: Need to clarify that “completing the security plan(s)” does not include completing the tasks outlined in the time line developed in R5.3 – the time line is required to be complete as part of the plan but not the tasks in the time line.
Yes
Recommendation # 1 – Include the timeline diagram located in the FAQ document titled “CIP-014 Physical Security Process Flow” in the Guideline and Technical Basis section of the standard. This diagram clearly demonstrates the timing between the different requirements. Because of the subsequent risk analysis’s in R1, verifications in R2, and potentially the processes outlined in R3, R4, R5, & R6, questions on timing (answered by the diagram) potentially will arise throughout the life of the standard. Recommendation # 2 – Add the words “catastrophic failure” to the Purpose statement. On a webinar, there was discussion concerning the Purpose statement and it was stated a number of times that “widespread instability, uncontrolled separation” meant to convey the concept of “catastrophic” – there will be a lot of folks involved in the implementation of the standard who did not hear the webinar comments. Recommendation # 3 – Rather than the term “primary control center” used in all the proposed requirements, use a different term or phrase such as the “facility that has direct Supervisory Control”. The word “direct” in the recommendation of “direct Supervisory Control” should replace the need for the word “primary” - primary makes one think of primary and backup (which is not addressed in the standard). The concern with using primary control center, even though “control center” is not capitalized, brings up a mental picture of primary (and backup) Control Centers as defined in the NERC glossary. The standard should be straight forward, not using terms that can be confused.
Individual
David Rudolph
Basin Electric Power Cooperative (BEPC)
Yes
Yes
R2 – A concern to consider is whether there is an adequate pool of unaffiliated third party verifiers to meet the 90 day timeframe. Possible solutions would include (1) increase the 90 day requirement to six months; or (2) Revise the requirement to allow the NERC Registered Entity to notify the appropriate Regional Entity of the verifier pool constraint and request the Regional Entity act as the verifier or specify an acceptable alternative.

Yes
Yes
The SDT should be applauded for the diligent work performed in short order to meet the requirements of the FERC order RD14-6-000 while allowing flexibility in the manner the Registered Entity may be compliant.
Group
Edison Electric Institute
David Dworzak
Yes
Yes
Yes
Yes
EEI supports the draft standard CIP-014-1 as fully responsive to the FERC March 7 order. The project has moved along a very aggressive timeline and naturally raises a broad range of practical and implementation issues. Based on extensive discussions with member companies, EEI recommends that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify for companies several questions on the timing of the various implementation stages of the standard, including especially that security plans are subject to change over time for a broad range of reasons. In addition, EEI asks the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. Observing the many meetings and webinars that have taken place recently, EEI also recommends that the SDT consider adding language in the implementation guidance around the application of the terms 'control center,' 'primary control center,' and 'transmission station' in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms.
Group
Southwest Power Pool Regional Entity
Bob Reynolsa
No

SPPRE does not agree with the applicability because it excludes certain facilities that could pose a significant risk to the BPS reliability if rendered inoperable or damaged as a result of a physical attack. Other facilities that should be applicable are those where high impact BES Cyber Systems are found. Additionally, any Special Protection System and automatic load shedding system capable of shedding 300 Mw or more should be included. Reference CIP-002-5 Attachment 1 (Impact Rating Criteria 1.1, 1.2, 1.4,2.9, and 2.10). SPPRE also disagrees with the decision to limit applicability to only the primary control center.
No
SPPRE believes that greater clarity is required with respect to the risk assessment to be performed. At a minimum an extreme contingency study needs to be performed that takes out the entire facility, all voltages present. The study should also not consider any operating guides or other mitigation when evaluating the impact of the outage. In Section 2.3 technical basis should be changed to engineering basis. Additionally, the unaffliated verifying entity should not be the party performing the original study, under the principle that an auditor cannot audit ones own work; to do so would not be consistent with the expectation of verification by an unaffiliated entity.
No
SPPRE disagrees with the inclusion of Requirement 4.2. Prior history is not a predictor of future events and could result in critical facilities not being protected until after a sucessful first damaging attack with adverse BES reliability impact. Requirement 5.3 should be a project plan with measurable milestones for implementing the physical security enhancements and modifications.
Yes
SPPRE recommends that subsequent risk assessments should be peformed at least every 36 calendar months regardless of whether previous risk assessments had identified critical facilities. It is more important to identify facilities that should be on the list than those that might not need to be on the list anymore.
Individual
Randi Nyholm
Minnesota Power
Yes
Yes
Yes
Overall Minnesota Power agrees with the approach laid out by the Standard Drafting Team in Requirements 4-6, but requests that the SDT consider modifying the wording of R5.1 as follows. Resiliency or security measures designed to deter, detect, delay, assess, communicate, or respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4. An auditor could interpret the use of “and” in

"…deter, detect, delay, assess, communicate, and respond…" to mean that each resiliency or security measure be designed to meet all of these, where we believe and hope that the intent of the sub-Requirement is that the resiliency or security measure identified in the physical security plan be designed to "…deter, detect, delay, assess, communicate, or respond…", while recognizing that it may meet more than one.
No
Individual
Bob Thomas and Kevin Wagner
Illinois Municipal Electric Agency
Agree
Florida Municipal Power Agency American Public Power Association
Individual
Jack Stamper
Clark Public Utilities
No
Section 4.1.2 of the Applicability section states "Transmission Operator." This reference in the Applicability section should be more specific based on the the actual conditions under which CIP-014 would be applicable to a Transmission Operator. Clark suggests the reference should be revised to "Transmission Operators that have operational control over the primary control center of a Transmission station or Transmission substation identified in section 4.1.1."
Yes
Yes
No
Individual
Frank Pace
Central Hudson Gas & Electric Corporation
Yes
No
In regards to R2.2 as currently drafted, the unaffiliated verifying entity should have to ensure verification within 90 days and not the TO, since it is that entity performing the verification. In regards to R2.3 as currently drafted, there appears to be a lack of an appeals process in cases

of disagreement between the unaffiliated verifying entity and the TO concerning the recommendations formulated by the unaffiliated verifying entity.
Yes
No
Individual
Earl F. Cass
EF Cass Consulting Inc.
No
the applicability section table should be modified by either removing the 500kV line or making it a 3000 value. By giving it a 0 value in the table it send a different message than the text indicating all 500kV facilities are in. Also, in the draft RSAW Compliance Assessment approach for R1, it would appear that a Transmission Owner needs to comply with R1 and R2 in order to determine if the standard applies to them. If an entity is required to have a process for determining applicability then it needs to be a requirement. The applicability section should produce a yes or no answer. I spoke with Nick Webber of WECC and his response back was "Much like the requirement of all entities to apply CIP-002, all entities registered as for the TO function must complete CIP-014-1 R1 and R2. Each TO must complete R1 to determine if R3-R6 apply. The TO then must subsequently have that R1 assessment reviewed as required in R2." An entity should not have to comply with 2 of the requirements in order to determine if the standard applies to them. If all TOs are expected to comply with R1 and R2, then move the criteria into the requirement, if that is not the intent, clarify that once an entity reviews the applicability section and determines the standard does not apply they are finished. The rationale for requirement R1 indicates the criteria is in R1 when it is actually in the Applicability section.
Yes
This standard has the perceived importance of protecting national security and being so critical as to expedite its development through modification of nearly all associated controls. I agree physical security of critical facilities is of paramount concern but not at the expense of producing a sound standard. After listening to two of the webinars it is clear to me that the majority of the entities responsible for ultimately complying with this standard and those that will enforce the requirements are unclear as to what is required. I would suggest running it past the "Experts" for their review prior to the first vote.
Group
Tampa Electric Company
Ronald L Donahey

Yes
Yes
Yes
Comments to R5 Tampa Electric Company appreciates the excellent work of the standard drafting team (SDT). They and their support staffs have evidently worked very hard to produce in a very short time a family of documents that create a workable framework for improving the physical security of Transmission substations and primary Control Centers. We also commend NERC and the SDT for reaching out to the industry through a live a technical conference and by conducting a series Webinars in local and national venues. Moreover, we fully support the intent of the SDT as it has been articulated so well in the technical conference, in NERC and FRCC Webinars and in EEI and NATF conference calls. Unfortunately, there is a critical ambiguity in the text of requirement R5 that is problematic and needs to be addressed by the SDT. Our main concern is that requirement R5 literally reads that all provisions of the security plans for our primary control center and for all our substations and switchyards, including the installation and construction of any physical security upgrades, must be completed "within 120 calendar days following the completion of Requirement R2." Such a requirement may well be impossible to meet depending on the extent of the upgrades, the need for facility outages, and the number of locations that are affected. Members of the SDT have made it very clear in the Webinars and conference calls that they did not intend this result. Instead, the SDT intended to require registered entities, "within 120 calendar days following the completion of Requirement R2," to develop and document plans that include definite timelines for completing any security upgrades that are necessary to protect against the vulnerabilities and threats that are identified under requirement R4. Given that the text of R5 is contrary to the intent of the SDT, Tampa Electric urges the SDT to clarify that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. This clarification can be accomplished in the guidance document to the standard or by our preference, editing the text of the standard and issue a revised standard for a second ballot. Removing "and implement" from the text of requirement R5 should remove the ambiguity and conform the text to the intent of the SDT. This edit, combined with R5.3 expresses the SDT's intent on this issue: R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following

attributes: [VRF: High; Time-Horizon: Long-term Planning] 5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

Yes

Comments: Comments to Definitions Tampa Electric also urges the SDT to define certain terms that appear in the standard: 1) “Transmission substation” and “Transmission station,” 2) “collector bus,” and 3)“primary control center. There terms are not defined in the NERC Glossary and may not have definitions that are universally accepted by the industry. “Transmission substation” and “Transmission station” Many industry practitioners use the term “Transmission substation” generally, whether or not any transformers are installed in the facility they are describing. Other practitioners apply the term “Transmission substation” only to facilities that include transformers. The standard implicitly uses the term “Transmission station” in reference to transmission switching arrangements that do not involve transformers. However, the more commonly used term for a transmission switching arrangement that does not include transformers is “Transmission switchyard.” NERC addressed this issue in the Guidelines and Technical Basis section of CIP-002-5. The SDT could easily carry that text over to the Guidelines and Technical Basis section of CIP-014-1. However, it would be better to add definitions for “Transmission substation” and “Transmission station” to the Glossary of Terms Used in NERC Reliability Standards. The relevant text in CIP-002-5 is copied below for the convenience of the SDT. CIP-002-5 Guidelines and Technical Basis clarifications of “Transmission stations” and “Transmission substations” The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist. “Collector bus” “Collector bus” is another term that is not defined in the NERC Glossary and that may not have a definition that is universally accepted by the industry. “Collector bus” appears in 4.1.1.1 and in 4.1.1.2. of CIP-014-1 in text that was carried over from CIP-002-5. 4.1.1 Transmission Owner that owns any of the following: 4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added] 4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added] If “Collector bus” is not defined or clarified, some TOs may conclude that some part of

every transmission substation or switchyard that receives the output of a generator(s) is excluded from the scope of the standard. However, that is not the case nor the intent of the SDT. Therefore, the drafting team should consider whether it should define or clarify in the guidance document, the term “collector bus” “Primary control center” The NERC Glossary defines “Control Center” in this manner: One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. What might not be clear for the purposes of CIP-014-1 is what exactly distinguishes a “primary control center” from other alternate “Control Centers.” Some registered entities can operate substations from multiple locations. Often, there is one self-designated “main control center” or “primary control center” for which there might be multiple alternate or “backup control centers.” Given that alternate or backup control centers have capabilities that are comparable to so-called main control centers, it might not be clear in some systems whether “primary control center” in CIP-014-1 applies to more than one Control Center. The SDT can solve this problem by adding a definition of “primary control center” to the NERC Glossary or by adding text to CIP-014 that for each critical substation the TO or TOP can designate any Control Center as the “primary control center.”

Group

Black Hills Corporation Entities

Bob Case - NERC Compliance Manager , Bob.Case@blackhillscorp.com

No

Black Hills Corporation (referred to as BHC hereafter) believes that Section 4.1.1 has appropriate applicability specifics, but Section 4.1.2 only says “Transmission Operator”, which initially implies a much greater scope. Request that similar to Section 4.1.1 styling, Section 4.1.2 alternatively state “Transmission Operators notified by a Transmission Owner according to Requirement R3.”

No

Although BHC agrees with the overall approach, it has significant concerns regarding the use of the term “risk assessment” without a clear definition of intent. CIP-002 regulatory expectations in the Western interconnect for RBAM have consistently referred to the classic risk definition as “risk” times “probability”. However, the further expectation is that the probability of an event is assumed to be 100%, such that the “risk” them becomes equal to the “impact”. CIP-014 does not currently lay out the same expectations, which could allow Transmission Owners and other affected (or unaffiliated) parties to disagree over the role of “proabability” in defining risk. This problem can be resolved in the CIP-014 draft by: 1. leaving the risk assessment language as is, but adding the above statements about “probability” of occurrence being 100%, or 2. changing all references of ‘risk assessment’ in the standard, to ‘impact assessment’, or 3. leave the risk assessment language as is, but make it clear that CIP-014 is deviating from the historical CIP-002 RBAM definition of risk, such that the probability

of the event can change the perceived risk (and that such an interpretation is congruent with the FERC order. This last option seems to be closest to the intent of Paragraph 8 in the FERC directive, but represents a significant departure from past NERC CIP guidance, and needs to be highlighted as such. As written, the TO has exclusive determination say in identifying applicable Transmission stations, substations and primary control centers. R2 speaks to a third party verification of that assessment, but Black Hills believes that coordination of the BES would be better served by having the TO & TOP reach a consensus on the assessment, prior to having the assessment validated by a third party. Requirement 2.1 directs the Transmission Owner to select an unaffiliated Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. Firstly, Planning Coordinator does not appear in the NERC functional registry and should not be casually equated with the TP and RC functions; without first equating the Planning Coordinator to the PA function per the NERC glossary. Secondly, none of these NERC functional entity designations appear in the applicability section of the standard. Therefore, it can be assumed that the unaffiliated PC, TP, or RC are not obligated to conduct the assessment themselves, but rather the assessment is conducted by mutual agreement of the TO and unaffiliated PC, TP, or RC acting as third-party assessor. If this is not the correct assumption, then the PC, TP, and RC functions should be noted in the applicability section. If the Transmission Owner is affiliated with the Transmission Planner and Planning Coordinator, then the third-party review should be performed by the entity's Reliability Coordinator. The reference to "primary control center" is adequately explained in the rationale section of R1, but confusion between it and "back-up control centers", "emergency dispatch center", and those control centers that can only monitor status seem to justify an up-front definition in the standard. Recommend that a special definitions section be added, or the term be clearly defined at its first instance in Section 3. R2.4 could benefit from some added guidance regarding the protection of sensitive or confidential information. Is the intent to employ the entity's baseline confidentiality banner, or something more robust such as that required by CIP-003-3 R4 or CIP-011-1. The latter seems more appropriate for this CIP standard.

No

BHC has the same concern with R4 as expressed in the opening comment of the previous section regarding the definition risk assessment. The tailored evaluation required by FERC directive paragraph 8 introduces a probability of less than 100%, which is in conflict with prior NERC guidance on risk definition. As previously noted, if the unique probability of a threat is to be taken into consideration along with the impact, this change from CIP-002-3 expectation should be clearly highlighted. In addition, the inclusion of probability in the risk assessment will increase disagreements between unaffiliated entities, which will require a mechanism for resolution. BHC questions R4.2: The current language states "Prior history or attack". BHC believes this opening should state "Prior history of attack" because the current language does not provide an indication of what 'prior history' is being referred to. BHC agrees with the AZPS suggestion that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions, which would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. BHC believes that the

120 day requirement for R5 should be limited to the development of the security plan, and that full implementation should be dependent on the complexity of the plan. Implementation timing of the entity's plan should be approved by the applicable RC. Provisions could be added for temporarily derating the facility, if the implementation timing were considered by the RC to be excessively long. By mandating a 120 day implementation, entity's security plans may be down-sized to meet the 120 day implementation window, rather than to meet the potential threats and vulnerabilities at the facility. If "implementing" only means the specific deliverables of R5.1, R5.2, R5.3, and R5.4 (i.e. the timeline required by R5.3 is created, but not executed), then "implementation" needs to be more clearly defined. BHC has a further concern that R5.1 language reads too close to the "Identify, Assess, Correct" language already remanded by FERC in the CIP v5 standards. Alternative language for R5.1 might be "Resiliency or security measures designed to prevent potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." This simplification is not expected to change entities efforts, but could be more appealing to FERC. BHC agrees with the reasoning of AZPS to simplify R6.1 to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise." If this language consolidation is not acceptable, then alternatively recommend that Section 6.1.1 be expanded to include other similar certification providers, e.g. the National Sheriffs' Association Institute for Homeland Security offers a Certified homeland protection Professional (CHPP) designation (https://ndpci.us/certification/CHPP_Certifications.php), so as not to appear preferential.
No
Individual
Ayesha Sabouba
Hydro One
Yes
We agree with the Applicablity. R1 has provided flexibility in the assessment method.
Yes
Subsequent risk assessments should be performed every 36 months (to align with CIP requirements) instead of every 30 months. The FERC Order allows for the verification to be completed by NERC, the Regional Entity, an RC or another entity. The standard only identifies that the verification can be completed by a registered Planning Coordinator, Transmission Planner, or Reliabity Coordinator, or an entity with transmission planning and analysis experience; it does not mention NERC or the regional entity.
Yes
The Standard allows the TO and TOP sufficient flexibility to complete R4, R5 and R6.
Yes
Will FERC accept R2.3 and R6.3, which allows the TO or TOP to document why they are not following the recommendations from the verification? The FERC Order did not suggest this. It

is extremely important that all jurisdictions follow the same standard, so that the mitigation of risk to physical security is consistent. Having some jurisdictions who follow a more stringent standard will increase costs to ratepayers in those jurisdictions. The standard should provide a definition for “unaffiliated”.
Group
ERTF
Joe Tarantino
Agree
The following comments are in agreement with LPPC and ERTF as well as comment from our own entity LCRA: • Use of “primary control center” is ambiguous (R1.2 and others); • Unaffiliated third party review needs to be longer than 90-days, suggestion to be 180-days (R2.2); • Issue with non-disclosure agreement vs. Public Power’s obligation to disclose information (R2.4); • Expansion of the Security Plan third-party reviewer to include those functions that are identified in Requirement 2.1 (R6.1). • The standard does not address substations/stations that are owned by multiple Transmission Owners. LCRA TSC recommends adding language describing NERC’s expectations associated with jointly-owned substations/stations or substation/stations with multiple asset owners.
Individual
John Falsey
Invenergy LLC
Agree
NPCC
Individual
David Kiguel
David Kiguel
No
1. For clarity suggest that the word “verify” be changed to “confirm” in sub-requirement 2.2 so that it reads: “The unaffiliated verifying entity shall either confirm the Transmission Owner’s risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). 2. Sub-requirement 3.1 should cover both, addition and removal of elements from the identified facilities list. Suggest changing to: “In the case of addition(s) to, or removal(s) from the identified Transmission stations or Transmission substations list developed under Requirement R1 and verified/modified according to Requirement R2, the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the change(s).”
No

Sub-requirement 6.1.1: While Certified Protection Professional (CPP) or Physical Security Professional (PSP) might be recognized certifications in the U.S.A., that is not necessarily the case across the Canadian Provinces. Recommend to add: “or equivalent in those jurisdictions where such certifications are not recognized.” Sub-requirement 6.4: In addition to the non-disclosure agreements referred to in this sub-requirement, the standard should specify that the reviewing individuals having access to the confidential information must have security clearance and training, similar to the requirement in other CIP standards. Also, the security clearance must be obtained according to the established procedures in the respective jurisdiction.
Yes
The Implementation Plan obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. While performing and completing the vulnerability assessment before the effective date of the standard may constitute a recommended good practice, from a statutory perspective, compliance with the standard before its effective date may not be enforceable in all jurisdictions. An entity cannot be found in violation of the standard at a time when the standard is not yet effective. Recommend changing the implementation plan to require completion of the assessment after the effective date of the standard.
Group
JEA
Tom McElhinney
Agree
APPA
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
National Rural Electric Cooperative Association (NRECA)
Yes
Seminole supports the comments by NRECA. Additionally, Seminole supports the use of CIP-002-5 medium impact criteria for use in CIP-014. CIP-002-5 has at least one issue that will apply to CIP-014 as well. There are multiple ways to interpret the phrase Transmission Facility. One example is clarifying what is in the scope of a Transmission Facility. The definition or other documentation should state that the substation is exclusive of the criticality of any connected substation and clarify that a Transmission Facility as used here does not include Transmission Lines.
Yes
Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. As this standard is based on the same standards as the impact ratings in CIP-002, it would be cleaner to identify any facility that is determined critical under the Assessment with a separate (non-exclusive) impact rating such high physical impact and use this term for applicability for R3-R6. If an entity has a qualified third party perform the R1 assessment on

behalf of or in cooperation with the registered entity, does this also meet the requirement R2? Note that the draft RSAW, not under review here, states that R1 and R2 may occur concurrently. R2.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R1.
Yes
Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. Requirements R4.1, 4.2, and 4.3 should be moved to the guidelines and technical basis as there is excessive flexibility provided to the auditor for concluding whether the evaluation is adequate and potential that an auditor may choose to determine that identification of events was inadequate. R5.2 requiring law enforcement contact information is redundant with EOP-004-2 R1. If an entity has a qualified third party perform the R5 security planning on behalf of or in cooperation with the registered entity, does this also meet the requirement R5? R6.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R
No
Group
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing
Marcus Pelt
Yes
Yes
Yes
Yes
Clarification should be made in the implementation guidance for CIP-014-1 that Verifiers who are also Registered Entities in functions applicable to CIP-014, are not subject to penalty under the requirements of CIP-014 due to verification duties performed at the request of a responsible Transmission Owner and/or Operator.
Group
Arizona Public Service Company
Janet Smith
Yes

