Name (48 Responses)
Organization (48 Responses)
Group Name (28 Responses)
Lead Contact (28 Responses)
Question 1 (69 Responses)
Question 1 Comments (76 Responses)
Question 2 (68 Responses)
Question 2 Comments (76 Responses)
Question 3 (69 Responses)
Question 3 Comments (76 Responses)
Question 4 (0 Responses)
Question 4 Comments (76 Responses)

Individual
Bo Jones
Westar Energy
Yes
Yes
Yes
In Requirement 1.3, the statement “and the following as appropriate” is vague and subject to interpretation. Who determines what is appropriate? We feel it would be better if the SDT would specify for each event, which party should be notified.
Group
SERC OC Standards Review Group
Gerald Beckerle
No
We agree with removing the training requirement of R4; however we believe that drills and exercises are also training and R4 should be removed in its entirety because drills and exercises on an after the fact process do not enhance reliability.
No
It is confusing why R3 is not considered part of R2, which deals with implementation of the Operating Plan and it appears that R3 could be interpreted as double jeopardy. We suggest deleting R3.
No
No event should have a reporting time less than at the close of the next business day. Any reporting of an event that requires a less reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity.
We believe that reporting of the events in Attachment 1 has no reliability benefit to the bulk electric system. In addition, Attachment 1, in its current form, is likely to be impossible to implement consistently across North America. A requirement, to be considered a reliability requirement, must be implementable. We suggest that Attachment 1 should be removed. We have a question about what looks like a gap in this standard: Assuming one of the drivers for the standard is to protect against a coordinated physical or cyber attack on the grid, what happens if the attack occurs in 3-4 geographically diverse areas? State or provisional law enforcement officials are not accountable under the standard, so we have no way of knowing if they report the attack to the FBI or the RCMP. Even if one or two of them did, might not the FBI, in different parts of the country, interpret it as vandalism, subject to local jurisdiction? It seems that NERC is the focal point that would have all the reports and, ideally, some knowledge how the pieces fit together. It looks like NERC’s role is to solely pass information on “applicable” events to the FERC. Unless the FERC has a 24x7 role not shown in the standard, should not NERC have some type of assessment responsibility to makes inquiries at the FBI/RCMP on whether they are aware of the potential issue and are working on it? “The comments

expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers.”
Individual
Michael Johnson
APX Power Markets (NCR-11034)
Yes
Yes
Yes
In my opinion the remaining items with 1 hour reporting requirements will in most cases require the input of in-complete information, since you maybe aware of the outage/disturbance, but not aware of any reason for it. If that is acceptable just to get the intitial report that there was an outage/disturbance then we are OK. I believe it would help to have that clarifed in the EOP, or maybe a CAN can be created for that.
For Attachment 1 and the events titled "Unplanned Control Center evacuation" and "Loss of monitoring or all voice communication capabiliy". RC, BA, and TOP are the only listed entity types listed for reporting responsibility. We are a GOP that offers a SCADA service in several regions and those type of events could result in a loss of situational awareness for the regions we provide services. I believe the requirement for reporting should not be limited to Entity Type, but on their impact for situational awareness to the BES based on the amount of generation they control (specific to our case), or other criteria that would be critical to the BES (i.e. voltage, frequency).
Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely “recognition” starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition.
Project 2008-06 proposes to withdraw the terms “Critical Asset” and “Critical Cyber Asset” from the NERC Glossary. In order to avoid a reliability gap when this occurs, we propose including High and Medium Impact BES Cyber Systems and Assets. The revised wording to add, “as appropriate” to R1.3 is a concern. We understand the SDT’s intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. R4 continues to be an onerous requirement for smaller entities. Verification was not part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1. Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3.
Group