See related comments under Requirement 2 below.
Yes
AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications for Requirements 1-3. AZPS suggests that the drafting team modify the term “risk assessment” to “BES impact assessment” in Requirements 1-3. The term risk assessment is not a defined term in the NERC Glossary of Terms. It is used in other CIP standards (CIP-002, and CIP-004) each with a different context. Changing the term to “BES impact assessment” ensures that the risks will be categorized and evaluated correctly. Requirement 2.1 directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. However, none of these NERC functional entity designations appear in the applicability section of the standard. Thus it is assumed that the entities listed above are not obligated to conduct the assessment once selected but rather the assessment is conducted by mutual agreement. AZPS suggests that the drafting team provide clarifying language in the requirement to indicate that the assessment is conducted by mutual agreement between the Transmission Owner and the third-party assessor. AZPS is concerned that the term “primary control center” will be confused with the NERC Glossary Term “Control Center.” The definition of Control Center is partially defined as “monitor and control the BES…”. The rationale for Requirement 1 introduces the term “operationally control” in its definition of primary control center which is further defined to mean “causing direct physical action”. The concept of monitoring is explicitly excluded from this definition. To avoid confusion, AZPS suggests that the drafting team define the term primary control center or adopt a new term that clearly differentiates itself from the common term “control center”.
Yes
AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications or clarifications for Requirements 4-6. AZPS is concerned that Requirement 4.3, which requires the Transmission Owner to evaluate threat warnings from a myriad of sources, will result in inconsistent application by entities. The threat sources need to be consistent, and the threats evaluated must be relevant. AZPS suggests that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions. This would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. Requirement 6 requires Transmission Owners to secure a third-party review of the security plan developed under Requirements 4 and 5. AZPS strongly supports the development of security measures to protect critical substations. However, AZPS believes that requirements 6.1.1 through 6.1.4 add a level of specificity that does not provide an improved reliability benefit and has the potential to create a bottleneck that would make compliance within the short 90-day timeframe very difficult. AZPS contends that the most important quality of the third party reviewer is electric industry physical security expertise. Further, AZPS does not believe that the CPP or PSP certifications provide additional value from a realiability standpoint since neither certification has a sector specific focus. For these reasons AZPS would suggest that 6.1 be simplified to read: “Each

Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise.”
No
Individual
David Jendras
Ameren
Yes
No
(1) Regarding R3 and R3.1, we believe that the 7 day requirement is too short and 30 days would be more appropriate to notify other utilities. (2) R4 should have wording added to the requirement that the R4 evaluation is to be completed 120 days after the completion of R2. Then, the R5 wording should be changed so that the R5 physical security plans should be completed 120 days after the R4 evaluation is completed.
Yes
No
We recommend adding language in the implementation guidance around the application of the terms ‘control center’, ‘primary control center’, and ‘transmission station’ in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies’ ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms. Also, we recommend that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify several questions on the timing of the various implementation stages of the standard, including particularly that security plans are subject to change over time for a broad range of reasons. In addition, we ask the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes

R1 - It appears the intent of R1 is for a TO (which meets the applicability section 4.1.1) to perform a risk assessment (as defined in the standard) on only those substations that meet the applicability section 4.1.1, not all substations owned by a TO which meets the applicability section 4.1.1 description; however this is not 100% clear. The verbiage of the second sentence in R1 states “The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.” The use of the word “any” in this sentence has led some to believe that a TO (which meets the applicability section 4.1.1 description) will have to assess all of their substations, even those that do not meet the section 4.1.1 description. To address this possible issue, LES recommends replacing the word “any” in R1 with “applicable”. R2 - Smaller TOs may not have the in-house resources to perform the risks assessments required in R1, and may need to contract with a third party to perform these assessments. If the performing third party is not affiliated with the TO, is a second unaffiliated third party verification required as stated in R2? Please revise the requirement to address this situation.
Individual
Gary Kruempel
MidAmerican Energy Holding Company
Yes
MidAmerican Energy Holdings Company (MEHC) agrees with the applicability section.
Yes
MEHC agrees with the R1 through R3 approach. However, MEHC suggests the following changes to improve the standards as written: The term “unafilliated third party” is used in R2 and in R6, but in parts 2.1, 2.3 and 2.3. “unaffiliated verifying entity” and in part 6.3 “unaffiliated reviewing entity” is used. Unless the intent was that the terms have different meanins, it is suggested that “unafilliated third party” be used throughout the standard.
Yes
MEHC agrees with the R4 through R6 approach. However, MEHC suggests the following changes to improve the standards as written: The following rewording of R5 is recommended to clarify that the “build out” of security enhancement schedule. R5 Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator’s primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The plan shall be completed within 120 calendar days following the completion of Requirement R2. Implementation of the plan shall be as documented in the plan.
Yes

1. The standard anticipates the potential for joint responsibility in involving transmission operator control centers for substations identified by transmission owners. It is suggested that additional guidance be provided regarding joint ownership of substations The following addition to the first paragraph under the Requirement R1 heading which is similar to an aswer to this questions in the webinars is suggested: For substations that are jointly owned the owners may jointly designate one of the joint owners to perform the risk assessment for that substation. 2. It is suggested that a clarification be made to the RSAW with regard to the following question: " As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" By referring to risk assessment this seems to imply the stations/substations identified after the completion of the requirement R1 risk assessment rather than just the applicability requirements. It is suggested that the words "as a result of your risk assessment" be deleted from this question. 3. Item 3. in the guidance for Requirement R2 seems to actually be guidance for Requirement R1. However, it does not provide useful guidance for Requirement R1; therefore, it should be removed. The guidance for Requirement R1 that gives the TO discretion to choose its own methods and criteria is preferred. 4. The following modification to one of the sentences in the "Performing Risk Assessment" section of the guidance document is suggested: "Using engineering judgment, the Transmission Owner should develop criteria (e.g. imposing a fault near the removed substation) to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection."
Individual
John Canavan
NorthWestern Energy
Agree
Arizona Public Service, Bureau of Reclamation, Portland General Electric, WECC
Group
Western Electricity Coordinating Council
Steve Rueckert
No
WECC questions why generation assets are exempt from analysis and verification required by Requirements R1 and R2. It is possible that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading. WECC recommends removing the 500 kV line in the Weighted Value table. All 500 kV facilities are to be assessed per Applicability Section 4.1.1.1 and including 500 kV lines in the table in applicability section 4.1.1.2 with a zero value seems more likely to add confusion than to provide clarifying information. Applicability section 4.1.2 makes it look like the standard is applicable to all Transmission Operators. WECC suggests adding some clarifying language to indicate that the standard is only applicable to Transmission Operators notified per Requirement R3. This may serve to make the standard more acceptable to Transmission Operators in general.

No
The periodicity for risk assessments and the forward looking time frame for including planned substations do not match. Entities are only required to consider stations planned in the next 24 months, while the risk assessment is applied on a 30 month cycle, or a 60 month cycle if the entity previously identified a null list of applicable stations. This potentially leaves a 6 to 36 month gap. We would encourage the SDT to match the periodicity of the application to the planned implementation window or include language requiring any new asset be evaluated under R1. WECC notes that the time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. WECC suggests that at a minimum NERC and the Regions engage in extensive outreach to ensure that the Transmission Owners are aware of this and that if possible the drafting team revise the language of Requirement R1 to make this clear. Requirement R2, part 2.2 appears to be assigning responsibilities to the unaffiliated verifying entity (registered Planning Coordinator, Transmission Planner, or Reliability Coordinator) yet these entities are not included in the applicability section. If these entities are to be held accountable in the standard for actions, why are they not included in the applicability section?
No
From a compliance perspective, WECC notes that the criterion identified in R4 is too vague to enable a consistent approach across regions or even entities. Identifying a basic set of attack vectors that must be considered (ie: direct fire ballistic attack, indirect fire attack, explosive device attack, vehicle-borne attack, arson/incendiary attack) fosters a far more consistent approach while allowing the entity the flexibility to tailor their assessment and security plan to the unique characteristics and threat landscape of their asset(s). WECC is concerned that the language of Requirement R5 is confusing or contratictory. Requirement R5 requires the applicable entity to “develop and implement” a documented physical security plan…within 120 calendar days following the completion of Requirement R2. However, part 5.3 requires a timeline for “implementing” the physical security enhancements and modifications specified in the physical security plan. WECC questions whether Requirement R5 requires the physical security plan to be “developed” or “developed and implemented” within 120 calendar days following the completion of Requirement R2. If Requirement R5 requires “development and implementation” within 120 calendar days following the completion of Requirement R2, what is the purpose of the timeline for implementing the physical security enhancements and modifications specified in the physical security plan required by part 5.3?
Yes
WECC believes that the proposed standard addresses the FERC Order and has voted affirmative to approve CIP-014-1. However, as noted in our comments above we believe there is opportunity for enhancements and clarification that if implemented would improve the standard and still meet the FERC Order. WECC encourages the drafting team to consider implementation of these suggestions prior to the final ballot or NERC to submit a SAR for consideration of these suggestions immediately after approval of the standard.
Group

NCPA Compliance Management Operating Committee
Steve Hill
No
The Standard Drafting Team (SDT) estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability or uncontrolled separation. The Applicability section creates a lot of work for many TOs an TOPS to identity those 30 or less transmission stations out of the 55,000 substations. The SDT might consider a higher level of applicability as was done for EOP-010-1, Geomagnetic Disturbance Operations i.e. apply the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.This would be a more efficeint filtering process. Benefits of such an approach would be (1)Simplification and tighter security of critical information and informaton sharing (2) streamling and simplicaton of requirements for unaffiliated third party review, for example one reviewer could handle the risk assessment, vulnerability and threat assessment and review of security plans (combines requirements R2 & R6 together) (3)Time and resources of the entity could be more efficiently and economically managed as all reviews could be handled by a single Reviewer in a continuous manner rather than starting a stopping for different phases. (4) Saves many entities who would fall out of the process after going through the first three requirements. I expect RCs, ISOs and Regional Entities already know this
No
Applicability is a key issue here. Comments to question 1 apply here as well. Why subject all Transmission Owners who may meet the "medium impact under CIP-002-5.1 to a third pary review for all medium impact stations and substations when only 30 stations will be affected (please define the difference between a Transmission station and Transmission substation. A third party review is appropriate for the 30 or so stations involved, but seems excessive for all owners to obtain third party review when the expectation is that 30 out of 55,000 are te ones of real concern. NCPA elected to have an independent third party risk asssessment and vulnerability assessment performed at its 5 generation facilities and control center. The assessment cost is approximately $150K and takes about 9 months to complete. NCPA'a assets are also low impact. The risk assessment, vulnerability and threat assessments and development of the security plans are able to performed by the same third party reviewer that flows together without interruption. The way in which the requirements are structured creates alot of consultants or third party reviewers running around, with 99% of them stopping work after R3. How much money will be spend for that and for what purpose? There has to be a better way segregate the 99% from the 1% where the real concern is.
No
Same line of reasoning as given in the response to the question 2. If the Applicability Section were changed R1, R3, R4,and R5 could be combined together and R2 and R6 could be combined together. This simplifies the standard and gets to the heart of the Reliability

Concern without creating a Consulting industry to perform third party reviews. (If you don't like the suggestion, maybe I found a new business opportunity)
Yes
The Implementation Plan is too agressive. I cite NCPA experience as described in our response to question 2. I find it interesting the the CIP-version 5 standards have essentially a two year implementation plan for medium and high assets and yet this proposed standard has a 6 month implementation plan.
Individual
Joe O'Brien
NIPSCO
In R2 we are not sure who would do the verification. On one of the webinars a member of PJM suggested that another PJM member could be a candidate. However it is likely that a PJM member is not a PC, TP or RC as prescribed in the requirement; that role is performed by PJM itself. Any further guidance would be welcome; we do not consider this a "show stopper". The hard work that went into putting this project together in such a short time frame is appreciated, thanks.
Individual
Wayne Sipperly
New York Power Authority
Agree
APPA
Individual
Megan Wagner
Westar Energy
Yes
No
The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time.” While not specifically

referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments.
Yes
Yes
Effective Date: The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs: Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2. Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5. Delete 'and modify or' in the last High VSL for R6. Guidelines and Technical Basis: Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6. Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary. Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29. Make 'outage' plural in Bullet c. at the top of Page 30. Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30. Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3. Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6. Spell out TO and TOP throughout the document. RSAW: The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '…any risk assessments conducted prior to the effective date of this standard are not relevant…' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective. Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2. Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4. The phrase 'and compensating mitigating measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Individual

Amy Casuscelli
Xcel Energy
Yes
Yes
Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team. R1 requires an assessment of facilities, including those to be in service within the next 24 months, followed by an additional review every 30 or 60 months. If a facility is brought into service, it is unclear when the review should be performed due to the 6 month gap between the in service date and the review. R2 requires a Transmission Owner to have an unaffiliated third party "verify" the risk assessment performed under R1. By contrast, R6 requires each Transmission Owner to have an unaffiliated entity "review" the evaluation performed under R4 and the security plan under R5. Xcel Energy recognizes that use of "verify" and "review" reflects the Commission's wording, but it would be helpful if the standard explained the difference between the two terms, if there is a difference. The 90 days prescribed by R2 to obtain third party verification may be too restrictive due to the availability and/or capacity of applicable resources. The standard requirement which imposes the action/deliverable by a third party, but the accountability to the TO/TOP, is also a cause for concern. It might be better to have the timing of R1 and R2 combined as this would enable flexibility of performing the assessment and completing the third party verification within the overall timeframe desired. We also suggest the Regional Entities or NERC be considered as parties that can provide third party verification and contract out if desired. It would also be helpful to expressly clarify in R2.1 that an "entity with transmission planning or analysis experience" could include a peer TO/TOP or a panel of employees from peer TO/TOPs, for example from the North American Transmission Forum. Allowing peer review would assist in identification and dissemination of best practices, we believe. R2.3 requires documentation of any recommendation to add or remove facilities as recommended by the verifying entity, but does not specify if any actions are required if no recommendations are made. Since the VRFs reference various levels of severity based upon documentation of recommendations, it would seem beneficial to allow a "no recommendations" option. Also, it is unclear if there are specific criteria the third party reviewer should utilize to review/verify and make recommendations if facilities are to be added or removed. While an entity could indicate why recommendations were or were not adopted, it would be useful to have verification criteria defined more clearly. R3 seems to be unclear in whether TOs or TOPs have operational control over facilities. In order to more clearly identify that TOPs have operational control, R3 should indicate that the TO shall notify the TOP of the identified facility.
Yes
Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team. The rational for R4 and R5.1 indicate that there is no required timeframe to complete the evaluation of the potential threats and

vulnerabilities to identified facilities, but it does indicate the linkage of completing this when the physical security plan developed as part of R5 and within 120 days of completion of R2. We suggest that it might be more efficient to combine R4 and R5 or clearly show the linkage to reduce confusion about the timing of these two activities. Maybe the standard should require entities to develop a physical security plan after the risk assessment is completed, not after a verification of facilities as specified in R2. If R2 returns a null set, this seems ambiguous as we may still be required to have a physical security plan, even if blank. Since R4 would only be considered applicable if the R2 risk assessment process identifies facilities, referencing R4 in R5 would seem more intuitive. R5.2 states that the physical security plan must include law enforcement's contact and coordination information. However, guidance on law enforcement and coordination has already been established with the adoption of EOP-004-2. It is also unclear by what is meant by "coordination". Since reporting a physical threat to a Facility is a requirement of EOP-004-2 and in order to remove ambiguity around the word coordination, we propose changing R5.2 to read "notification of law enforcement consistent with EOP-004-2". This would avoid potential confusion whether the R5.2 requirement is different than the EOP-004-2 requirement. R6.1, While there will be some regional variances, if an entity spans multiple regions or even some governmental agency jurisdictions, what protection does an entity have against reviewer discrepancies or differences? For example, the Xcel Energy registered entities anticipate using a common risk assessment methodology, and similar security plans. It would be efficient to have a single evaluator provide the review for all three Xcel Energy registered entities. It would also be important for Regional Entities to apply consistent criteria when auditing the risk assessments and security plans. R6.1.2, if the ERO does not meet any or some parts of the criteria established in R6.1, it is uncertain how the ERO will be able to determine and approve an organization that does. Our security department, like the departments at other utilities of similar size, consists of a mix of multiple CPP and/or PSP holders, prior law enforcement professionals and several career military experts, including nuclear military asset security. It would seem that resources within the industry are the most knowledgeable resources available to evaluate physical security plans, given the criteria, and would have more utility specific knowledge than outside entities. Similar to our comments regarding R2.1, since the industry has the most knowledge on threats and vulnerabilities, and means to prevent them, we again propose adding an option to allow for industry (but non-affiliated) peer review of the physical security evaluation, either directly or through a group organization such as the North American Transmission Forum. Allowing peer review is likely to assist in identifying and disseminating best practices, thereby improving security. R6.3. Similar to our comments regarding R2.3, if no recommendations are made for changes to the evaluation by the unaffiliated reviewing entity, does this conclusion need be documented? Since some of VRFs are built off this requirement, it would seem to follow that all aspects be included to ensure certainty for the industry.

Yes

Since existing criteria from CIP-002-5.1 is used to identify facilities in scope, Xcel Energy suggests the addition of the proposed requirements be incorporated to CIP-006-5 (rather than in an entirely new standard) to more closely align and standardize the oversight of R3 and R6. In addition, this would centralize all physical security requirements within a single

Standard. Additionally, there is a significant amount of language in the requirements to specify the affected parties. We suggest the Standard Drafting Team seek opportunities to more concisely outline the applicability and the subsequent obligations in the requirements, to improve ease of understanding. We see an opportunity for the audit or risk functions of the Regional Entities to align with the third party review criteria established in the proposed standard. Although the expertise to perform this function may not currently be in place, the Regional Entities could easily develop the knowledge and expertise, and the reviews could naturally integrate within their other review and assessment activities. Overall, the standard is very comprehensive as drafted and it is balanced in a manner that allows for maximum flexibility. Consistent with NERC's evolution to results-based standards, it is appropriate for the standard to focus on the desired results of increased security of critical facilities, rather than mandating rigid actions that may or may not be suitable for individual facilities and entities. Allowing industry the latitude to design its own mitigating measures ensures those measures will be the most practical and cost effective as appropriate for the particular nature of each facility. The flexibility of this proposed standard is the best opportunity for the industry to execute a comprehensive solution based on assessments and security that relies on the unique design and characteristics of the operating systems of each utility.
Individual
Mahmood Safi
Omaha Public Power District
No
The Omaha Public Power District (OPPD), suggests replacing the term "primary control center", using the NERC defined term "Control Center", with "primary Control Center".
No
OPPD, in general, is in agreement with the approach taken in CIP-014-1 for identifying critical Transmssion stations and substations. We agree that risk assessment be conducted using transmission planning analysis, however, we suggest that this standard identifies what applicable planning analysis is used. We think the TPL standards provide the ability for the Transmission Owners to determine the worst case extreme event for identifying critical transmission stations and substations. OPPD believes that leaving R1 open and vague would encourage various interpretations of the term 'transmission planning analysis' as it applies to a 'risk assessment'. This may place the industry and the ERO in the same position as they were with the ealier versions of CIP-002 and the associated RBAM. Referencing the applicable TPL standards attemptes to remove some of this ambiguity by providing a more concise framework to evaluate those worst case extreme events. Furthermore, since TPL standards associated transmission planning analyses are performed in coordination with the PCs, risk assessment verification by PCs/RCs will not require a re-assessment of a study that has already been performed. We suggest that the SDT consider specifically defining 'transmission planning analysis' to avoid repeat of the uncertainty and vagueness associated with the CIP-002 RBAM. OPPD asks the SDT to consider revising requirement R1 as following: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments

of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The transmission planning analysis shall be based on the applicable portion(s) of the TPL standards and specifically referenced. [VRF: High; Time-Horizon: Long-term Planning] 1.1. Subsequent risk assessments shall be performed: • At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or • At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. 1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.
Yes
Yes
OPPD believes that the third-party verifications in requirements R2 and R6, to be performed once every 60 calendar months, not each time when a risk assessment analysis or security plan is changed that does not significantly change the facilities identified or the associated security plan. The transmission entity can still perform analysis and update security plan accordingly as required by this standard, however, the third-party verification should be reserved for major changes to the assessment or the plan or otherwise be done every 60 calender months.
Individual
Bruce Metruck
New York Power Authority
Agree
APPA
Individual
Russell Noble
Public Utitliy District No. 1 of Cowlitz County, WA
American Public Power Association
No

We strongly disagree with applicability statements being outlined in the requirement. We support APPA's recommendation to further define TOP applicability in section 4.1.2 to avoid nuisance compliance certifications.
Yes
However, the TOP does not receive any relief from R1-R2 null set(s) and will be required to provide attestations to auditors and yearly certification of the absence of any notice from Transmission Owners.
No
We are very concerned with the preferential endorsement this Standard affords to ASIS International. We know of at least one other security organization that offers a security certification: the Certified Homeland Protection Professional (CHPP) designation form the National Sheriffs' Association Institute for Homeland Security. If this requirement is left unchanged, FERC's statutory obligation in determining a proposed reliability standard is "not unduly discriminatory or preferential" may trigger the standard to be remanded back to NERC. It is for this concern, and only this concern Cowlitz votes negative. However, Cowlitz plans to vote affirmative in the final Ballot, regardless of any concerns to allow NERC to meet FERC requirements.
Yes
Cowlitz commends the SDT's effort in a very difficult situation.
Individual
Dennis Minton
Florida Keys Electric Cooperative
No
• Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is FKEC’s understanding that a “station” equates to a switchyard that does not include transformers; and a “substation” is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. • Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
No
• Comments: R1.1 – FKEC recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straight forward than a 2.5 year focus and it’s easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. • R2 – The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word “should,” not “shall” or “require.” The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what “verify” means in the standard.

Guidance and rationale is helpful, but does not carry to legal weight of the standard language. • R2.1 – This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. o Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in theNERC facility ratings alert responses. o How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. o If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired – this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. • R2.2 – This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. • R2.4 – The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity • R3.1 – The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. FKEC believes 30 days is more appropriate timeframe for this requirement.

No

• It's unclear how an auditor will judge compliance with R4 and its subrequirementsas it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. • R5.1 – FKEC strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement and resiliency will be next to impossible to audit. • 5.3 – After the word "modifications " add ",if any," as this is a possibile outcome. • R6 – Same as comments on R2 in Question 2 above. and R2.1. • R6.1.1 – NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides

for the necessary skills under this standard. • R6.1.2 – It is highly unlikely that the ERO is not going to approve consultants for industry use. This should be removed. • R6.1.3 – All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. • R6.1.4 – It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Yes
Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
Individual
Bill fowler
City of Tallahassee
Agree
APPA
Individual
Chris Scanlon
Exelon
Yes
Yes
R2.1 Drafting Team could consider adding a note to R2 Guidance section similar to that which is included in the recently approved MOD-032 standard. "Planning Authority and Planning Coordinator" (hereafter collectively referred to as "Planning Coordinator")combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria lists "Planning Authority" and they are not yet synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator."
Yes
No
Individual
Linda Jacobson-Quinn
FEUS
Agree
APPA WECC

Individual
Dean Ahlsten
Eugene Water & Electric Board
Agree
American Public Power Association (APPA)
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Yes
No
Do not support the third party requirements, seems like a full employment effort by security consultants and others. Administratively burdensome and time-consuming at the expense of actual security improvements.
No
Again, do not support the third party review requirements. Already an auditable standard approach.
No
Individual
Steven Wickel
Public Utility District No. 1 of Chelan County
Agree
LPPC and APPA
Individual
John Yale
Public Utility District No. 1 of Chelan County
Agree
LPPC and APPA
Individual
Hugh Owen
Public Utility District No. 1 of Chelan County
Agree
APPA and LPPC comments
Group
Con Edison and Orange & Rockland
Peter Yost

No
Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section. That will obligate these entities to meet the 90 day review period stipulated in R2.2, if they are identified as a verifying entity by the Transmission Owner.
Yes
Yes
Yes
Section: Purpose Comment: Use of term “primary control center” should be clarified. If an entity has a primary control center and a redundant back up control center, is the back up control center also in scope for CIP-014? Requirement 1: is the intent of the Standard that the R1 risk assessment be applied to transmission stations or substations identified under Applicability 4.1.1.4, as meeting NPIRs? Requirement 4: If under Requirement R4 a Transmission Owner owns or operates a single substation that employs multiple voltage levels, then which portions of that substation would be covered by CIP-014-1 and the Entity’s physical security plan, and which would not be covered? Requirement 5: Consideration of transmission system “resiliency” is more appropriate to be applied during the R1 risk assessment, as opposed to the R5 physical security plan. Recommend moving references to resiliency to R1.
Individual
Mike Marshall
Idaho Power Co.
Yes
4.1.2. Seems vague in its description lending the reader to believe that TOPs are in scope at all times which is inconsistent with guidance later in the standard which states they are only required to perform actions when informed they are in scope by a TO. Further Clarification is needed in this section.
Yes
Further clarification is needed on several points. There is no specificity to provide consistency with how the "risk assessment" should be performed or what methodology or components to the methodology should be used. Additionally, there is no defined meaning of "widespread instability, uncontrolled separation, or Cascading within an Interconnection." Does this refer to regionally identified IROLs or some other objective criteria or only based on the analysis performed? Additionally, there is no mechanism built into R3 to allow for a dispute between a TO and a TOP if they disagree on a particular station or substation as there is in the third party reviews under R2 and R6 where there is a mechanism to disagree with the reviewer.
Yes

Further clarification is needed on several points. 4.2 & 4.3 leave open much room for interpretation under audit to say you did or didn't consider a particular source or threat. There is also some consternation over the use of "potential threat" in this requirement. There are a great many potential threats many that are so remote and nearly impossible to protect against that the risk does not outweigh the cost. It seems like these sub-requirements are a potential audit findings trap by the way they are worded. There are also no criteria specified for what the unaffiliated third party will be looking for in their review of the entity's evaluation. There is a great deal of concern for how these third parties will be able to handle or be willing to handle the influx of these reviews especially considering the short 90 day timeframe listed in 6.2.
Yes
There is great concern related to information protection related to turning over information concerning vulnerabilities of the grid and related facilities to outside parties. Even with the use of NDAs, these third parties are not subject to the same NERC reliability standards (i.e. CIP standards, information protection, etc) as the entities, will not be audited on their information protection practices, and may have no accountability to the regulators in the event of a disclosure of sensitive information, inadvertent or otherwise. It is a concern that the TO is responsible for 3rd party verification to be completed within a tight 90 day window, especially considering the critical infrastructure information being exchanged. Contractual exchanges and negotiations could impede upon the 90 day window. Also, TO's may need time to review the R2 study results and possibly mitigate study discrepancies. The date R1 needs to be performed is unclear. Does it need to be performed within a certain amount of time after the effective date? The implementation plan states that the initial risk assessment must be performed on or before the effective date of the standard. However, the RSAW for R1 states that "any risk assessments conducted prior to the effective date of this standard are not relevant." Does this mean the initial risk assessment must be performed “on” the actual effective date of the standard? Is there a basis for the short notification window in R3? The seven calendar days window for the TO to notify the TOP seems quite short. Additionally, there is a discrepancy in the review timeframes in R1 in which a look ahead of 24 months is required for stations and substations that are in the planning process but the risk assessments are performed every 30 months leaving a 6 month gap in the analysis. It would also seem more intuitive and consistent with other CIP standards to have the risk assessment requirement performed on an even year rather than a 30 month basis (i.e. 36 months.)
Individual
Chad Bowman
CHPD
Agree
CHPD is supportive of the comments submitted by APPA
Group
ACES Standards Collaborators
Ben Engelby

Yes
We support a clear and defined “bright line” criteria that has been industry vetted and FERC approved as the starting point for the risk assessment in R1.
No
(1) Conceptually, we agree with this approach but have identified the following issues and concerns. (2) R1 requires additional clarification. The Guidelines and Technical Basis section states that the “bright line” criteria in applicability section is used to identify an initial set of stations and substations that must be further evaluated in R1. It is our understanding that if a TO owns one 500 kV transmission station and no other transmission facilities, then that 500 kV station would meet the applicability section 4.1.1.1 criteria. The TO would be required to perform a risk assessment to identify if that facility was rendered inoperable, it could result in widespread instability, uncontrolled separation, or Cascading in an Interconnection. In other words, if the applicability section is met, the TO must perform a risk assessment, but the remainder of the standard (R4-R6) would not apply unless loss of the Facility would result in widespread instability, uncontrolled separation or Cascading. Please confirm if our understanding of applying the requirements is the correct approach. (3) We see a significant compliance risk created by Requirement R2 and question why the unafilliated third party verification cannot be integrated into the Regional Entity compliance monitoring and enforcement processes to minimize costs and limit access to highly sensitive information. The third party verification creates a compliance problem outside of the TO’s control because the TO is dependent on a third-party for regulatory compliance and there is no obligation on any of the third parties (i.e. RC, PC) identified in the standard to verify the risk assessment. Thus, the TO will have to rely on consultants to perform the verification. Since all TOs will be working towards the same efffective date, there will be a backlog and the reviews may not be completed by the timelines established in the standard. Review by consultants also will increase the number of people with access to highly sensitive information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. All of these issues could be resolved if NERC and Regional Entities conducted the review. The review could be performed as part of a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolved the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. As an alternative, we suggest that a companion requirement that compels either the RC or PC to perform the verification. This would also reduce the costs impacts and distribution of sensitive information since these entities will already be familiar with the TOs they are verifying and will already have access to highly sensitive information. (4) Regarding R3, this requirement does not warrant a 7-day timeline. This is not a near real-time issue. We suggest 30 days as a reasonable notification period.
No

(1) We see a significant risk of the compromise of highly sensitive information created by Requirement R6 and question why the unaffiliated third party review cannot be integrated into the ERO compliance monitoring and enforcement processes. There is no compliance obligation on these third parties to complete the review within the required timelines, which could subject the TO to potential compliance violations. Furthermore, there is a limited set of companies with qualified personnel capable of performing this review. Given that all of the Transmission Owners will be working toward the same effective date of the standard, it is highly likely that a backlog of work would occur. Furthermore, review of the evaluations by consultants will increase the the number of people with access to higly senstivie information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. To resolve this inssue, NERC and Regional Entities could hire qualified personnel to perform these reviews. NERC and Regional Entities could perform a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolve the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. (2) How can the 'cost to benefit to risk to the BES' be measured consistently across each facility, region and risk? Does a Registered Entity have to authority to not implement a 'recommendation' from a third party based upon a cost to benefit to risk analysis? (3) Given that third parties are required to evaluate critical facility information, further guidance is needed for the required controls to prevent unintended release of highly sensitive and confidential information. What is the risk to the Registered Entity if the information does get leaked? Is this a violation to the Registered Entity, even if the leaked information was not caused by the Registered Entity? We are concerned that if this information were to be leaked, the Registered Entity could be liable for increased risk of attack, additional time and costs to address the leak and could impact the BES due to changes in operations from shutting down those facilities. (4) Part 4.2 has a potential "prove the negative" issue. How do you prove that you considered similar facilities particularly when similar facilities could includes other company's facilities. To resolve this issue we suggest replacing "similar" with "nearby facilities" or "asset owner's other facilities in the area". (5) Part 4.3 could be interpreted as requiring consideration of all threat and intelligence information including information that is not relevant to a given area. To remedy this issue, we recommend using the term "current and local" to describe the types of intelligence and threats that must be considered. (6) We believe that Part 5.2 is redundant to the EOP-004-2 – Event Reporting, especially Attachment 2 Event Reporting Form line 4. Please consider removing and comparing the standard in its entirety to EOP-004-2 to avoid unnecessary duplication. (7) For Part 5.4, please modify the language to clarify that it only applies to facilities identified as a result of application of Requirements R1 and R2. (8) For Part 6.1 please modify "… from the following" to "… from one of the following". This will make it perfectly clear that only one entity must be selected.
No

Thank you for your time and consideration.
Individual
David Thorne
Pepco Holdings Inc.
Yes
Yes
Yes
Yes
There seems to be a conflict between the RSAW, Consideration of Issues or Directives and the Timeline included in the FAQ. To meet the overall timeline for the entire standard, the risk assessment must be started prior to the Effective date of the standard. There should be no prohibition for completion of the Risk Assessment prior to the Effective date of the standard. The FAQ Timeline states: “Initial performance of R1 must be complete on or before the effective date of the standard…” The Consideration of Issues or Directives #12: “…This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard…” The RSAW under R1 Evidence Requested states: “Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).”
Group
American Public Power Association (APPA)
Allen Mosher
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. CONTROL CENTER - Use the defined term “Control Center” by capitalizing as “primary Control Center” or explain why lower case “primary control center” is different and needs to be used in the standard. Consider inserting “with operational control” after primary Control Center, to express the intent of the text box Rationale for Requirement R1 that the control center must be capable of taking electronic actions that can cause direct physical actions at the identified station or substation. Please also clarify whether the periodic use of a

backup control center as the entity's primary control center would make R4 and R5 applicable to both the primary and backup control centers. UNAFFILIATED - needs to be either defined or a footnote needs to be added to the standard to explain that "unaffiliated means that the selected verifying or reviewing entity cannot be a corporate affiliate," as stated in the guidance section. CONFIDENTIALITY Publicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS: R1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3.2 The Transmission Owner will keep confidential all records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard. R4.4 The Transmission Owner and each applicable Transmission Operator will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1. APPA suggests technical edits to Requirements R2.4 and R6.4 to insert "or made available to" after "exchanged with." This change would clarify that sensitive or confidential information does not have to be actively "exchanged" between entities to be subject to the protections directed under Requirements R2.4 and R6.4. APPLICABILITY 4.1.2 - The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would

be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective: 4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3. Please also confirm that the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. TIMELINES to complete third party verification under R2 and third part review under R6 are both too short. Increase 90 days to 120 days or 180 days. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A short 90-day time limit may not be sufficient time to conduct and verify a revised or supplemental BES assessment. For security reviews, conducting a meaningful review with sound recommendations applicable to a specific TO's or TOP's facts and circumstances may also take time along with necessary discussions with the TO. A short review window is more likely to lead to disagreements with the TO which in turn would lead to discrepancies that would need to be justified – which in turn might cause the reviewer to avoid making proposals that should be considered by the TO or pressure on the TO to accept recommendations that could be improved upon. R1 GUIDANCE - TRANSMISSION PLANNING BASE CASES: Please revise the Guidance for R1 to clarify that TOs should start their initial and subsequent risk assessments with a common regional or area transmission planning base case used for transmission planning purposes. The base case should include existing BES stations and substations and those planned to be in service within 24 months within the region or area, to ensure forward-looking risk assessments and security planning. R2 VERIFICATION - Third party verification of third party risk assessments conducted under R1: some medium sized TOs with applicable transmission stations and substations may contract with a third party consultant to conduct necessary BES risk assessments, to ensure accurate and comprehensive consideration of the risk of widespread cascading, instability and uncontrolled separation. Such entities seek clarification that a single expert risk assessment study, in conjunction with a verification by an unaffiliated PC, TP or RC would suffice.
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. R4 CLARITY - Under R4, combining the applicability of this requirement to both TOs and TOPs with applicable control centers within a single sentence is confusing and could be read to imply that a TOP that is affiliated with a TO must arrange for a separate third party review. We recommend revising R4 to read as follows: R4 Each Transmission Owner that

owns a Transmission station or Transmission substation identified in Requirement R1 and verified according to Requirement R2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s) and Transmission substation(s), identified in Requirement R1 and verified according to Requirement R2. Each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to their primary control center identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning] R4.2 TYPO – Please change: "Prior history or attack..." to "Prior history OF attack..." Make conforming edits to the RSAW. 30-MONTH CYCLE - Identification of new threats and vulnerabilities in R5.4 does not change the 30-month cycle for conducting reliability studies and security evaluations: The standard needs to make clear that the security plan needs to take into account threats and vulnerabilities that are known at the time the plan is developed and the approved plan is capable of addressing new threats and vulnerabilities as they emerge, but that there is no NERC requirement to revise the plan between 30 month cycles and for the NERC CEA to audit such revisions. The TO should apply its existing security plans and procedures to evaluate and mitigate evolving security threats. The TO may also revise the security plan in mid-cycle if it so chooses without arranging for a third party review, but that action does not obviate its obligation to conduct the "subsequent" risk assessment and threat evaluation and security plan on the 30 month cycle. The CEA will audit the processes the TO uses to develop its plans, rather than the content of the plans. REQUIREMENT R5 CLARITY – R5 states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." Please change "implement" to "complete." The use of implement can easily be read to require the actual implementation of physical security measures within 120 days, rather than the completion of the security plan, starting the 90 day clock for unaffiliated third party review under R6. In contrast, R6 states that: "The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5."

Yes

APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. See comments on definitions under Question 1. RSAW for R1 poses the following question: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" This question combines a multi-step process into a single question that cannot be answered as yes or no by many TOs. Please break the RSAW for R1

into three discrete questions: 1…Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1? 2…Have you conducted a risk assessment of each applicable station or substation identified under Applicability section 4.1.1.? 3…Did the risk assessment identify one or more Transmission station(s) and/or Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? RSAW R1 evidence request text from near the top of page 6: (R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant). The draft Implementation Plan states that the risk assessment required by R1 "must be completed on or before the effective date of the standard," yet the RSAW language provided above seems to exclude such an assessment. RSAW R1 "Note to Auditor" on page 7: “Review entity’s answer to the above Question and if the auditor can verify the answer is ‘no,’ Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary.” The text appears to reference the following question from page 6: “As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?” This question is poorly worded, because TOs not meeting the applicability requirements of 4.1.1 are effectively exempt from this standard and do not need to perform a risk assessment. RSAW R3 "Question" on page 11: Please reword to add the following all caps text: “Are THERE any primary control centers identified in Requirement R1, Part 1.2 THAT ARE not under operational control of your NERC registration? RSAW R4 "Compliance Assessment Approach" on page 14: Change “or” to “OF” (R4 Part 4.2) “Prior history OF attack...” See the language used in the Guidelines and Technical Basis on page 31 of the standard. RSAW R5 "Note to Auditor" on page 16 states: “Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence.” The requirements of the standard do not address "probability" or "likelihood" of occurrence, so these factors should not be in scope of the compliance audit. Rather, auditors should address whether the security plan is complete and the TO or TOP addresses the issues raised by the third-party reviewer.
Individual
Melissa Kurtz
US Army Corps of Engineers
Agree
Western Area Power Administration
Individual
Shirley Mayadewi
Manitoba Hydro

Yes
Yes
No
(1) Manitoba Hydro has concerns about the need to have a third party to review or verify risk assessments and physical security plans. It is unclear at this point what measures or counter measures are being alluded to here as far as protecting critical assets such as lines and towers. This may potentially be financially burdensome as well as questionably effective. (2) Also missing in the standard is conflict resolution between a TO and this third party reviewer. Clarification should be provided on who weighs in on this and how NERC audits a system that has been verified by a third party. As currently drafted it appears that the third party reviewer/verifier would have no liability under the standard.
Yes
(1) R6.1 – It is not clear whether only one or all of the qualifications in Section 6.1.1 through 6.1.4 must be met. Accordingly, R6.1 should be rephrased to refer to “one of the following”.
Individual
Debra Warner
self
No
While the reqirement for unafflilated third party verification of the security plan is required by the FERC order, I believe the mandate will lead to future security compromises.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
FirstEnergy supports the proposed requirements R1 through R3.
Yes
FirstEnergy supports the proposed requirements R4 through R6 but offers two comments: 1) In regard to the inclusion of “primary control centers,” we suggest the team add language within the Guidelines and Technical Basis section for requirement R4 and potentially the inclusion of an additional FAQ item to document some of the team’s feedback provided

during the webinar sessions. During the webinar the team provided a good explanation of how CIP-014 is uniquely different than physical protections provided under CIP-006 and that CIP-014 provides perimeter protection of the primary control center location or site and not just the subset of the control center that may house cyber assets protected under CIP-006. 2) Regarding requirement R5, during the industry webinars it became evident that there is some confusion associated with the word “implement” as used in the statement “shall develop and implement a documented security plan(s)” and that some industry stakeholders questioned if implement intended completion of all identified tasks stated within the plan(s). While FirstEnergy understood the requirement as described by the team during the webinars, to alleviate any confusion and better clarify the intended application, FirstEnergy suggests changing “implement” to “initiate” or “issue” so that it reads “shall develop and initiate a documented security plan(s)”. This wording may better align with part 5.3 and the guidance provided in the Guidelines and Technical Basis section that states “Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors.”
No
FirstEnergy supports the proposed standard and appreciates the teams consideration of our comments intended to help clarify a few areas of the standard. FirstEnergy appreciates the team’s efforts in producing a quality standard within an expeditious schedule and believes the team has provided a product that meets the core expectations described by the FERC Order.
Group
Seattle City Light
Paul Haase
Yes
Seattle City Light supports the Question 1 comments of APPA, with one exception in the area of Confidentiality. Seattle's comments about Confidentiality, in place of APPA's comments on this topic, follow. CONFIDENTIALITY The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be

kept confidential by the owner of the records and information, those entities with authorized access to the records and information, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language: R1.3 Records and information related to the risk assessments conducted under this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R3.2 Records and information related to the risk assessments conducted under Requirement R1 of this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R4.4 Records and information related to the evaluation of physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and/or Control Center(s) identified in Requirement R1 conducted under this standard that are designated confidential by the Transmission Owner or Transmission Operator are [intended to be] exempt from public disclosure.

Yes

Seattle City Light supports the Question 2 comments of APPA as well as the additional comments of Salt River Project (SRP) regarding 3rd party verification. Third Party Verifiers (SRP): SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or

fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Yes
Seattle City Light supports the Question 3 comments of APPA.
Yes
Seattle City Light supports the Question 4 comments of APPA.
Group
SPP Standards Review Group
Robert Rhodes
No
We have some concern with the undefined term ‘collector bus facility’. Without a definition for collector bus facility some may consider the entire switchyard at a generating station as a collector bus facility. We do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
No
The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate

confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time.” While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments. We strongly suggest that the SDT expand on this addition to R1 in the guidance document to provide needed clarification to the industry.
Yes
Yes
Effective Date: The use of the term ‘implement’ needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs: Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2. Insert ‘and verified according to Requirement 2’ following the reference to Requirement R1 in all the VSLs for R5. Delete ‘and modify or’ in the last High VSL for R6. Guidelines and Technical Basis: Replace ‘drafting team’ with ‘SDT’ in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6. Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary. Insert ‘Transmission’, capitalize ‘Owner’ and delete ‘or operator’ in the 1st paragraph under Requirement R2 on Page 29. Make ‘outage’ plural in Bullet c. at the top of Page 30. Capitalize ‘Transmission Owner’ in the 4th bullet in the middle of Page 30. Capitalize ‘Owner’ in the 1st line of the paragraph immediately preceeding Requirement R3. Insert ‘Requirement’ in front of R5 in the last line of the paragraph immediately preceeding Requirement R6. Spell out TO and TOP throughout the document. RSAW: The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states ‘…any risk assessments conducted prior to the effective date of this standard are not relevant…’ is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there ‘This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.’ We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective. Replace ‘with’ with ‘within’ in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2. Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4. The phrase ‘and compensating mitigating measures’ in the 4th row

in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Group
Colorado Springs Utilities
Shannon Fair
CSU agrees with APPA comments with exception to the confidentiality section, please see CSU's comments below. CONFIDENTIALITY Publicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS: R1.3 All records and information related to the risk assessments conducted of this standard are exempt from public disclosure. R3.2 All records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard are exempt from public disclosure. R4.4 All records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 of this standard are exempt from public disclosure. Adding confidential in the standard would create undo compliance burden and auditing challenges.

Yes
Yes
Yes
Yes
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is NRECA's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
No
R1.1 – NRECA recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straightforward than a 2.5 year focus and it's easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. R2 – The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word "should," not "shall" or "require." The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what "verify" means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. R2.1 – This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. Are

there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in the NERC facility ratings alert responses. How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired – this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. R2.2 – This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. R2.4 – The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity R3.1 – The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. NRECA believes 30 days is more appropriate timeframe for this requirement.
No
It's unclear how an auditor will judge compliance with R4 and its subrequirements as it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. R5.1 – NRECA strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement, and resiliency will be next to impossible to audit. 5.3 – After the word "modifications " add ",if any," as this is a possibile outcome. R6 – Same as comments on R2 in Question 2 above. and R2.1. R6.1.1 – NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard. R6.1.2 – It is highly unlikely that the ERO is going to approve consultants for industry use. This should be removed. R6.1.3 – All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. R6.1.4 – It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Yes
Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.

Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
Yes
Yes
Yes
ATC supports the draft standard, with the realization that the aggressive time line has raised a broad range of issues or ambiguities resulting from the use of vague language or generic terms. While ATC understands the necessity for this approach, given the compressed timeframe directed by the FERC Order, the project's condensed timeline may not have afforded for the necessary and careful consideration of these terms. Improved guidance around the application of generic terms would increase clarity and help the industry. ATC also supports a follow up effort commensurate with typical standards drafting processes and timeframes to allow for further consideration, improvement, and cleaner language to assure effective implementation of the standard. An example of language like this is in Requirement R1, which includes the vague terminology of "widespread instability, uncontrolled separation, or Cascading." Risk assessment findings can vary significantly depending on the assumptions, criteria, and methodology used for the assessment, and a more thoughtful use of terms could provide for a more uniform risk assessment basis.
Individual
Brian Evans-Mongeon
Utility Services
No
We have seen in the previous versions of the CIP standards that "Risk Assessments" are not performed consistently, and create more problems than they solve, and even violation determinations. The solution in CIP-014 to this inherent problem seems to just add another level of review, but there is no guarantee of consistency within these assessments. Additionally, it seems the drafting team is suggesting a single assessment ("Concurrent with R1 study" specified in R2), this this might eliminate the review stage all together. A clear applicability section with a "brightline" approach would be more appropriate and consistent with the progression of the CIP standards overall. Otherwise, what prevents an auditor from making a determination that the assessment performed was not sufficient or incomplete, even with a 3rd party validation? Entities need a clear definition to avoid the problems of the past. If the drafting team wants to limit the scope of Facilities this could be detailed in the "Exemptions" portion of the "Applicability" section of the standard. 1. The "Exemption"

section needs to be clarified. If this applies to the entire section number it 4.2. If it is only applicable to the last bullet it is under give it the appropriate number (4.1.2.1) Suggested re-write 4. Applicability: 4.1. Functional Entities: 4.1.1 Transmission Owner 4.1.2 Transmission Operator 4.2. Applicable Facilities: The following Facilities, systems, and equipment, owned or operated by each Responsible Entity in 4.1 above are those to which these requirements are applicable. 4.2.1 Transmission Facility operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. 4.2.2 Transmission Facility that operate between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. ADD TABLE HERE 4.2.3 Transmission Facility at a single station or substation location that is identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. 4.2.4 Transmission Facility at a single station or substation whose unplanned unavailability would result in the loss of at least 3000 MW of generation. 4.2.5 Control Center that controls: 4.2.5.1 Transmission Facilities identified by identification under 4.2.1 through 4.2.4; or 4.2.5.2 Two or more Facilities which contain a Cyber System(s) which have been identified as a High or Medium Impact BES Cyber System. 4.2.6 Exemptions: 4.2.6.1 All facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission. 4.2.6.2 Transmission station or substation connected to only one other Transmission station or substation. 4.2.6.3 Transmission station or substation that does not operate above 200kV. 4.2.6.4 control centers not designated as a “primary control center”
No
1. What is a Transmission “station”? What is the definition of station and what is it intended to cover that substation does not. Generally in the NERC glossary “station” is associated with Generation, not Transmission. 2. There is a concern between R1 and R5. a. R1 states that substations planned to be in service within 24 months should be identified, which would presumably be for stations under construction. b. R5 will then require a Physical Security plan to be in place within 120 days of identification, regardless of the current status of the station. c. Possibly adjust language to allow sites under construction to have the later of 120 days or the operation date of the station. 3. R1.2 should be reworded: “The TO shall identify the primary Control Center with operational authority of each Facility identified in the R1 risk assessment.” 4. R2, if the assessments are concurrent, could this be a joint effort, with the result being 1 report? 5. R2.1, “unaffiliated” needs some clarification. Is this unaffiliated with the TO in any way? Could the TO use their Planning Coordinator, Transmission Planner or RC for the assessment, or do they need to seek out an entity from another region?
Yes

1. R4, what is the time frame for the evaluations? Is this to be conducted during the 30 or 60 month cycle outlined in R2 or more frequently? 2. R6.1, These are all “or” statements and 6.1.1 through 6.1.4 should be bullets, not numbers (this is outlined in the CIP-002-5 page 6, and should maintain consistency with the CIP standards format). 3. R6, Does the ERO have to approve of the third party reviewer? Is there going to be a criteria to determine “demonstrated physical security expertise”?
Yes
1 “primary control center” is confusing. NERC has a defined term “Control Center” which is intentionally not being used. What is the intent of not using the defined term? If the undefined term remains in use more clarity needs to be given on “primary control center”. 2. what is the definition of “widespread?” Does this mean outside of a Balancing Authority Area, outside of a Region or outside of an interconnection? More clarity is needed in the term. Additionally, TO’s may not have the data required to perform this type of assessment. There needs to be process in place for the TOs to obtain the data required to perform the appropriate assessment. 3. The SDT should review projects such as PRC-006 or MOD C, and define groups within the requirements to reduce the length of requirements. For example R4 could be reduced to the following, making the requirement easier to read and adding much needed clarity: “Each Applicable Entity shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Applicable Facilities as identified in R1 and verified in R2. The evaluation shall consider the following:… “ RSAW Comment: R1 “Evidence Requested” section doesn’t provide a time frame for the first assessment, no assessment prior to effective date will be considered, but there must be an assessment completed before the effective date to be complaint. This is a catch 22.
Individual
Dan Inman
Minnkota Power Cooperative
Yes
Yes
Yes
Yes
In the “Draft_RSAW_CIP-014-1_v1_2014_0409.pdf” document, on page 4 of 22, there is a Note to Auditors Concerning Third Party Verifications and Reviews. In this section there is a mention to the “concept of reliance means using the work of others to avoid duplication of efforts”. While the reference to “duplication” was in regards to unaffiliated third party verifications and reviews, we appreciate the SDT be congnitive of “duplication of efforts” as their developing the Standard and the RSAW. With the very restrictive timeframe for which the development of the Standard was required, this concept can get lost. We did see another

area in the Standard CIP-014-1 R5.2, which may be considered “duplication of efforts”. CIP-014-1 R5.2 states, the TO/TOP should have in their physical security plan(s) law enforcement contact and coordination information. On June 20, 2013, FERC approved Reliability Standard EOP-004-2, which identified types of reportable events and thresholds for reporting, requires responsible entities to have an operating plan for reporting applicable events to NERC and other entities (including law enforcement), and requires reporting of threshold events with a 24 hour period (Docket No. RD13-3-000). This Standard covers the need to incorporate law enforcement contacts in the operating plan. Requesting this type of information in both the operating plan required in EOP-004-2 and physical security plan in CIP-014-1 is a “duplication of efforts”. MPC believes the intent for CIP-014-1 was to identify and mitigate physical security risks, while the intent for EOP-004-2 is to improve reliability of the BES by requiring the reporting of events by Responsible Entities. MPC suggests removing Requirement 5.2 in CIP-014-1.
Individual
John Allen
City Utilities of Springfield, Missouri
Agree
APPA
Individual
kim moulton
Vermont Transco LLC
Yes
While we do agree with the need for the standard and the importance of it we do have comments on the proposed standard. The intention of this standard is to protect those facilities that are most critical to the bulk electric system. The CIP-002-5.1 criteria brings into play many facilities that while deemed critical to an entity are not likely critical to this standards definition and would not cause wide area impact.
Yes
Specifically the filtering of assets. While starting with CIP-002-5.1 as a starting point, the amount of analysis and assessment to determine if these facilities are critical and applicable to this standard may not be possible in the timeline proposed for this standard if a full transmission planning analysis will be needed. Many planning analysis performed previously by entities were not assessed to the specific defininition included in this requirement and therefore could require considerable work to be performed to analyze. The wording suggests that a full transmission planning assessment should be performed for all CIP-002-5.1 facilities and not to just those an entity feels may cause wide area impact. What if you do not agree with the third parties review of your assessment? what evidence will be required to prove that you do not need to agree with their assessment? If an entity identifies a facility as critical does this require that the control center operating this facility must also have a full physical security plan per the requirements later in the standard?

Yes
how long will and entity have to complete their plans designed due to the evaluation of threats? It appears that the standard is saying that you must develop a plan and a timeline to complete your actions associated with the plan. What if a timeline needs to be adjusted at some point, will an entity have to notify their RRO? Or just track all changes and their need to provide to an auditor during a full audit of the standard?
No
Group
Western Area Power Administration
Lloyd A. Linke
Yes
Western agrees with what we understand as the applicability, based on the CIP-014 Workshops. However, we have some concern with the undefined term 'collector bus facility'. Without a definition for collector bus facility we are concerned that some parties may consider the entire switchyard at a generating station as a collector bus facility. Based on the discussion during the CIP-014 Workshops we do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Yes
Western agrees with the approach of using Requirements R1 and R2 to identify whether an entity is subject to Requirements R4-R6. However, we suggest that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assessment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term "BES impact assessment" so it is clear that the initial evaluation is of risk to the BES if the substation is damaged or rendered inoperable. Western recommends revising R1 1.1 to: "Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment." This would consolidate the two bulleted actions and make them equally applicable. We believe a 60 month interval would be a more appropriate period for this type of assessment. Western suggest the drafting team clarify requirement 2.1, which directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment; however, these NERC functional entity designations do not appear in the applicability section of the standard. We also suggest reconsidering the short 90-day period to ensure verification of the risk assessment. This may not allow every Transmission Owner to establish a contract with an unaffiliated verifying entity during the standard's implementation time period.

Yes
: We recommend striking the qualifier regarding the ASIS “Certified Protection Professional or Physical Security Professional” from the standard R6-6.1.1 as it is inclusive of only one organization and may not provide the best support for each entity . Simply having these certifications does not guarantee the necessary knowledge to perform this unique work. We believe the language does not support the intent of the FERC Order as identified in paragraph 11. We request the Drafting Team clarify the scope of the third party review process identified in R6 and tie the requirement to a specific and established method as consistent in accepted practices, such as the ISO processes. We recommend the third party review process be clarified as a review of the primary entity’s adherence to their established processes in evaluating threats and vulnerably, as well as their security plan(s). We believe the current audits conducted by the regional entities satisfy the third party review process as identified in the FERC Order, paragraph 11. We do not believe R6-6.4 adequately protects the sensitive information contained in the risk, threat, and vulnerability assessments, or the security plan(s). These reports may contain sensitive and/or classified information, or otherwise information that if released would jeopardize the BES, with little to no penalty for an offending party.
Yes
In the VSL for requirement R5, in all four severity levels, states that the security plans need to be developed for the facilities “identified in requirement R1”. However Requirement R5 only requires the plans to be developed for facilities ‘identified in Requirement R1 and verified according to Requirement R2,”. The VSL should be modified to include the statement ‘and verified according to Requirement R2. The first row in the Table, in the RSAW, describing the evidence required in requirement R1, it states that any risk assessments conducted prior to the effective date of this standard are not relevant. The Implementation Plan states that “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” There appears to be a conflict between these two statements, unless the intent is that the initial risk assessment needs to be completed on the effective date. Also, normally, unless the implementation plan provides a different time line, you need to be compliant by the effective date. In the RSAW for requirement R6 the fourth row in the Evidence Requested table, it asks for evidence that includes the “reasons or compensating mitigating measures for not implementing the recommendations for the reviewing party.” Requirement R6.3 of the standard only requires the Transmission Owner or Transmission Operator to “Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.” These two statements should be clarified in order to ensure consistent enforcement.
Individual
Lynnae Wilson
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.
Yes

Vectren supports the use of the CIP-002-5.1 medium impact criteria. This approach focuses on the facilities that could have a true adverse impact to the Bulk Electric System and provides consistency with approved standards.

No

Specifically, Vectren recommends that R2 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to designate registered Planning Coordinators, Transmission Planners, or Reliability Coordinators as the approved verifiers for entity risk assessments AND to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later – leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

No

Specifically, Vectren recommends that R6 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later – leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

Yes

Vectren recognizes that this drafting effort required significant contraction of drafting and approval processes, and Vectren appreciates the work of the drafting team. Vectren is

supportive of the goals of the standard, supports R1, R3, R4 and R5. Vectren urges the drafting team, NERC and FERC to remove entirely or add detail to the requirements R2 and R6, and to add specific audit criteria in the RSAWs, so that entities can have some confidence that their risk assessments performed in good faith, will be considered compliant with this Standard.
Individual
Venona Greaff
Occidental Chemical Corporation
Agree
Ingleside Cogeneration, LP
Group
Texas RE
Derrick Davis
Yes
The applicability should include the TP, PC, RC, and the unaffiliated entity as they are noted in this standard.
No
1. For R1, the Transmission Owner is not the appropriate entity to conduct the type of transmission analysis that the requirement describes. It seems like a more logical process would be for the Transmission Planner to conduct an analysis of all substations meeting the applicability in 4.1.1.1 thru 4.1.1.4, and then, if the removal of a substation results in Cascading, instability, or uncontrolled separation, the TP will then notify the TO & TOP to conduct the security threat evaluation per R4 at only those substations identified by the TP. 2. R1 - A “risk assessment” pertains to the physical security of Transmission Facilities while a “risk-based assessment” pertains to identification of Critical Assets and Critical Cyber Assets. The two phrases are too similar in meaning to each other, but possess differing meanings and intents. 3. For R2, if the approach described in #1 is accepted, it may also satisfy R2 in those cases where the TP is independent from the TO. The independent verification would also be the responsibility of the TP, utilizing another TP, the PC, the RC, or an unaffiliated entity as described in the current language. 4. For R3, if the approach described in #1 is accepted, the initial notification to the TOP would originate from the TP.
No
1. The sequence and timelines for R5 and R6 need to be reviewed. R5 states the TO “shall develop and implement” the security plan within 120 calendar days of completion of R2. R6 states the 3rd party evaluation can occur concurrently with or after completion of R5. It seems like the 3rd party evaluation should be completed before the plan is implemented in R5, otherwise the entity may be planning for or implementing measures that may not be appropriate for the risk level. 2. R6 also 3. Also, who evaluates the implementation phase of security plan and whether or not it was implemented correctly or if the plan was effective? There should be an entity assigned for this task. There should be an exercise (like GridEx) to

test the plan. 4. The third party reviewer could be the same entity in R2 and R6. This could be a question of independence. It also does not indicate the third party actually verifies the implementation of the security plan(s) in R6. This does not permit the Compliance Enforcement Agency to place reliance upon the work of the third party.
Yes
Several places in the standard refer to notifying the Transmission Operator for stations that meet the higher risk profiles. However, the language is not clear as to what is expected from the Transmission Operators when a physical security incident occurs at one of those substations during real-time operations. Finally, this entire process can exceed four hundred days, which is excessive.
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
No
FMPA commends the efforts of the SDT to lay out an excellent process for risk assessment in accordance with the FERC Order in such a short time frame. We only have few comments. WHAT DOES “CONTROL CENTER” MEAN Is there a signifance for not using the capitalized term of Control Center throughout the standard? It seems to FMPA that the defined term “Control Center” ought to be used. If the intent is that “control center” and “Control Center” mean two different things, then, what does “control center” mean? If the intent is to include large TOs that may be part of a large TOP, such as a large utility in an RTO, that do not have Control Centers; then, FMPA recommends using a different term such as “the location of the SCADA system that has remote control of breakers associated with the identified substation/station” or similar might avoid confusion. WHAT DOES “UNAFFILIATED” MEAN The term “unaffiliated” may be a source of ambiguity and conflict without further definition. For instance, dictionary.com defines affiliated as: “being in close formal or informal association; related” So, this would imply that peer members of the Transmission Forum are affiliated, which we do not believe is the intent of the SDT. FMAP believes the SDT’s intent is as Black’s Law Dictionary defines affiliate: “1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.”; which would mean that peers within the Transmission Forum are unaffiliated, but subsidiaries of a company are affiliated, or members of a Joint Action Agency are affiliated. It also aligns with FERC’s definitions for Affiliate in their market based rates regulations 18 C.F.R. 35.36(a)(9) and in the Pro Forma OATT. FMPA suggests using a footnote to clarify use of the term unaffiliated, such as “Use of the term unaffiliated is in relation to Black’s Law Disctionary defition for affiliated: ‘1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.’”

PROPER QUALIFICATIONS FOR RISK ASSESSMENT VERIFICATION FMPA appreciates the challenges of defining qualification for independent verifiers while offering registered entities a broad choice for selection. We interpret that requirements R2 and R6 grant the applicable entity sole authority to choose the 3rd party verifier as long as they meet the qualifications contained within those requirements. Is FMPA correct in that interpretation? CHANGE MANAGEMENT OF THE RISK ASSESSMENT The standard is somewhat ambiguous on what happens if the responsible entity chooses to revise it's risk assessment of R1 sooner than the required 30 or 60 calendar months. Does every minor revision to the risk assessment require another 3rd party review? Or would only major system changes (e.g., due to adding a major new investment in the power system like a new 500 kV line) require review? Or regardless of system changes, would the review occur once every 30/60 months? FMPA suggests clarification to R2 to say that minor revisions to the risk assessment due to minor power system changes in between the 30/60 month periods do not need a separate 3rd party verification.

No

Again, FMPA commends the SDT for a job well done. Just a few minor comments. See response to question 1 concerning use of the terms "control center" and "unaffiliated". CHANGE MANAGEMENT OF THE VULNERABILITY ASSESSMENT AND SECURITY PLAN Similar to our comments regarding change management of the risk assessment, it is ambiguous as to how we would implement change management related to the vulnerability assessment and security plans. R4 has no periodicity requirement, but, instead seems to require responsible entities to continuously reevaluate their vulnerability assessments in response to events listed in bullets 4.1, 4.2 and 4.3. If the entity changes their vulnerability assessment to include new threats, does every revision require a new 3rd party review? How do we come to agreement what constitutes a valid "trigger" for a new vulnerability assessment? It seems to imply that each of us would need to have an independent 3rd party on retainer to review our assessment of every intelligence or threat warning from governmental or regulatory agencies, or new attacks that each entity becomes aware of. Is that the intent? If so, what consititues a "warning", e.g., is it an "official" warning through some sort of official channel, such as a NERC Alert? If so, what happens if an entity decided to act on an "unofficial warning", such as a media release, to revise their vulnerability assessment – would that also need a 3rd party review? FMPA suggest clarifying 4.3 with "Official intelligence or threat warnings …". R5 seems overly ambitious. 120 days, or 4 months, is not a lot of time to perform a vulnerability assessment and develop and implement a security plan, especially in response to a newly identified threat vector/warning, and especially considering that a revised security plan may include capital investments in measures like new enclosures, vehice barriers, or the like. Is the intent that a security plan could be a phased approach, e.g., implement an interim security plan within 120 days while future improvements to that plan take longer? If so, then the language of the requirement ought to reflect that intent. FMPA suggest a modification to R5 such as: "… shall develop and implement the first phase of a documented physical security plan(s) … within 120 calendar days …" In addition, R5 does not seem to fit temporally with R2 and R4 well. R2 requires periodic risk assessments every 30/60 months. R4 seems to require changes to vulnerability assessments in response to newly known threat vectors. The timing

of R5 refers to R2: "… within 120 calendar days following the completionof R2" with no reference to a revision to the vulnerability assessment. This causes FMPA to belevie that revisions to the security plan as a result of a new threat vector and a revised vulnerability assessment of R4 would not need to be required until 120 days following the next periodic risk assessment of R2. Is that the intent? If that is the intent, if an entity chooses to revise the security plan earlier, would that then need an 3rd party verification at that time, or at the time of the periodic risk assessment?
Yes
FMPA has concerns for the RSAW and the lack of direction to auditors from the RSAW concerning the scope of their review. The auditor should not have a subjective decision regarding the sufficiency of the risk assessment, vulnerability assessment or security plan of the TO/TOP. The unaffiliated 3rd party is the source of qualified expert subjective opinion on the sufficiency of the risk assessment, vulnerability assessment and security plan. As such, the RSAW ought to clearly define the scope of the auditor's review of the risk assessment, vulnerability assessment and security plan. FMPA suggests rewording the "Compliance Assessment Approach"portions of the RSAW that call for these reviews to read something like the following (specific to R1): Review the entity's risk assessment to answer the following: a. Were all of the entity's assets, existing and planned to be in service within 24 months of the date of the documented risk assessment, and applicable to the standard (Applicability Section 4.1.1), included in the assessment? b. Was a transmission analysis or transmission analyses identified and documented to evaluate whether any applicable Transmission station(s) and Transmission substation(s), if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? The auditor is not to evaluate the sufficiency of such analyses; but rather whether such analysis was documented. c. Was the assessment conducted within the timeframes identified in bullet 1.1? d. Was the primary control center(s) identified in accordance with bullet 1.2?
Individual
Thomas Foltz
American Electric Power
Yes
Yes
Yes
Yes
It is AEP's understanding that regarding R5, the phrase "develop and implement a documented physical security plan…within 120 calendar days" means that, within 120 days, the physical security plan must be completed and that the entity is working toward implementing the plan and does not mean that the plan must be fully implemented within

120 days. AEP urges the clarification of that expectation within R5 so that the requirement is unambiguous. Regarding R6.4, please clarify whether the procedures for protecting sensitive or confidential information would include suitable terms and conditions within a third party contract.
Group
Duke Energy
Michael Lowman
Yes
Yes
Yes
Yes
(1) Duke Energy suggests that language should be incorporated either in the proposed standard or RSAW to allow for the flexibility in modifying the timeline specified in R5.3. We believe there are unforeseen circumstances that could occur which would result in the proposed timeline shifting from the intended completion date. Examples include, but are not limited to: a. Unplanned outage of transmission or generation facilities that results in canceling scheduled work. b. BES reliability concerns should the facility be out of service for a short or extended period of time. c. Third party vendor's availability in implementing recommendations made by an entity or unaffiliated third party verifier. For these reasons, we believe a provision is needed to allow for this type of flexibility in modifying the timeline specified in R5.3.
Individual
Anthony Jablonski
ReliabilityFirst
Yes
ReliabilityFirst supplies the following comments for consideration: 1. ReliabilityFirst believes there may be a perceived disconnect between the Applicability Section and Requirements 5 and 6. Requirements 5 and 6 introduce new requirements surrounding the Transmission Owners "primary control center" though the "primary control center" is not listed within the Applicability section as an asset the Transmission Owner owns that is included in the standard. Consideration may be given to adding "primary control center" under section 4.1.1. [Note: Since "Control Center" is a NERC defined term, this term should be capitalized throughout the standard.] 2. Applicability section 4.1.1.4 - ReliabilityFirst believes the term "as essential" is ambiguous and may cause unintended compliance monitoring implications. ReliabilityFirst recommends the following for consideration: "Transmission Facilities identified

[in] Nuclear Plant Interface Requirements [which provide offsite power].” ReliabilityFirst believes the recommended language addresses the intent of the SDT.
Yes
ReliabilityFirst supplies the following comments for consideration: 1.Requirement R1 - ReliabilityFirst believes there may be a gap in the timing of performing the risk assessment for new Transmission stations and Transmission substations which are planned outside the 24 month window as required in Requirement R1. For example, as written, if a new Transmission stations or Transmission substation is planned for month 25, it would not be included within the initial risk assessment. Thus, there is a potential for this new Transmission stations or Transmission substation to not be assessed for 30 calendar months (for a Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable …) or 60 calendar months (for a Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability…” With the potential gap in assessing new Transmission stations and Transmission substations being so long, ReliabilityFirst believes reliability may be compromised. For these reasons, ReliabilityFirst recommends the following for consideration: “Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months)…” and including a new bullet under Part 1.1 which states “At least prior to the implementation of all new Transmission stations and Transmission substations (if not assessed within the initial or subsequent risk assessment)” 2. Requirement R3 part 3.1 - From a standards writing perspective, if there is only one sub-part, ReliabilityFirst recommends including it within the Parent requirement R3. Typically sub-parts are only included if there are more than one.
Yes
ReliabilityFirst supplies the following comments for consideration: 1. Requirement R5 - ReliabilityFirst requests clarification on why the term “primary control center” is used throughout the document instead of just “control center”, as it seems both a primary and secondary control center would be of equal importance (and have similar vulnerabilities) to reliability.
Individual
Larry Watt
Lakeland Electric
Agree
Florida Municipal Power Agency (FMPA)
Individual
Donald E Nelson
MA Dept. of Public Utilities
Agree

Agree with the comments made by NPCC.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Agree
American Public Power Association (APPA). In addition, Austin Energy states the following: The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this Standard may be subject to disclosure under state open records laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard designating the produced, gathered, used and maintained records related to compliance with this Standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure.
Individual
Kevin Lyons
Central Iowa Power Cooperative
Agree
ACES
Group
Peak Reliability
Jared Shakespeare
Yes
Yes
Peak believes the RC entity should perform the R2 verification because the RC has the wide-area view in the Western Interconnection. The alternative would be to have individual transmission entities perform varied verifications, which could result in inconsistent methodologies and results.
No
Individual
Robert Trowbridge
Consumers Energy Company

Yes
With Michigan situated as a peninsula, Michigan infrastructure may be at a lesser risk, based on the limited number of interconnect avenues into and out of our system. Meaning the highest level of criticality likely would be identified as those key interconnect points, and not the entirety of our system. From our experience with the blackout of August 2003, BES implications were centered in southeast Michigan and although affected, we were able to successfully minimize/sustain our base load generation requirements. Any substation targeted in Michigan may not have a cascading effect on the BES.
No
We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
No
We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Yes
Develop a requirement to protect information shared between entities and third party organizations. Requirement number 6 should be revised to state “…third party reviewer that is either…” 6.1.1 or 6.1.2 or 6.1.3 or 6.1.4. R6 seems vague and should be revised
Individual
Chantal Mazza
Hydro Québec TransÉnergie
Yes
No
Hydro-Quebec TransEnergie (HQT) agrees with this approach but requests that the SDT remove the term "unaffiliated" from Requirements R2 and R6.1 HQT notes that the term "unaffiliated" is not used in FERC Order 146. Paragraph 11 of the Order states "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator." Moreover, it appears that it is not FERC's intent to introduce this restriction regarding the choice of a third party. HQT therefore believes that the use of the term “unaffiliated” goes above and beyond what was stipulated in the FERC Order. Furthermore, the term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities (RC, PC and TP) that the SDT is seeking in the draft standard. The Reliability Model uses the term "functional entity" to apply to a class of entities without making reference to specific organizations that register as functional entities. For some Canadian jurisdictions, the use of the term "unaffiliated" renders the standard more stringent due to the fact that certain Canadian entities such as Hydro-Québec TransÉnergie are simultaneously

registered as TO, TOP, PC and RC. For integrated modeled entities, the restriction of available options that would otherwise be available (such as selecting a PC, TP or RC for the risk assessment verification under R2), makes it difficult to identify an entity with the required expertise capable of performing the reviews stipulated in the standard. HQT believes that the risk assessment of a TO should only be verified by the RC or the PC that has supervision (real-time or planning) over the said TO's assets because only the RC or the PC can ensure a comprehensive approach to critical facility identification that considers the reliability of an entire area. For these reasons, HQT believes that the expression "third party" alone is sufficient and consistent with the expressed concerns in the FERC Order.
No
The same comments regarding the term "unaffiliated" in Question 2 above apply to R6. HQT believes that the SDT should remain general about the security measures that should be put in place. Requirement R5.1 states "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." We believe that rather than the standard dictate what type of measures are to be implemented, it should be rephrased to remain general and use similar language that is used in paragraph 9 of the FERC order. Suggest rewording the requirement to "Resiliency or security measures designed to protect against potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.".
Yes
The following are suggestions to facilitate reading of the standard, as well as its future translation: All requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary. R1: Remove "transmission analysis" from the sentence "The initial and subsequent risk assessments shall consist of transmission analysis or transmission analyses designed to …" We believe this repetition is unnecessary. R2.2: The first part applies to an entity that is not subject to the standard and should be removed from the standard. R2.3: Replace the word "identification" with "assessment". Remove the word "either" Rephrase R4, R5 and R6 (add "a"): " ...a transmission substation, or a primary control center". R4 and R5: Remove the part "…that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation". It only complicates the reading of the requirement (the TOP is not notified by the TO unless it has operational control over an asset identified in R1). If the first parts of R4, R5 and R6 are intended to identify the functional entities to which the requirement applies, we suggest "… and each Transmission Operator notified by a Transmission Owner under requirement R3, shall …" for the TOP portion (line 3 to 6 of R4, R5 and R6). We believe that it would greatly improve clarity and readability of the requirements. R6.1: rephrase to "from one of the following". Furthermore, the numbers 6.1.1 to 6.1.4 should be replaced with bullets as is the case in R1.1, R2.1, and R2.2. Rephrase R6.1 and R6.1.1 to reflect the language used in the rationale. We believe limiting the reviewer to someone with a CPP or PSP certification goes beyond what the FERC order requesting. Suggest rephrasing to "with appropriate expertise of the evaluation performed". Guidelines and Technical Basis on requirement R1: HQT agrees with the fact that the TO has discretion to

choose the specific method to establish the risk assessment, and that it is relevant that the Guidelines proposes examples. However, the proposed example of "removing all lines to a single Transmission station" seems to present a very stringent impact considering a physical attack on a facility. We ask the SDT to propose others less stringent examples that would be more in line with realistic physical attack, such as loss of a large section according to physical organisation of the facility, or loss of all main transformers, etc.
Group
Dominion
Connie Lowe
Yes
No
Measure M1 - R1.2 -- Measure M1 does not address sub-requirement R1.2 which requires the Transmission Owner to identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment. Dominion recommends the SDT determine whether M1 should include the control center. R2.3 - Relative to R2.3, Dominion does not agree that the TO should have to document the technical basis for retaining assets that have been suggested for removal by the third party. R3 - Dominion suggests R3 be revised to strike the words ‘and verified according to Requirement R2’, and changing R2 to R1.2 in the next two instances where R2 is mentioned. This is due to the reason there is nothing included in R2 that requires verifing primary control centers.
No
R5 and R6 are written for the initial risk assessment and don’t necessarily apply for subsequent risk assessments. Is the expectation that 3rd party reviews be performed for R4 and R5 every time R1/R2 is run, particularly if there are no changes? Dominion recommends that the SDT modify this in the event the R1 list changes (ie: add stations) to require a subsequent R4/R5 reassessment. If stations drop off, or no change to R1 list for subsequent assessments, then subsequent R4/R5 reassessment is not required. R6 - Through continuous improvement processes and lessons learned, there will be expected changes to the security plan(s). What changes are allowed to the security plan(s) without triggering a 3rd party review?
No
Individual
Michiko Sell
Public Utility District No. 2 of Grant County, WA
Public Utility District No. 2 of Grant County, WA
Yes

Language contained in R1 does not align the performance of risk assessments of Transmission stations and Transmission substations with the actual commissioning or energization of such facilities. To ensure that risk assessments and subsequent risk assessments address existing and planned Transmission stations and Transmission substations to be in service within a risk assessment window the following edits are recommended to R1: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months) .. 1.1. Subsequent risk assessments shall be performed at least once every 30 calendar months. (this would apply to all applicable TOs) GCPD also supports comments made by APPA regarding the insertion of the language addressing Confidentiality and treatment of Critical Facilities Information. GCPD's suggested language is as follows: Risk assessments and evaluations of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure.
Yes
R2 references primary control center(s). Since Control Center is a NERC defined term GCPD suggests that all references to the Control Center be capitalized within the Standard and that "primary" be defined within the standard to not include "back-up" Control Center(s).
Yes
GCPD appreciates the flexibility built into the Standard language that allows tailored evaluations of potential threats and vulnerabilities to its own facilities. GCPD supports APPA's suggested edits to the Standard to enhance clarity of requirements under R4, R4.1 & R4.2. In addition, APPA's suggested removal of "and implement" under R5 clarifies that the intent of R5 is to develop the physical security plan, not fully implement the plan within 120 calendar days. This would better align the Standard language contained in R5.3.
Yes
GCPD feels that the implementation schedule is somewhat arbitrary and demonstating compliance with the implementation schedule conflicts with language contained in the proposed RSAW. GCPD supports RSAW edits as proposed by APPA to address these discrepancies. GCPD proposes the following edits to Requirement language addressing implementation timing to allow for enforceable and auditable time lines not dependent upon the unique completion date of the initial risk assessments conducted by the RE. 2.2. ...The Transmission Owner shall ensure the verification of the initial risk assessment performed under Requirement R1 is completed within 90 calendar days following the effective date of this Standard. Subsequent risk assessments shall have verifications completed within 90 calendars days of completion of the risk assessment. R5. ...and primary Control Center(s) within 210 calendar days following the effective date of this Standard. Changes to recognized applicable facilities under this Standard as identified under Requirement R1 and verified according to Requirement R2, shall require review of the physical security plan(s) within 90

calendar days of completion of associated risk assessments. ... General commentary: in October 2012 the Cost Effective Analysis Process (CEAP) was approved for a “pilot”. The NERC CEAP was intended to integrate cost consideration and effectiveness into the development of new and revised standards. The first phase of the CEAP was to be implemented during the SAR stage to determine cost impact and identify “order of magnitude” or potentially egregious costs, to determine if a proposed standard will meet or exceed an adequate level of reliability, and what potential risks are being mitigated. The second phase was to be conducted later in the standard development process and afford the industry the opportunity to offer more cost efficient solutions that may be equally effective to achieving the reliability intent of the draft standard. This report would be posted at the time the standard is balloted. The report was intended to present the data collected in a manner which will provide the industry with representative cost implementation and effectiveness information to allow a more informed choice during balloting. Based upon the urgent nature of this Standard, phase two would need to be applied. The CIP-014 Standard requires costs to be incurred to comply with Requirement R5. In addition, there may be substantial costs incurred to implement the Physicial Security Plan(s). The CIP-014 Standard is an ideal standard upon which to exercise the CEAP. The information resulting from the CEAP would be beneficial not only to government officials, but also the industry as a whole.
Individual
Brett Holland
Kansas City Power & Light
No
There is a use of the term "critical" being used in several NERC Standards, which can cause unintended confusion. Since the applicability of this draft Standard is derived from the approved CIP-002-5.1, can this proposed Standard be added as a revision to CIP-002-5.1?
No
In R1, we have concerns about the ambiguity associated with the term "assessments". Can you provide examples of the types of assessments that would be acceptable to meet R1 and that would be CIP audit worthy in the future. We have the same concern in R2 with the term "third-party". Will there be a list of pre-approved third party contractors or will the RE's review and approve a third-party at the request of the registered entity prior to their use in the verification process as described in R2?
No
Same comments about "third-party" from Question 2.
No
Group
APPA
Joe Tarantino
American Public Power Association (APPA)

SMUD supports the APPA comments and is specifically concerned that records and information developed and maintained under each of the requirements for this standard are afforded the necessary protection through an introduced section, #7 Critical Facilities Information. We respectfully ask the Standard Drafting Team to ensure that AUTHORIZED ACCESS to information pertains to ANY RECORD AND INFORMATION associated with the Physical Security Standard.
Individual
Nick Braden
Modesto Irrigation District
Modesto Irrigation District supports the comments submitted by American Public Power Association/Large Public Power Council
No
MID agrees that maintaining selection criteria consistent with CIP-002-5 is a prudent approach. However, if a facility is worthy of protection against a cyber attack, why is that same facility not worthy of consideration and evaluation for a potential physical attack? Inclusion of 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' as an additional criteria is also prudent. These criteria focus on the immediate impact of the physical attack. What is missing is the longer term impact - if serious physical damage is the result, can the damaged system perform adequately during subsequent peak loading periods? MID understands that these changes would extent the scope of the standards coverage beyond what was included in the FERC order. MID would like to respectfully suggest that the FERC order is a step in the right direction but did not fully consider all of the potential physical attacks that could cause 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' or impair long term reliability of the system. MID feels that in responding to the FERC order, it would be acceptable to ‘do the right thing’ and step up to the challenge and evaluate all facilities identified in CIP-002-5 as high or medium impact the system against possible physical attacks.
Yes
Yes
No
Individual
Dixie Wells
Lower Colorado River Authority
Agree

Lower Colorado River Authority
Individual
Alan Johnson
NRG Energy, Inc.
Yes
This standard should not address generation interconnection facilities because the BES is designed to withstand the loss of generation facilities through the use of regional reserves.
Yes
NRG agrees the approach described in Requirements 1 through 3 address the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: • Primary control centers are referenced in the “purpose” of the standard, but are not included in the “applicability” section. For clarity, NRG suggests the addition of section 4.1.1.5, stating “Control Centers and backup Control Centers associated with the Transmission stations and Transmission substations identified in requirements 4.1.1.1 through 4.1.1.4.” • R1 directs that the Transmission Owner to perform an initial risk assessment with subsequent studies and include an unaffiliated third party to verify the risk assessment performed. NRG is concerned the standard does not indicate how information shared under this Requirement will be protected and held in confidence. NRG believes the information subject to this standard should be treated as Critical Energy Infrastructure Information (CEII). • R1 is vague in providing guidance as to the criteria to be used in developing the risk assessment. NRG appreciates this is intentional to allow flexibility in developing the assessment. However, this results in the potential for a determination of non-compliance during the audit process. NRG suggests reliance on the CIP-002 standard used for defining Critical Assets, which is based on solid metrics. • R2 seems to allow the same third party to perform both the initial risk assessment and the review of the initial risk assessment, potentially negating the need for a separate review. • R2.2 calls for review of the results of the initial risk assessment by an unaffiliated third party. The standard provides no guidance regarding the criteria (assumptions, contingencies, etc.) to be used for this review, which could provide results differing from the initial assessment. More objective measures should be incorporated.
Yes
NRG agrees the approach described in Requirements 4 through 6 addresses the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: • R5.1 provides no guidelines or examples of how to combat certain threats, or even what threat thresholds require accounting for. NRG appreciates the flexibility built into the requirement. However, NRG is concerned this flexibility could result in “interpretation” issues during future audits of compliance with the standard. • The ability to meet the time horizon commitment for providing the third party assessment of the vulnerabilities and security plan are contingent upon the availability of certified parties that

can adequately perform these assessments. NRG is concerned there may be a lack of qualified resources available to the industry to complete the necessary reviews within the required time frame. • Because the reliability of the bulk power system depends on numerous susbstations all across the nation, it would be more effective to increase the monitoring of the grid to ensure timely, effective re-routing of power when a disruption occurs. • Minimum physical standards should be established within the security plan that include industrial standard chain link fencing with barbed wire topguards; gates secured with chains and locks (not the alloy metal collar around a post); signage that clearly states No Trespassing every 100 ft., or on each perimeter side at small footprints; cameras that are monitored by the appropriate transmission control center, security control center or a contract central monitoring service and capable night viewing to be able to identify intruders.
No
Individual
Curtis Klashinsky
FortisBC
Yes
No
The audit provides an independent review of an entity's application of the standard and therefore, an additional third party review should not be required as described in R2. It is agreed that if a null set is identifed, the rest of the standard does not apply.
No
The third party review of the security plan does not guarantee an objective evaluation as they would be funded by the requesting entity. The standard could state that the entity should follow an industry standard technical guideline. The audit provides an independent review of an entity's application of the industry standard technical guideline and therefore, an additional third party review should not be required as described in R6.
No
Group
New Brunswick Power Corporation
Alan MacNaughton
No
New Brusnwick Power (NB Power) agrees with the “applicability section” but not with portions of the preamble above, in question 1, which expands beyond applicability and states that “Furthermore, the standard drafting team expects many who are “applicable” to the standard will not identify facilities through their Requirement R1 risk assessment and

Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." To our knowledge there is no evidence to support the standards drafting teams statement that they expect that many of the applicable entities will not identify facilities through R1 and R2. FERC's statement that "we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" is not sufficient evidence. NB Power is concerned that the cost impact of this standard may be underestimated as a result of this view that the number of critical facilities will be small. Please see comments below with respect to R1 and R2.

No

In general, a TO may not have the capability to conduct a risk assessment to determine if an identified facility that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such an assessment requires a wide area view of the Interconnection. It is proposed that the risk assessment be conducted by a PC, or RC for the area in which the facility is located. Doing so would satisfy the third party verification requirement as the TO would not be conducting the analysis. It is the opinion of NB Power that the technical details concerning the transmission analysis, in the proposed standard, are overly vague. This could lead to an inconsistent application of the analysis between entities as well as create obstacles with consensus concerning the proposed 3rd party verification. NB Power suggests a clear analysis methodology be drafted to establish a common basis for study criteria with the ability for each entity to apply additional specific requirements for their respective area. For corporate bodies, such as a vertically integrated utilities, that are registered as the RC, TOP, PC, TP and TO for a particular area, it is the opinion of NB Power that the requirement for unaffiliated 3rd party verification is overly stringent and of little value. The verifying party is limited to entities that have transmission planning or analyses experience, or, are registered as a PC, TP, or, RC from an adjacent area. NB Power is of the view that there are no unaffiliated entities with sufficient knowledge of the local transmission system to provide a meaningful verification within a 90 day period. As a government owned utility, NB Power is required to follow procurement processes which will make it difficult to meet the 90 day period for the third party verification. NB Power is also concerned that it could be non-compliant with the requirement if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance. It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated verifying 3rd party in requirement R2.3. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated verifying 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd parties recommendations.

No

NB Power is concerned with the 120 day timeline to implement a physical security plan that would meet the third party verification requirements. Having limited knowledge of physical security issues NB Power will likely rely on the third party verifier to work with NB Power in developing a security plan. NB Power is not aware of any analysis that was done to ensure that there is enough capacity within the “physical security industry” to support the work load increase resulting from the approval of this standard and as such is concerned that 120 days may be insufficient. NB Power is concerned that it could be non-compliant with R6.2 if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance. It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated reviewing 3rd party in requirement. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated reviewing 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to a consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd party’s recommendations.
No
Individual
Mark Wilson
Independent Electricity System Operator
Yes
We agree with the inclusion of the Transmission Owners and Transmission Operators as they have the obligations to conduct an evaluation of the potential threats and vulnerabilities to a physical attack on each of their respective transmission stations/control centres.
No
While the proposed R1 to R3 collectively meet the FERC requirements for having an entity to identify the critical facilities and having the assessments of such identification verified, we believe it is more appropriate that the 3rd party verification be performed by NERC registered entities only (which could be the Reliability Coordinator, Planning Coordinator or Transmission Planner). An entity that has transmission planning or analysis experience may only have an outside equivalent representation of the BES and their ability to conduct an analysis with a “wide area” view of consequences may not be possible. As such, we suggest to revise Requirement 2.1 by eliminating the second bullet point : “An entity that has transmission planning or analysis experience”.
Yes
Individual

Kenn Backholm
Public Utility District No.1 of Snohomish County
Agree
Salt River Project ("SRP")
Individual
David Grubbs
Ciy of Garland
No
Applicability: The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective: 4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3. Please state clearly the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
No
R1 - The auditors should be limited to verifying that a study was completed using the assumptions agreed to by both the TO and the reviewer. The auditor should accept any study and assumptions jointly agreed to by the TO and the reviewer without requiring additional engineering justifications as to why one type of study was used instead of the auditor’s preferred methodology. To summarize and echo FERC Commissioner Norris in his clarifying statement, included with the FERC Order that is the basis of the CIP-014 Standard, that if the Planning Studies indicate a transmission solution that would cause the substation to no longer cause the cascading outage that the transmission project could be initiated in lieu of the security plan. The additional transmission solution would potentially add other operational benefits other than just “security” and therefore may be more practical than the security plan in R4 through R6. In the guidance document, statements should be made that a TO may make additional planning studies at any time prior to the 30 months and if the third party reviewer concurs the updated study no longer shows a cascading event, whether due to changing grid conditions or system improvements, the standard would no longer apply including the continued implementation of the security plan. The TO should also notify the owner of the primary control center the substation no longer causes a cascading event. R2 - Timelines to complete third party verification under R2.2 and third party review under R6.2 are both too short. Increase 90 days to 120 days or 180 days. a. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A 90-day time limit may not provide sufficient time to conduct and verify a revised or supplemental BES assessment. b. For security reviews, conducting an accurate and meaningful review with sound recommendations applicable to a specific TPs facts and circumstances may require

additional time for assessment and discussions with the TO. A short review window is more likely to lead to misunderstandings, or disagreements with the TO which in turn could lead to discrepancies or improper application of the assessment requiring justification. This could cause the reviewer to avoid making recommendations that should be considered by the TO and improve the TO's assessment. c. As currently written, it appears if the TO disagrees with the reviewer's comments and writes a technical reason why he believes the original conclusion were correct, the recommendation(s) by the reviewer may be rejected and the TO's decision is final. Although I agree with this position it may be interpreted differently by the auditors. Please clarify which was the intent of the SDT. R3 - No comments
No
R4 - Sub requirement 4.1 should be modified to include specific language focusing the security study to those elements within the substation that can affect the reliability of the BES. The security plan should protect those elements of the substation as identified in the planning study in R1 that could cause the cascade or other unacceptable event identified in R1. Many substations identified in these studies are very large geographically and potentially very expensive to protect elements that may be located 30 to 50 feet above the ground. If these elements are determined to be critical they should be protected. If not, there is no justifiable reason to expend the resources to protect these devices. The security plans should concentrate on the protection of elements that could actually cause a cascading event, otherwise large expenditures may be made while adding no benefit or improvement to the reliability of the BES. R4.1 should read: 4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) including the identified elements within the station, substation or control center, that need to be protected that could initiate the cascading collapse identified by the planning study in R1; Under both R4 and R5 clarification should be provided to the auditors affirming that auditors do not need the work papers, or backup information used in preparing the security plan, it is preferable auditors be allowed to only view the plan on site and not be allowed to take a copy of the plan for their files due to the sensitive nature of the security plan. Having copies of the security plans of critical targets consolidated into the files of the auditing entity increases the security risk to the plan and identified assets do to a security beach or accidental release of the file. While having one security plan of a critical location is a security risk in and of itself, having a compilation of security plans by one entity becomes a national security risk. R5 - states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." The "and implement" should be deleted. It should be made clear the facilities, additional employees or other measure identified in the plan are not required to be in place at the end of the 120 days. The requirement should be clearly stated that a timeline needs to be developed as part of the plan and the TO and TOP will implement the plan per the timeline identified in the plan. The implementation may require several years to get through budget cycles, procurement, installation and implementation. R6 - The standard should make clear the auditor is not to audit the security plan for its content or appropriateness, but to confirm a security plan has been developed and that particular

security plan has been reviewed by a qualified entity. It should also be clear that a TO could expand its actual security beyond that identified in the approved/reviewed plan without requiring an additional review of such modification. Example: The original, approved plan had card readers on the doors and cameras within the yard. During the 30 months until the next required review, the TO added motion detectors as additional security measures at the substation even though they were not required in the initial security plan. The installation of additional monitoring or security measures beyond those in the approved plan should not initiate the need for a new security plan or third party review.
Yes
Definitions: primary control center - although not capitalized and therefore not a defined term, it is used in this standard in requirements 1, 3, 4, 5, and 6. The same term "primary control center" (again not capitalized) is used with a completely different meaning in standards EOP-008 in requirements 1.3, 1.5, 1.6, 2, 3, 4 and 7.1. Similarly "primary control room" is used in EOP-005 requirement 5 and in EOP-006 requirement 6 and is defined as the control center from which a TOP normally operates as opposed to the backup center. In CIP-014, it is defined/implied to be the control center that actually controls the circuit breakers at two or more substations. • If the term “primary control center” is used there will be confusion over the different meanings within the NERC Reliability Standards. • A completely different term should be used such as “primary local control center” or “primary transmission operations center”. The SDT apparently meant a "facility that has direct Supervisory Control". The term should be defined completely in the standard and should become a defined term within the Glossary of Terms used in NERC Reliability Standards. Proposed defined term: Primary Transmission Operations Center - One or more Transmission Owner or Transmission Operator facilities hosting operations personnel having primary operational real-time control of the BES elements in one or more remotely located substations using SCADA, EMS or other electronic means.” Please clarify whether these security plans are also required at any backup control center. Many of these control centers are generally not manned on a 24 by basis. unaffiliated - should be either defined or a footnote needs to be added to the Standard to explain that unaffiliated - means the selected verifying or reviewing entity cannot be a corporate affiliate, as stated in the guidance document. • Would two entities that do not have a direct ownership stake in each other but both are parties to an ownership in a third organization be considered to be unaffiliated? Example: Two utilities each have an ownership of a joint power plant but no ownership of each other. • What if they both had no ownership of the third party but both had purchase contracts with a third party? An explanation needs to be in the standard and not in the separate guidance document.
Individual
Michael P Moltane
ITC
Yes
ITC agrees with utilizing, as a starting point, the CIP-002-5.1 “medium impact” rating to determine the facilities needing enhanced physical security. As ITC indicated in its comments

to FERC in Docket No. RD14-6, these new physical security Standards must be developed in a coordinated manner to avoid duplicative, overlapping, or contradictory requirements among the various existing Reliability Standards that cover a similar if not an identical set of assets. By ensuring “that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1,” the SDT has fully met our expectations with respect to the applicability of the standard.
No
ITC believes that limiting physical security requirements in CIP-014-1 to those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection does not adequately raise the bar for critical infrastructure protection of valuable and strategic substation assets. Indeed, those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection certainly warrant additional physical protection. However, so does any other substation asset deemed critical through the cybersecurity initiatives already in place through applicable companion Reliability Standards. If a substation is deemed critical through the CIP-002-5 screening process, it at a minimum, should warrant an “evaluation of potential threats and vulnerabilities of a physical attack to the facilities (CIP-014-1 R4). ITC supports using the brightline test criteria of CIP-002-5, as noted in our comments for Question 1, above, but also feels that all substation assets passing the brightline test criteria should move directly to R4 for an assessment of threats and vulnerabilities, eliminating the need for R1 and R2. This has the benefit of using industry-vetted, bright-line criteria that creates valuable consistency between physical and cybersecurity assessment practices. This does not undermine the Commission’s three-part requirement for addressing physical security, but rather allows the responsible entity to meet the Commission’s first requirement (identification of critical assets) by using the same critical asset identification criteria for physical and cybersecurity. ITC believes if a facility is critical enough to warrant cybersecurity protection, then it should also warrant physical security and that the requirements should not be so narrowly defined to ignore the importance of substations beyond those few whose individual loss causes cascading outages. This simplified approach avoids potential contradictory and duplicative requirements between existing CIP standards, and would allow this standard to focus exclusively on physical security aspects and not on asset identification
Yes
Yes
Transmission systems tend to have facilities for which inoperability, while not causing immediate system failure or separation, would nonetheless leave the system in a degraded state. This degraded state will require system operators to reconfigure the system in a way to mitigate the loss of such facilities, but at that point, a new group of facilities could effectively become “critical” as that term is currently defined in CIP-014-1. For example, the loss of a given substation may cause several transformers to be inoperable, and with the long lead time for replacement components, the transmission owner would realistically need to plan for

the substation to be out of service for an extended period of time. During this time in which the substation is out of service, a second tier of assets may exist for which inoperability would now cause separation or failure of the type that would afford them a “critical” designation as currently defined under CIP-014-1. This condition would persist for as long as the original equipment was out of service. If the SDT were to adopt ITC’s proposed modifications to R1 (see above), this would not be an issue, since all CIP-002-5 substations would already be covered by CIP-014-1. However, if the SDT chooses not to adopt ITC’s proposal, the SDT should consider whether entities should assess the transmission system in this new degraded condition to determine if new critical assets are created due to the degraded condition (i.e., a reapplication of the analysis performed in the current R1 to determine if the loss of a particular substation causes widespread cascading.) The Standard could also trigger additional transmission system studies to determine if the transmission system remains reliable during the extended period in which the critical assets remain out of service.
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
Yes
These comments are submitted on behalf of the following PPL NERC Registered Affiliates: Louisville Gas and Electric Company and Kentucky Utilities Company; PPL Electric Utilities Corporation, PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP. The PPL NERC Registered Affiliates support the draft standard. As members of EEI, we also support the comments being submitted by EEI. In addition, we have provided specific comments that we believe would add clarity to the standards and simplify the requirements. We urge the SDT to consider our comments and incorporate them as appropriate when developing the final standard that will be balloted. Comments: Section 4.1.1.2 includes in the applicability Transmission Owners that own Transmission Facilities that are operating between 200kV and 499 kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other Transmission stations or substations and has an “aggregated weighted value” exceeding 3000 according to the table set forth in section 4.1.1.2. Because section 4.1.1.1 covers transmission facilities operated at 500 kV and above and section 4.1.1.2 only references Facilities operating between 200 kV and 499 kV, the fourth row in the table in section 4.1.1.2 referencing voltages of “500kV and above” is unnecessary and should be removed.
Yes
Requirement 1: 1. Requiring completion of an initial risk assessment for Transmission stations and substations planned to be in service within 24 months can lead to audit difficulties. Planned in service dates often change for a variety of internal or external reasons. It is requested that the SDT consider changing this language to a more easily identifiable trigger

such as requiring the risk assessment to be performed before a new Transmission station or substation is energized. 2. Does the R1 risk analysis require consideration of the impact of loss of lines with voltages below 200 kV in an identified Transmission station or substation? 3. It is unclear when the R.1 risk assessment needs to be completed. This should be clarified. 4. The wording in the Rationale for Requirement 1 box identifies the primary control center, but it also notes that control center electronic actions can cause direct physical actions at the Transmission station and substation. This would typically implicate the backup control center as well because the backup control center will have similar functional capabilities. There appears to be a disconnect between the use of the term primary control center and the parenthetical that follows which appears to include any control center that performs the listed functions.
Yes
Requirement 5: In the VSL table, does implemented mean complete execution of the plan including any necessary construction, or does it mean having initiated the plan but not necessarily completed all planned construction? There are only 10 days between VSLs. Requirement 6: 1. Similar to Requirement 2.3, the sub-requirements under Requirement 6.1 should be bullets, not individual sub-requirements. 2. Does R6 require subsequent third-party reviews when the security plan is revised? If so, what are the criteria?
Yes
We recommend that the SDT include a timeline within the standard which includes all required steps.
Individual
Eric Olson
Transmission Agency of Northern California
Agree
American Public Power Association
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Agree
American Public Power Association
Individual
Tony Eddleman
Nebraska Public Power District
No
Due to the imposed time constraints and expedited development of this standard, sufficient time isn't available to develop more realistic criteria for determining applicable substations creating unnecessary work and expense for transmission planners and reviewers.
No

The third party verification is unnecessary and should be deleted from the standard. There is no other unaffiliated third party that has knowledge and expertise comparable with the incumbent Transmission Planner who develops the detailed models, performs the reliability assessments, and develops the required long term plans for the Transmission Owner on an annual basis. If the verification remains in the standard, 90 calendar days is not a sufficient amount of time to complete verification. A Transmission Planner may ask a Planning Authority (PA) to review its risk assessments, but the same PA will likely be asked to review multiple utilities. Recommend at least 180 days to complete the verification.
Yes
Since we are using CIP-002-5 for identifying Transmission stations and substations, the confidential information for these facilities is already protected under CIP-011-1 Information Protection. CIP-014-1, requirements 2.4 and 6.4 are redundant with already approved requirements and are not needed. Adding requirements for protecting sensitive or confidential information in this standard will create confusion and double jeopardy. CIP-006-5 covers physical security and any information pertaining to the substations identified through the CIP-002-5 criteria. CIP-011-1 already protects this information. Due to the expedited development of this standard, sufficient time isn't available to provide clear requirements in the standard to evaluate compliance. The RSAW does contain language that will help, but the RSAW isn't the enforceable document and can be changed without industry approval. We've learned from implementing the other CIP standards that auditors can take a completely different position than what was meant by the drafting team with little recourse for utilities.
Group
GridWise Alliance
Ladeene Freimuth
Yes
Yes
Yes
Yes
GWA includes electric utilities, information and communications technology service and equipment providers, Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs), academic institutions, and energy consulting firms. GWA appreciates the acknowledgment in the Order of the significant efforts that industry already is undertaking to enhance the resilience of the electric grid and thereby protect the grid from a range of threats, including physical, cyber, natural, and other hazards. Industry has been working in close partnership with various levels of government to enhance grid protection, reliability, resilience, and security. This collaboration is ongoing and should be fostered for the

future. As you are aware, the electric grid is dynamic in nature. Electric grid owners and operators are making investments to enhance the reliability and resiliency of the grid, and are actively managing the operation of the grid to prevent outages and to restore power expeditiously, when outages do occur. As this process moves forward, GWA wants to underscore the importance that the result not be overly burdensome or inhibit innovation. It is important that the risk assessment process indeed be limited to truly "critical" infrastructure that is deemed essential to the functioning of the bulk electric system. This will help ensure that protection measures are reasonable and cost-effective, as well as cost-sensitive, to help minimize costs to industry and also to consumers, who ultimately must bear the costs of these investments. Industry is working hard to monitor and stay ahead of the myriad threats that could arise – physical, natural, cyber, and otherwise – recognizing that the types of threats and the motivations of potential actors continue to change over time. NERC should partner with FERC to ensure that an all-hazards approach to addressing risk is undertaken going forward. We appreciate the Order's acknowledgement of the vital need to protect confidential and sensitive information. Yet, we are concerned about the nature of information-sharing under this Order, and what protections and assurances, in fact, would be implemented to prevent the inappropriate sharing of confidential information. While also recognizing the need to protect the confidentiality of such sensitive information, we also note that it is important to ensure that information sharing is facilitated between the government and the private sector, as well as within the private sector. Vendors who supply critical systems and equipment are incorporated into this process, since continued coordination and cooperation among all the stakeholders is essential.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
No
A) The FERC order directs that the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. It does not require verification of the specific or particular facilities identified. Therefore, SCE&G believes this section should be clarified and specifically state that the assessment itself (i.e. the methodology used by the owner or operator) be verified and not the facilities. B) SCE&G would like the drafting team to comment on the liabilities a NERC registered entity may assume as the third party when they are used to verify the risk assessment. Specifically, if in a future audit the owner or operator's assessment is found noncompliant, then would the independent NERC registered third party entity suffer any noncompliance as well? It is important for NERC registered entities to understand their compliance risks as third parties before they agree to perform independent verification of other entities assessments.
Yes

Yes
The requirement for unaffiliated third party verification throughout this standard is not consistent with other NERC Reliability Standard verification requirements. SCE&G is concerned that this standard sets precedence for future standard third party verification which would be very costly, confusing and burdensome.
Group
SERC CIPC
Cynthia Hill-Watson
Yes
Recommend that the drafting team include the Transmission Planner who would be performing the risk assessment in the applicability as discussed in R1.
No
Recommend that the Transmission Planner perform the risk assessment in R1 instead of the Transmission Owner. Need further clarification and examples for the term “unaffiliated”. Would “peer” reviews studies that do not have a single registered entity with controlling interest suffice as an “unaffiliated” third party reviewer? What role does the SDT envision the ERO (including regional entities) playing in the review process?
No
Recommend adding electric utility experience to 6.1.3 and 6.1.4. Consider removing the requirement for CPP and PSP certifications. Rationale: Numerous other mandatory enforceable standards (e.g. MTSA, CFATS, and CT-PATS) that do not require specific certifications nor are we aware of similar certifications in cyber elsewhere in the CIP standards. Suggest clarification of “electric utility experience” and “physical security experience” to allow the ERO and registered entities to justifiably select authorized third party reviewers.
Yes
Until the process of the standards has more fully matured there should not be a presecribed methodology for conducting the Security Vulnerability Assesments (SVAs) as long as generally accepted criteria as well as as stated in the standard in 4.1, 4.2, and 4.3 are followed in the development of the evaluation and plan(s). The comments expressed herein represent a consensus of the views of the above named members of the SERC CIPC only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Individual
William Temple
Northeast Utilities
Yes
Standard Drafting Team should define the term widespread. NU suggests the following definition: Widespread – An event that causes voltage collapse, Cascading and/or instability

that results in uncontrolled separation across significant portions of the Interconnection. The registered entity shall use regional criteria to evaluate.
Yes
Requirement 1 should match that language in the FERC order and not limit the assessment to Transmission System analysis and allow for an opportunity to apply technical expertise and judgment prior to the Transmission System analysis. We agree to Requirement 2 and Requirement 3.
Yes
Suggest standard allow entities to have a Master Physical Security Plan and that the standard provide for flexibility to accomplish mitigation activities associated with the results of vulnerability assessments and capture those under a separate mitigation plan (similar to the action plans associated to vulnerability assessments being conducted on Cyber Assets).
No
Group
Foundation for Resilient Societies
William R. Harris
No
1. Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 — "System Restoration Coordination"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 — "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 — "Notifications and Information Exchange Between Reliability Coordinators." The Joint U.S.-Canada report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded these findings in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.- Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force

Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf> 2. Balancing Authorities would be exempted under the standard. According to the NERC Compliance Registry, there are 19 Balancing Authorities that are not also Transmission Operators or Owners. The following standards apply to Balancing Authorities but not to Transmission Operators or Owners: Standard BAL-001-2 — "Real Power Balancing Control Performance"; Standard BAL-002-1 — "Disturbance Control Performance"; Standard BAL-003-1 — "Frequency Response and Frequency Bias Setting"; Standard BAL-004-0 — "Time Error Correction"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies"; Standard IRO-006-5 — "Reliability Coordination — Transmission Loading Relief". If critical substations and their Balancing Authorities are attacked in a coordinated manner, what entity will balance demand and generation and manage the emergency, especially if the attack causes a regional load imbalance? 3. Generator Operators would be exempted under the proposed standard. Generator Operators have vulnerable and hard-to-replace Generator Step Up (GSU) Transformers, just as Transmission Operators have these transformers. Generation facilities could present contingencies in excess of spinning reserves, especially in congested areas with import of large megawatts of power over long transmission lines. Hence, Generator Operators should be included in mandatory physical security protection standards. 4. The standard does not require modeled contingency planning for scenarios of physical attack. Contingency planning for physical attack should include megawatt capacity of all generators at single generation facility, not just failure of some individual units at the facility. 5. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard. Physical attack of multiple transformers is different than the random failures planned for under the standard N-1 criterion. We have already seen attack on multiple transformers and their circuits at the Metcalf substation. The standard's criterion for violation of IROL limits would not be valid if the IROL limits assume random failures rather than coordinated physical attack. 6. Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, MISO, and SPP. In all, these control centers manage power for 141 million Americans. Control centers for Reliability Coordinators, Balancing Authorities, and Generator Operators are included in the "High Impact" Criteria for CIP-002-5.1 How can the standard drafting team take the CIP-002-5.1 criteria for substations but not control centers of Reliability Coordinators, Balancing Authorities, and Generator Operators? FERC Directive RD14-6-000 specifically requires protection of critical control centers in Footnote 6: "… the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers." 7. While FERC Directive RD14-6-000 [146 FERC ¶61,166] did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Such measures might include: Opaque Fencing; Concrete Jersey Barriers; Motion Sensors; License Plate Scanners; Intentional Electromagnetic Interference (IEMI) Detectors; Gunfire Locators; Limiting of Close Public Access, Including Recreational Access; Armed Private Guards; Police Details; Deployment of National Guard

Troops; Better Stocking of Spares—e.g., Transformer Bushings and Radiators; Equipment Monitoring and Redundant Telemetry to Control Centers. Instead, the standard relies upon self-devised security measures without prioritization or other guidance. 8. The Metcalf incident unambiguously showed the value of equipment monitoring in mitigating physical attack on power transformers. Gunfire locators, had they been installed at Metcalf, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement. Intentional Electromagnetic Interference (IEMI) Detectors could likewise provide real-time warning. If threat sensors with reliable and cyber-protected alerts are not part of a physical security system, it will be impossible to mobilize time-urgent countermeasures and impractical to take precautionary measures at other at-risk facilities vulnerable to coordinated attack. 9. Intentional Electromagnetic Interference should be a physical threat included in the standard, because IEMI attack could occur in the physical proximity of facilities and could cause permanent physical damage in additional to temporary upset. IEMI detectors are a cost-effective measure as these devices cost approximately $15,000 per unit. 10. The Metcalf Incident was both a physical attack and a cyber denial-of-service attack. The need for linkage between physical and cyber is explicitly called for in the RD14-6-000 Order of March 7, 2014, para 5, footnote 3. The implementation plan under this Order must require responsible entities to identify and protect cyber assets that link facilities and control centers that are otherwise identified as critical to the reliability of the BES. Communications and Network entities routinely provide hardened and alternate routing for military, other government and the Defense Industrial Base and their services should be an explicit requirement for Physical Security Standards that apply to any units and control centers that are identified by Responsible Entities as critical to the Reliability of the BES. 11. Review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans. 12. Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP—an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked. 13. RD14-6-000 directs NERC to submit for approval a physical security standard that would apply to the most critical facilities of the Bulk Electric System. The Standard Drafting Team has narrowly interpreted “critical facilities” to mean transmission facilities and directly linked control centers. We disagree with this narrow interpretation. Given the NERC interpretation and the 90 day deadline for standard development, NERC’s draft standard holds tightly to the most minimal facilities and therefore has significant gaps in protection as we describe in our foregoing comments. Some of these gaps, such as the exemption of Reliability Coordinators

and Balancing Authorities, are so fundamental that they should be addressed immediately. For other gaps, we ask that NERC open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of BES operations sufficient to ensure identification of facilities that could cause cascading outage, single points of failure, data connectivity needs, and other processes and technologies essential to grid protection—in short, a standard designated CIP-014 Version 2. An approved SAR for a Phase Two standard should be concurrent with NERC Board of Trustees approval of the current standard in development.
No
Same answer as provided to Question 1.
No
The third party review is not adequately specified. The Joint U.S.-Canada Outage Tasf Force Report (April 2004) determined that lack of Reliability Coordinator oversight, and legal authority, contributed to inadequate supervision of transmission operators, and reduced visibility of regional inadequacies. See our comment to Question 1 for our view that Reliability Coordinators and Balancing Authorities must be involved.
Yes
We recognize that FERC has established a 90-day review process, and that NERC has worked to meet the tight deadline. Hence, the Foundation for Resilient Societies asks NERC to develop a SAR for Physical Security Standards - Phase 2. In this process, analytical modeling should be undertaken to identify and prioritize physical security risks that include cyber vulnerabilities, and that relate to the need for reliable warning and communications via redundant channels to control centers and to law enforcement. It should not be acceptable to exclude Regional Coordinators and Balancing Authorities, both groups needing to review and perhaps upgrade their own physical security, and both groups playing key roles in oversight of the operating entities, both TOs and GOs, whose physical security may be essential to prevent long-term outages through coordinated attacks. For additional materials prepared by the Foundation for Resilient Societies, contact the FERC staff designated to assist NERC with standard setting in FERC Docket RD14-6-000.
Individual
Guy Andrews
Georgia System Operations Corporation
No
Georgia System Operations Corporation (GSOC) appreciates all the effort going into the draft of CIP-014-1 Physical Security Reliability Standard. GSOC supports the comments submitted by NRECA.
No
GSOC supports the comments submitted by both Georgia Transmission Corporation (GTC) and NRECA
No

• GSOC supports the comments submitted by both GTC and NRECA. • In addition, GSOC suggests in R4.2 changing “Prior history or attacks on” to Prior history of physical security related events at” to better describe the subrequirement. • GSOC suggests in R6, last sentence, changing the word “development” to “developed” in order to be consistent with the word “performed” in the same sentence.
Yes
GSOC supports the comments submitted by NRECA
Individual
David Godfrey
Texas Municipal Power Agency
Agree
City of Garland and American Public Power Assocation
Group
Bureau of Reclamation
Erika Doot
No
The Bureau of Reclamation (Reclamation) believes that the Transmission Planner, Planning Coordinator, and Reliability Coordinator should be included in the Applicability section of the standard and should be responsible for reviewing the Transmission Owner’s risk assessment (BES impact assessment).
No
Reclamation agrees with this approach. However, to promote consistent identification of critical facilities within an interconnection, Reclamation believes that the third-party review should be conducted by the Transmission Owner (TO)’s Planning Coordinator or Transmission Planner. If the Transmission Owner is also the Transmission Planner and Planning Coordinator, the third-party review should be performed by the Reliability Coordinator. Reclamation also suggests that the drafting team modify the term “risk assessment” to “BES impact assessment.” In the physical security community, the term “risk assessment” generally refers to “The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.” See ASIS International, General Security Risk Assesment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term “BES impact assessment” so it is clear that the initial evaluation is of risk to the BES if the substation is rendered inoperable or damaged. Reclamation also recommends revising R1.1 to require subsequent risk assessments every 60 months for all Transmission Owners. Reclamation believes that periodic risk assessments are necessary, but has not seen evidence that the costs associated with updating risk assessments every 30 months rather than every 60 months would provide commensurate reliability benefits. Reclamation recommends that the drafting team update R1.1 to state, “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged

could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.”
No
Reclamation agrees with the requirements to develop a threat assessment and physical security plan. Reclamation also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers. However, Reclamation does not believe that the proposed requirements will allow adequate time for a comprehensive review. Reclamation suggests that at least 180 days would be a more appropriate timeframe for a detailed threat analysis and physical security plan review. Reclamation also requests that the drafting team clarify the scope of third party reviews of these threat assesments and physical security plans, perhaps by adding additional detail to the Guidance and Technical Basis section. Reclamation is not convinced that third-party reviews will increase reliability. Reclamation believes that each entity is in the best position to evaultate threats to its facilities and determine appropriate mitigation plans. Reclamation is concerned that the well-intentioned third-party review mandated by the order could result in classified or national security related information falling into the wrong hands. Reclamation does not believe that non-disclosure agreements will adequately protect this sensitive information.Reclamation believes that audits by regional entities in essence provide a “third-party” review of an entity’s threat assessments and physical security plans.
Yes
Reclamation is concerned that the term “primary control center” will become confused with the NERC Glossary term “Control Center.” As indicated by the use of the term “monitor” in the definition of Control Center, Reclamation does not believe that the concept of “operational control” has been equated with “causing direct physical action” to date. To avoid confusion, Reclamation suggests that the drafting team replace the R1 phrase “primary control center that operationally controls eachTransmission station or Transmission substation” with the phrase “primary control center that physically controls each Transmission station or Transmission substation.”
Individual
David Revill
Georgia Transmission Corporation
No
Georgia Transmission Corporation (GTC) supports the efforts of the drafting team and believes that their efforts to create the CIP-014 Standard are moving in the right direction. GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.
No
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. -GTC is concerned that the language of the standard and rationale around the use of the term “unaffiliated” in R2 and R6 does not

provide sufficient clarity for a registered entity to have confidence in the consistent applicability and auditability of the requirement. GTC suggests additional examples or requirement language to consider whether: -entities that are not under the same corporate parent but which have contractual obligations between each other would be considered “unaffiliated” - organizations or teams made up of representatives of multiple utilities with no one utility having a controlling interest in the findings of the group would be considered “unaffiliated”
No
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. - GTC requests revision to the requirement language or addition of guidance around the phrasing of “unique characteristics” in R4 to address whether all equipment within an identified substation has to be assessed in R4 or if an entity has the option to focus their threat and vulnerability assessment on specific facilities in the substation which were identified as causing the adverse effects described in R1. -GTC is concerned that the language of the standard and rationale around the use of the term “unaffiliated” in R2 and R6 does not provide sufficient clarity for a registered entity to have confidence in the consistent applicability and auditability of the requirement. GTC suggests additional examples or requirement language to consider whether: -entities that are not under the same corporate parent but which have contractual obligations between each other would be considered “unaffiliated” - organizations or teams made up of representatives of multiple utilities with no one utility having a controlling interest in the findings of the group would be considered “unaffiliated”
Yes
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. -GTC suggests that in M2 the word “communications” be changed to “notifications” to follow the language of the requirement. -GTC suggests that in M2 and M6 the measures should be updated to include evidence of the qualifications and independence of the respective review teams. -GTC suggests that M6 the measures should be updated to include evidence of the implementation of procedures for information protection used during the third-party review.
Individual
Scott Langston
City of Tallahassee
Agree
APPA
Individual
Bernard Johnson
Oglethorpe Power Corporation
Agree
Georgia Transmission Corporation (GTC) National Rural Electric Cooperative Association (NRECA)

Group
National Grid
Michael Jones
Yes
It should be clear that the applicability section of the standard is only intended to provide a valid, technically sound basis to be used as the ‘starting point’ to those transmission facilities or stations that should be included in the risk assessment. We suggest the following modifications: 4.0 Applicability: 4.1 Functional Entities: 4.1.1 Transmission Owner that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard. Should the risk assessment identify critical assets then the Transmission Owner is subject to the remaining requirements (R3 through R6) of the standard. 4.1.2 Transmission Operator
No
While we support using the CIP-002-5.1 criteria as a starting point for applicability of the draft standard, we do have concerns with the inclusion of the phrase “within an Interconnection” in R1. FERC Order RD14-6 directs that "[a] critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System". By introducing the word “within,” the Standard could inadvertently draw widely different interpretations of how to assess risks to the BPS. In practice, this could open up the potential for the inclusion of regional or localized transmission impacts, which we believe is in contrast with the Commission intended scope in the Order. As a result, we suggest that the wording in R1 be modified to the following: “A critical facility is one that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation or cascading failures widespread across significant portions of an Interconnection". Alternatively, we recommend clarifying in the guidance documents that ‘widespread’ and ‘within an Interconnection’ proposed words are intended to apply to impacts to the BPS that reaches deep into the Interconnection, and not affecting a small portion of an Interconnection. For example, if an Interconnection has relatively small Balancing Authorities (BAs), ‘widespread’ would need to be interpreted as impacts that would be crossing several, i.e. more than two, of those BAs in order to be considered ‘widespread’.
Yes
No
Individual
Donna Johnson
Oglethorpe Power Corporation
Agree

Georgia Transmission Corporation (GTC) National Rural Electric Cooperative Association (NRECA)
Individual
Joshua Andersen
Salt River Project
Yes
SRP supports comments submitted by APPA.
No
SRP supports comments submitted by APPA with the following additions: The time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. If possible, could the drafting team revise the language of Requirement R1 to make this clear? The periodicity of the risk assessments required by Requirement 1 and the time frame that the risk assessments appear to not align. The risk assessment is required to include Transmission stations and Transmission substations that exist as well as those planned to be in service within 24 months. However, the periodicity for conducting future risk assessments is every 30 calendar months or every 60 calendar months if the prior risk assessment did not identify any Transmission stations or Transmission substations. This potentially leaves a gap of six to 36 months where facilities may not have been assessed. In R2 it is not clear that the primary control center must also be verified, but in subsequent requirements it implies or states that it should be. If the intent in R2 is that the primary control center should also be verified, then it should state so in R2.2 and R2.3 in addition to stating stations and substations. Third Party Verifiers: SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated

with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
No
SRP supports comments submitted by APPA with the following additions: Third Party Verifiers: SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different

in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Yes
Section C “Compliance” 1.4 (page 13) which states “...all evidence will be retained at the TO and TOP facilities.” is contradictory with NERC Compliance Monitoring and Enforcement practices which allow data to be exchanged with and sent to Regional Entities such as in pre-Audit data requests and Mitigation Plans. In addition, this would be burdensome for the TO/TOP because the 3rd party verifying/reviewing entities would need to be on-site and potentially incur travel expense.
Individual
Patrick Farrell
Southern California Edison Company
Yes
No
SCE has concerns with both Requirement R1 and Requirement R3. In Requirement R1, SCE recommends that the verbiage be changed from “…that if rendered inoperable or damaged could result in widespread instability...” to “...that if damaged to the point of being rendered inoperable could result in widespread instability..." SCE requests this change to reduce ambiguity in the application of the word "damaged." In addition, language should be added to R1 that specifies: “…system instability such as uncontrolled separation or cascading within 15 minutes of compromise…,” as a 15-minute window would align with criteria in the CIP standards used to determine critical facilities. In the guidance section for R1, SCE would suggest changing the text from “…remedial action schemes (RAS) or special protection

systems (SPS)" to "…special protection systems (SPS)…," because as used in the NERC Glossary of Terms, a RAS is included as a type of SPS. In addition, SCE requests that R1 be revised to include specific examples and criteria for the risks to be measured. For instance, SCE believes the following could be among the examples and criteria specifically included: (a) Thermal overloads beyond facility emergency ratings; (b) Voltage deviation exceeding ± 10%; (c) Cascading outage/Voltage collapse; and (d) Frequency below under-frequency load shed points. With respect to Requirement R3, SCE requests that additional guidance be provided on how a "primary control center" should be identified, as that term in used in both Requirements R1.2 and R3. SCE also asks the team to consider changing the notification requirement in R3 from seven(7) to thirty(30) days in order to allow sufficient time for the transmission owner and transmission operator to perform the required communication.
No
SCE has concerns with Requirements R4, R5, and R6 that will be described below. With respect to Requirement R4, SCE notes that entities are required to "…conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)…" SCE requests the inclusion of additional guidance or examples of threats and potential vulnerabilities that an entity may want to consider. This will allow entities to perform a threat assessment and develop preventative measures that are commensurate with the intent of the standard. In addition, SCE requests additional guidance on physical security plans that allow for flexibility to deal with emergent threats. With respect to Requirement R5, SCE believes that in the guidance section, the drafting team should consider referencing standards that are used by security professionals or organizations, in order to ensure that the criteria to identify appropriate countermeasures to potential threats and physical attacks are evaluated along similar themes across industry. SCE also requests that the team consider rephrasing R5.1 from "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond…" to describe the control, to "…deter, detect and delay, and also assess, communicate, and respond…" With respect to Requirement R6, SCE requests that the team consider rewording Requirement R6.1 from "Each Transmission Owner and Transmission Operator…" to "Each Transmission Owner or Transmission Operator, with facilities identified as a result of R2,…"
No
Individual
John Hagen
Pacific Gas and Electric Company
Yes
Yes

R2 Comment: Suggest removal of the requirement for a third party risk assessment verification. Verifications already occur as part of internal compliance programs in CIP-002 and when audited by the Region. What if the assessment is performed by a third party, do you have to get another third party to verify? This creates a significant administrative burden, even if the Standard will only apply to a small number of entities and facilities. R3 (pg. 8) "…the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify…" Comment: Seven calendar days may be too short a time requirement, consider 10-14 days
Yes
R4 (pg. 9) "…shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)…" Comment: Consider stating "…conduct a physical security risk assessment to identify and evaluate potential threats and vulnerabilities…" The assessment should identify the potential threats and vulnerabilities to evaluate and implement the necessary protective, detective and corrective countermeasures R5 (pg. 10) states to develop and implement a documented security plan (s) within 120 calendar days of completion of R2 (unaffiliated third party verify the risk assessment form R1). Furthermore, R5.1 states to address the potential threats and vulnerabilities from R4. 120 days to implement the countermeasures may not be enough time (logistics, procurement, installation timelines, approvals, etc.). Comment: Could they say "…shall develop and begin implementation of a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days…" because in R5.3 it requires a timeline for implementing the enhancements. 6.1.1. (pg.11) "An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification." Comment: Shouldn't require a specific certification, should say something like "The third party must include in their review the qualifications of the staff performing the review." R6.1.2 (pg. 11) "An entity or organization approved by the ERO." Comment: What criteria is the ERO using to approve entities or organizations? The approval process needs to be spelled out. R6.1.3 (pg. 11) "An entity or organization with demonstrated law enforcement, government, or military physical security expertise" Comment: Does this mean we can use Law Enforcement agencies or firms with retired law enforcement personnel?
Yes
Compliance 1.2 (pg. 13) Comment: can they clarify by being less wordy and just start by saying "The responsible entities shall retain documentation as evidence for three years", followed by the rest in less words?
Group
ISO/RTO Standards Review Committee
Greg Campoli
Yes

Introduction The proposed standard provides adequate flexibility with respect to the risk assessments and security evaluations and plans. This allows the industry to capitalize on their experience in these matters, while also accommodating changes that warrant consideration. Applicability Section The applicability scope is reasonable in terms of identifying the appropriate functional entities to address physical security concerns. Similarly, the proposed standard establishes a reasonable approach for identifying the scope of facilities by 1) initially defining an objective set based on the CIP-002-5.1 criteria, and then 2) refining that set based on analyses that assess the relationship of those facilities to specific, system conditions/impacts metrics – i.e. widespread instability, uncontrolled separation, or Cascading within an Interconnection.
Yes
R1 R1 in conjunctions with the Applicability section is a reasonable approach for identifying the scope of facilities subject to R2 – R6. R2 Imposing a verification requirement is a reasonable way to facilitate an effective outcome in terms of identifying facilities that meet the impact thresholds established in R1. Requiring the use of an unaffiliated third party is reasonable because it mitigates the potential for inadvertent error in study work. Finally, allowing the verification to occur concurrently or subsequently, and leaving that decision to the discretion of the relevant functional entities, is appropriate. The functional entities should have the discretion to determine the most effective means of performing the verification. R2.1 requires that the verifying entity be either 1) a registered RC, PC or TP, or 2) another entity with appropriate planning or analysis experience. This is a reasonable approach that provides appropriate flexibility with respect to third party verification options. It also addresses the different operational and planning structures that comprise the North American electric grid – i.e. organized market regions where different entities can perform the different NERC registered functional roles (ISOs/RTOs) and vertically integrated regions where all the relevant roles under the standard may be performed by a single entity and, therefore, would require the use of an independent third party to perform the unaffiliated verification. R2.2 requires the third party verification to either confirm the TO analysis under R1, or, alternatively, recommend that facilities be added or deleted (the IRC assumes that a verification can confirm some results and also add facilties or remove facilities). Although R2.2 establishes a reasonable standard – i.e. verify TO results or recommend changes - the IRC offers the following comments. The requirement, as written, imposes the obligation on the third party verifying entity. However, the TO is the responsible entity under the standard – i.e. the TO is required to obtain the third party verification. The language should be revised to clarify that the relevant actionable obligation (to obtain the third party verification) lies with the TO. The next issue raised by R2.2 is the timing. The IRC appreciates the importance of the issues being addressed by the proposed standard and the goal of implementing the standard and the relevant processes contained therein in a timely fashion. However, practically speaking, 90 days may be difficult to meet depending on the number of Transmission Owners that require verification from a single Registered Entity. For example, in organized markets there may be numerous TOs all selecting their PC to verify. To the extent implicated in reviews under the standard, IRC members would make best efforts to perform any relevant verifications. This comment is merely intended to highlight the potential resource impacts

under the proposed 90 day timeline. The IRC proposes the following revisions to mitigate the issues in R2.2 described above. 2.2. The third party verification shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within a mutually agreed upon timeframe between the Transmission Owner and the third party but no longer than 180 calendar days following the completion of the Requirement R1 risk assessment. R3 R3 obligates the TO to notify a TOP that has operational control of a control center associated with a facility identified pursuant R1 and verified under R2. R3.1 requires similar notification if a facility is removed via those processes. The standard may benefit from including the draft guidance into the R3 rationale section that clarifies that operational control means the ability to take action that affects the physical status of the facility, and that it does not include directive control, which relies upon another entity to take operational action to change the status of the facility. The guidance document addresses this issue, but the SDT could add clarifying language to the rationale section of R3, similar to the language in the guidance document and/or the language in the R1 rationale section, which reads in relevant part: "… identify the primary control center that operationally controls that Transmission station or Transmission substation (i.e., the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity)."
The IRC has no comments on R4-R6.
No
Group
APPA
Paul Haase
Agree
The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities, physical infrastructure, including risk assessments

and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language (new subrequirements): R1 1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3 3.4 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under Requirement R1 of this standard. R4 4.1 The Transmission Owner will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 conducted under this standard.
Individual
David Francis
MISO
Yes
MISO supports the proposed applicability section and agrees that other entities do not need to be included. In particular, MISO would not support application of this Standard to Reliability Coordinators or Balancing Authorities, as these entities' control centers are adequately protected with regard to physicial security under CIP-006-3c and its successor standard. Moreover, these control centers are subject to the requirements of EOP-008-1 including the transfer functional control to backup facilities. MISO therefore agrees that the focus of CIP-014-1 should be those facilities that are not otherwise fully protected by CIP-006-3c, such as those that do not not rely entirely on Critical Cyber Assets to maintain reliability.
No
MISO recognizes that the Commission mandated third-party verification of the risk assessment required under R1, however the current language of R2 requires modification to address several concerns MISO has with regard to its potential role as a verifying entity. While MISO has every confidence that it can perform risk assessment verifications in a safe, responsible, and accurate manner, the combination of a high number of requests requiring

verification within a relatively short period of time presents some concerns to MISO regarding its resource allocation and availability. In particular, MISO recommends that the SDT add language limiting the universe of Transmission Owners/Operators that can seek verification from a particular verifying entity (potentially by geographical region or contractual or functional relationship) as well as modify the 90 day requirement to take into account that a single entity may have more requests than it can feasibly complete in such a short time period. An example of language that MISO could support is language that would allow a verifying entity and the requesting Transmission Owners/Operators to agree upon an appropriate completion date beyond the 90 days where the 90 day period will not allow completion of a robust verification due to resource constraints by the berifying entity. Finally, MISO respectfully requests that the SDT consider adding language to Requirement R2 that would allow verifying entities to limit liability related to both enforcement actions within the jurisdiction of FERC, NERC, and the Regional Entities and other actions that could be brought against verifying entities in other jurisdictions and venues unless it is shown that the entity lacked good faith or was grossly negligent.
Yes
No
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
No
The drafting team may want to consider language referencing the CIP-002 Critereon rather than outright copying it in order to prevent changing multiple standards as the CIP-002 standard evolves. CIP-002-5.1 Attachment 1: Overall Application gave guidance on how to treat joint ownership facilities. Tri-State feels that this new standard would also benefit from such guidance.
No
Rather than making it the Responsible Entity’s responsibility to find a third party to verify its assessment, Tri-State believes it would better suit the industry and the standard if R2 required either the Reliability Coordinator or Regional Entity to request TO's assessments on an intervaled basis. This meets the requirements of the March 7 FERC Order. Allowing the requirement to be broad enough to allow third party paid consultants with “transmission planning or analysis experience” creates a conflict of interest and contradicts the draft standard’s requirements for the use of “unaffiliated third part[ies]”. If third party – other than NERC or the RE – verification of the assessment is required by the standard, then this is effectively two audits (and two 3rd party assessments) on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the

standard is currently drafted. Tri-State recommends that rather than 30 months and 60 month risk assessment intervals for R1.1, they should be a more straightforward 36 months and 72 months respectfully in order to be consistent withnormal auditing time periods of three years. This will make the intervals easier to track with internal programs and controls.
No
Tri-State disagrees that the FERC order specifically forces the drafting team to have a requirement for 3rd party verification. The order uses the word “should,” not “shall” or “require.” Tri-State would argue that 3rd party verification would/will occur during scheduled audit times. Again if the drafting team feels a need to require an additional 3rd party verification, it should require the Regional Entity or Reliability Coordinator to request the plans.
Yes
While the FERC Order RD14-6 paragraph 13 does require NERC to file a proposed standard within 90 days, footnote 8 only requires that the proposed standard include timelines for certain elements, without specificity for what those timeframes should be. The bright line CIP version 5 applicability that is used within this standard became effective 02-03-14 and was giving industry 24 months to implement. The CIP-014 draft appears to assume those bright line considerations are already completed for industry and provides just over 6 months to complete an additional assessment to remain compliant. Without specific implementation timeframes provided by FERC, and to stay in closer alignment to the expected completion dates for CIP v5, Tri-State is recommending no less than a one year after this standard becomes effective for the R1 risk assessment to be completed.
Group
California Public Utilities Commission: Safety and Enforcenment Division
Raymond G. Fugere
Agree
California Public Utilities Commission Safety and Enforcenment Division
Group
Bonneville Power Administration
Andrea Jessup
Yes
4. Applicability: BPA believes that the medium list for HV transmission entities will result in numerous facilities having to be protected (all 500 kV) contrary to the drafting team comment that not many facilities will be deemed critical. 4.1. Functional Entities: BPA recommends that this section reference the criteria of CIP-002-5.1 for a “medium impact rating,” instead of re-stating it without citation. Otherwise it is confusing. For example, the source of the tabulated weighting criteria is unclear and it is difficult to know there is a connection to any previous or established standards.
No

R1 Terminology: Although the term “risk assessment” in this section is in alignment with language in the FERC order, BPA recommends that it be revised to consequence or impact assessment. This is a physical security standard, and the term risk assessment should be reserved for the physical security risk section of this standard and align with security industry use of the term. BPA believes the basic intent of R1 is to identify substation facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection can create unacceptable consequences to the BES and not to assess risk of the event happening. Also, BPA suggests that additional sub-requirements be added to provide clarity on what system conditions and performance criteria or methodology need to be considered in order to determine what stations and substations will be deemed critical. Similar language found in existing standards would be helpful. Examples: FAC-010-2.1 (System Operating Limits Methodology for the Planning Horizon), R1-R3; FAC-013-2 (Assessment of Transfer Capability in the Near-Term Planning Horizon), R1; TPL-001-4 (Transmission System Planning Performance Requirements), R1-R6; TPL-004-0a (System Performance Following Extreme BES Events), R1. "R1 1.1. Subsequent risk assessments shall be performed:" BPA recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” Justification: This would consolidate the two bulleted actions and make them equally applicable. BPA has been doing substation facility impact and security risk assessments for the past 15 years and our experience is that the criticality of a substation facility does not change once ranked; once it is determined critical it will always be critical particularly when information is used in a physical security risk assessment. A 5 year interval would be a more appropriate interval for this type of assessment as it would always be case of identifying new facilities and not excluding ones previously identified. "R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R2 first sentence to: "R2 Each Transmission Owner shall verify the impact assessment performed under requirement R1 by a third party entity other than the owner or operator." Justification: This fully aligns with the requirements of the FERC order by using the requirements of the FERC order. BPA believes the introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of an impact assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes that the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft “unaffiliated” is especially troublesome for federal government-owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the federal government

transmission owner. Also, BPA believes industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into widespread use. Please note that the FERC order only recommends this verification as it is stated as “should” and not as “shall.” "R.3 For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. [VRF: Lower; Time- Horizon: Long-term Planning]" BPA recommends revising the 7 day requirement in R3 and R3 3.1 to 30 calendar days. Justification: This information is not that time critical at this stage, and one week will not be enough time to complete all notifications.

No

R4. BPA agrees with the requirements to develop a threat assessment and physical security plan. BPA also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers as noted in R6 (Section R6.1.3.) However, BPA requests that the drafting team clarify the scope and purpose of third party reviews should they remain as part of the standard. BPA disagrees that third party reviews will increase reliability and notes the draft standard exceeds the scope of the FERC order Paragraph 11. BPA believes that each entity is in the best position to evaluate threats to its facilities and determine appropriate mitigation plans. Nonetheless if third review is deemed necessary, BPA believes that it should be allowed to have another federal agency perform its third party review. In other words, for purposes of this standard, another federal agency would be deemed to be “unaffiliated” with BPA. Keeping this information within the federal government will decrease the risk of inappropriate disclosure of such information. BPA believes that non-disclosure agreements with non-federal parties may be a poor substitute for this because they can only be enforced once a disclosure is made. At that point, it is often too late and the information is available to a wider audience than intended. "R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator’s primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Time-Horizon: Long-term Planning]" BPA recommends revising the 120 day requirement in R5 to 12 calendar months. Justification: This information is important to get right as security designs and enhancements will be built from this plan. 120 days is not be enough time to develop a complete and effective security plan

and incorporate finalized threat assessments. "R6 Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R6 first sentence to: "R6 Each Transmission Owner shall verify the risk assessment performed under requirement R4 by a third party entity other than the owner or operator." Justification: BPA believes the proposed revision fully aligns with the requirements of the FERC order by using the requirements of the FERC order. The introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of a risk assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft "unaffiliated" is especially troublesome for federal government owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the government transmission owner. Also, industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into wide spread use. Please note that the FERC order only recommends this verification as it is stated as "should" and not as "shall."

Yes

The current draft requiring "unaffiliated" third party review is more restrictive than the requirements language in the FERC order and meeting an unaffiliated requirement will be problematic for federally owned power and transmission systems. Paragraph 8 of the order: "Thus, the Reliability Standards should require the owners or operator to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process." BPA's interpretation of the FERC order is that consultation with peer entities would be acceptable methods for review of evaluation processes. In fact the order by its wording encourages such consultations without restriction as to business or corporate relationships. The draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities

corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The “unaffiliated” requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term “unaffiliated” and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard. Paragraph 11 of the FERC order: “In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity.” BPA believes the draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The “unaffiliated” requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term “unaffiliated” and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.

Group

California Public Utilities Commission: Safety and Enforcenment Division

Raymond Fugere

No comments

In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive. The use of unaffiliated verifying experts is a positive element in the draft standard. In general, the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. With respect to Rule R1, Section 1.1, the drafting group should consider whether there should be language added to the standard detailing a process whereby the 30 or 60 month intervals should be accelerated in the event of serious intervening situations. With respect to Rule R2, Section 2.1, the description of “an entity that has transmission planning or analysis experience” is overly vague and should be further clarified, or that the use of this type of expert should be limited to certain small transmission owners. With respect to Rule R2, section 2.4, the language requiring “non-disclosure” agreements is important and a positive element in the draft standard.

In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive. The use of unaffiliated verifying experts is a positive element in the draft standard. In general, we believe that the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3,

second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. Section 5.1 of the draft refers to “resiliency”. Does this term refers to actions such as building redundancy or improving protective schemes, as opposed to direct physical protection activities? The standard should clarify the meaning of the term resiliency. Section 4.1 of the draft refers to “unique characteristics.” Assuming this consideration includes availability of spares and ease of repair, the language is acceptable. With respect to Rule 5, section 5.2, the drafting group should consider language requiring the security plan to include contact and coordinating information for other utilities or important stakeholders, in addition to law enforcement. With respect to Rule R6, section 6.4 the language requiring “non-disclosure” agreements is important and a positive element in the draft standard. Section 4.2 lists the elements to be considered in evaluating the potential threats and vulnerabilities to physical attack, and specifically states "[p]rior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events and ...". We suggest that in additional to geographic proximity, that the section add language concerning "similarity of geographic characteristics". While geographic proximity, is a factor, ease of accessibility, layout and geographic contour, of an attacked facility is also important, if not more so.
Individual
Glen Sutton
ATCO Electric
Yes
No Comment.
Yes
Although the FERC order contains language that a third party verification occur, this type of verification is not used anywhere else in NERC reliability standards for similar activities (e.g. CIP-002 classification). ATCO Electric (AET)respectfully requests that the review be allowed to be performed by qualified in-house Engineering groups who already perform these functions. Mandating a third party verification presents a risk to timelines and the implementation of the other requirements.
Yes
AET agrees with the flexible approach outlined by the draft standard and respectfully offers these following comment for the drafting team’s consideration: R4 – Please consider altering the wording of the final sentence of R4 to “The evaluation shall consider, at a minimum, the following:”. This allows additional flexibility for entities with existing physical security assessment programs to continue to include those extra elements within their plans. R5 – For the timeframe dependency please consider altering the dependent requirement to R4 instead of R2. Within the rationale section the drafting team concedes that R4 must be completed prior to commencing R5 and the drafting team also states that R4 does not state when the evaluation must occur, only that it must occur in time to meet R5. AET respectfully suggests

that a linear progression be established just as in R1, R2, and R3. This would require a timeline be added to R4 for the completion of the physical security risk assessment (AET suggests 120 calendar days from the completion of R2). AET also respectfully suggests that R5 then be made dependent on the completion of R4 (AET suggest 120 calendar days from the completion of R4). R6 – Please consider the removal of the required certifications in R6.1.1. The FERC order specifies that the risk assessment be reviewed by "[…] or another entity with appropriate expertise" and does not specify any particular qualifications. In addition, no other CIP standard calls for specific certifications or qualifications. Neither engineering focused requirements (e.g. CIP-002) or cyber security focused requirements (e.g. CIP-003, 005, 007) specify that those requirements be reviewed or implemented by designated engineers or certified security practitioners (e.g. CISSP). The due diligence required of the entity will determine the level of rigor that that entity is comfortable with defending and should not be included in the standard.
No
Individual
Richard Vine
California ISO
Agree
ISO/RTO Standards Review Committee
Individual
Mauricio Guardado
Los Angeles Department of Water and Power (LADWP)
Yes
LADWP requests the Drafting Team to make the following changes: - For Secion 4, you may want to add Transmission Planner and Planning Coordinator to the applicability. These functions may have responsibility on at least R1 and R2. - Secion 4.1.1.1 – Add "(AC or DC)" as follows: "Transmission Facilities operated at 500 kV (AC or DC) or higher….."
No
LADWP requests the Drafting Team to make the following changes: - For R1, additional time is needed to make sure studies are fully completed and reviewed by TO and its applicable governing authorities. Add ", which is due 30 calendar days after the effective date of the standard" to R1 as follows: "R1. Each Transmission Owner shall perform an initial risk assessment, which is due 30 calendar days after the effective date of the standard and subsequent risk assessments of its Transmission stations and Transmission substations (existing and……" - For R1, change "24 months" to " 30 months" to align the assessment with subsequent risk assessments. - For R2.1, The term "unaffiliated" needs to be defined in the standard to avoid any misinterpretation. - For R2.2, change the "90 calendar days" to "120 calendar days" to allow sufficient time to resolve differences if Planning Coordinator, Transmission Planner or Reliability Coordinator are addressing other deadlines.

No
LADWP requests the Drafting Team to make the following changes: - For R5, replace the word “implement” with “complete” to avoid confusion as to whether the plan needs to be implemented within the timeline provided - For R5.1, the word “Resiliency” needs to be defined in the standard to avoid any misinterpretation. Resiliency means different things to different people - For R5.1, add the language “, mitigate the impacts of,” to the requirement as follows: “5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, mitigate the impacts of, and respond…..” - For R5.4, change the requirement language to read as follows: “5.4. Provisions to evaluate evolving physical threats to the Transmission station(s), Transmission substation(s), or primary control center(s), and their corresponding security counter measures. “ This sub-requirement should allow for the TO to revise its already-reviewed security plan within the 30-month cycle without necessarily having to make arrangements for a third party review of the revised plan (although it may do so if TO so desires) and without creating an additional 30-month cycle review that the normal course – this is a matter of efficiency and due diligence to address evolving threats - For 6.1, as previously mentioned, the word “unaffiliated” needs to be defined in the standard to avoid any misinterpretation. - For 6.1.3, change the requirement as follows: “6.1.3. A governmental agency with physical security expertise, which could be a City Department in which the utility resides that requires a review to be performed.” This clarification allows for additional flexibility of independent governmental agencies reviews. - For 6.1.4, change the requirement as follows: “6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise, such as the local police department in which the utility resides that requires a review to be performed.” This clarification allows for additional flexibility of independent entities or organizations reviews - For R6, add 6.1.5 with the following language: “6.1.5. A peer utility review group with demonstrated law enforcement, government, or military physical security expertise This clarification allows for additional flexibility of other Planning Coordinator, Transmission Planner or Reliability Coordinator review the work of their peers. In the alternative, expand to include Planning Coordinator, Transmission Planner or Reliability Coordinator with law enforcement, government, or military physical security expertise. - For 6.2, change the “90 calendar days” to “120 calendar days” to provide sufficient time to determine reasonable and sound recommendations. - For 6.3, chance the “90 calendar days” to “120 calendar days” to provide sufficient time to address any modifications recommended.
No
Individual
Laurie Williams
PNM Resources
EEI
No

R2.1 puts an unreasonable burden on registered PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO PNM can't force another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Group
Associated Electric Cooperative, Inc.- JRO00088
David Dockery
Agree
NRECA
Individual
Richard Vine
California ISO
Yes
Yes
We agree with the approach identified in R1 through R3, however we have the following comments regarding the SCOPE of the verification review required by R2.2: • The scope of the 3rd party verification is not well defined. What is the expectation and scope of the verification review? What level of quality is expected/required? Is the Transmission Owner responsible for scoping the verification process to ensure the review meets the required level of review? • Very little guidance is provided on the scope of the review. The scope of the review and verification work would need to be well understood before taking this verification work on. Is a technical analysis required as part of the review and verification process on the part of the 3rd party verifying the Transmission Owner's risk assessment and list of critical facilities, or is it simply to review the risk assessment and list of critical facilities that the Transmission Owner has provided to the 3rd party reviewer, based on their current knowledge of the transmission system from performing prior transmission planning studies? Will NERC be providing additional guidance regarding the scope of work required for verification by a 3rd party?
Yes
No
Group

Cooper Compliance Corp
Mary Jo Cooper
Yes
We support the applicability proposed by CIP-014-1.
No
We do not support the Standard as written today. We agree with the scope and content of the SAR. However, we are concerned with Requirement 6. Requirement 6 requires entities to seek out third parties to review their new physical security protection plans. We don't believe that entities should be obligated to seek assistance from third party individuals. This includes consultants or another unassociated entity. The purpose of the regions, NERC, and FERC are to provide a review of an entities compliance to Standards through the audit and self-certification process. No other Reliability Standards require an entity to use third parties to determine compliance or sufficiency of compliance documentation. We believe that this obligation may place some entities in difficult financial situation and could have a negative impacts in assuring that proper third party entities are being used. Should FERC, NERC, or WECC determine that entities are not following the spirit of the Standard than they may request a modification in a future Standard revision. We will support this Standard if Requirement 6 is removed.
No
We do not support the Standard for the same reason above. We do not support a third party review requirement other than that of the existing Standards. That is a review by FERC, NERC or the appropriate region.
Yes
We would like to address proposed comments by APPA that additional Standards are added to address confidentiality. We do not agree with APPA's position. The functional model requires registered functions to work together to secure reliability. Already, as a result of CIP Standards, vital communications between the Distribution Providers/Load Serving Entities and the Balancing Authorities and/or Transmission Operators have been compromised. Often, The Balancing Authorities and Transmission Operators are in fear of sharing important information with the Distribution Providers and/or Load Serving Entities because they feel they could be subject to a CIP violation. In some cases the Distribution Providers and Transmission Operators even share facilities. Having a requirement that prevents sharing vital information on physical security would simply not work and therefore we do not support APPA's comments.
Individual
Michael Mertz
PNM Resources
Yes
Support the comments submitted by EEI.

No
R2.1 could place an unreasonable burden on entities registered as PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO an entity cannot compel another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Yes
Support the comments submitted by EEI
Yes
Support the comments submitted by EEI
Individual
Jeffrey Fuller
Dayton Power & Light
Agree
Dayton Power & Light

Comments Received from Herb Schrayshuen

Question 1 – Response: No

Comments: The applicability of the standard is to Transmission Owners and Transmission Operators. Generating plants sites where the facilities production capability exceeds 1000 MW or other suitably larger amount should be included.

Question 2 – Response: No

Comments: In Requirement R1 the use of the term ‘transmission analysis’ and ‘transmission analyses’ in order to identify which substations should have a security plan is vague The TPL standards extreme cases should be used to clearly describe the specific required elements of the analysis. Failure to specify how the analysis is to be done will lead to inconsistencies in the analysis and thereby difficulty for audits of the standard.

In Requirement R2 the use of the word ‘unaffiliated’ introduces ambiguity. There needs to be an understanding (through the standard but if not feasible through RSAW or other tool-e.g. guideline) what “unaffiliated” means.

The term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities.

Question 4 – Response: Yes

Comments: The Implementation Plan can be read that it obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. The implementation plan should be adjusted.

The following is a suggestion to facilitate reading of the standard and stay whitn defined terms without introfucing new terms which are undefined: For all requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary.

While the requirement for unaffiliated third party verification of the physical security plan is something required by the FERC in its order, the mandate is misguided and will lead to security breaches while at the same time adding no incremental value to the physical security plan. The utility, which owns the assets, is already highly incentivized to put together a good security plan to avoid loss of its facilities to terrorism without third party verification. The utility may decide to use security consultants to help develop the plan if it involves new, state of the art physical security topics outside the utilities experience base. On balance the third party verification requirement outlined in R6 regarding the physical security plan is unneeded.

Additional comment received from Marcus Pelt, Southern Company

"The wording of Requirement R2.s, as it stands currently, could be interpreted to place requirements on the unaffiliated third party verifier when the responsible entity is actually the Transmission Owner. Southern recommends that R2.2 be reworded as follows to address this concern:

Proposed R2.2
2.2 The responsible Transmission Owner shall ensure the unaffiliated third party verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment. The unaffiliated third party verification may, but is not required to, include recommended additions or deletions of Transmission station(s) or Transmission substation(s)."