Northeast Power Coordinating Council
Guy Zito
No
Requirement R4 is unnecessary. Whether or not the process, plan, procedure, etc. is “verified” is of no consequence. EOP standards are intended to have entities prepare for likely events (restoration/evacuation), and to provide tools for similar unforeseen events (ice storms, tornadoes, earthquakes, etc.). They should not force a script when results are what matters.
No
R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the following as determined by the responsible entity:… Without this change it is not clear who determines what communication level is appropriate. R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following any change in assets or personnel (if the Operating Plan specifies personnel or assets), that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in “assets, personnel…. or incorporating lessons learned”, (or our preceding proposed revision). This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis. The only true requirement that is results-based, not administrative and is actually required to support the Purpose of the Standard is R3.
No
The SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. It is not clear what the difference is between a footnote and “Threshold for Reporting”. All information should be included in the body of the table, there should be no footnotes. Event: Risk to BES equipment should be deleted. This is too vague and subjective. This will result in many “prove the negative” situations. Event: Destruction of BES equipment is also too vague. The footnote refers to equipment being “damaged or destroyed”. There is a major difference between destruction and damage. Event: Damage or Destruction of a Critical Asset or Critical Cyber Asset should be deleted. Disclosure policies regarding sensitive information could limit an entity’s ability to report. Unintentional damage to a CCA does not warrant a report. Event: BES Emergency requiring public appeal for load reduction should be modified to note that this does not apply to routine requests for customer conservation during high load periods.
Requirement 4 does not specifically state the details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit/enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. The standard is too specific, and drills down into entity practices, when the results are all that should be looked for. The standard is requiring multiple reports. The Purpose of the Standard is very broad and should be revised because some of the events being reported on have no impact on the BES. Revise Purpose wording as follows: To improve industry awareness and the reliability of the Bulk Electric System “by requiring the reporting of major system events with the potential to impact reliability and their causes…” on the Bulk Electric System it can be said that every event occurring on the Bulk Electric System would have to be reported. Referring to Requirement R4, the testing of the communication process is the responsibility of the Responsible Entity. There is an event analysis process already in place. The standard prescribes different sets of criteria, and forms. There should be one recipient of event information. That recipient should be a “clearinghouse” to ensure the proper dissemination of information. Why is this standard applicable to the ERO? Requirement R2 is not necessary. It states the obvious. Requirements R2 and R3 are redundant. The standard mentions collecting information for Attachment 2, but nowhere does it state what to do with Attachment 2. None of the key concepts identified on page 5 of the standard are clearly stated or described in the requirements: • Develop a

single form to report disturbances and events that threaten the reliability of the bulk electric system. • Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements. • Establish clear criteria for reporting. • Establish consistent reporting timelines. • Provide clarity for who will receive the information and how it will be used. The standard's requirements should be reviewed with an eye for deleting those that are redundant, or do not address the Purpose or intent of the standard.
Group
Luminant Power
Stewart Rake
Yes
No
Requirements R1, R2, and R4 are burdensome administrative requirements and are contradictory to the NERC stated Standards Development goals of reducing administrative requirements by moving to performance requirements. There is only one Requirement needed in this standard: "The Responsible Entity shall report events in accordance with Attachment 1." Attachment 1 should describe how events should be reported by what Entity to which party within a defined timeframe. If this requirement is met, all the other proposed requirements have no benefit to the reliability of the Bulk Electric System. Per the NERC Standard Development guidelines, only items that provide a reliability benefit should be included in a standard.
No
Luminant agrees with the changes the SDT made, however, the timeline should be modified to put higher priority activities before reporting requirements. The SDT should consider allowing entities the ability to put the safety of personnel, safety of the equipment, and possibly the stabilization of BES equipment efforts prior to initiating the one hour reporting timeline. Reporting requirements should not be prioritized above these important activities. The requirement to report one hour after the recognition of such an event may not be sufficient in all instances. Entities should not have a potential violation as a result of putting these priority issues first and not meeting the one hour reporting timeline.
The following comments all apply to Attachment 1: • As a general comment, SDT should specifically list the entities the reportable event applies to in the table for clarity. Do not use general language referencing another standard or statements such as "Deficient entity is responsible for reporting", "Initiating entity is responsible for reporting", or other similar statements used currently in the table. This leaves this open and subject to interpretation. Also, there are a number of events that do not apply to all entities. • Destruction of BES equipment should be Intentional Damage or Destruction of BES equipment. Unintentional actions occur and should not be a requirement for reporting under disturbance reporting. • Actions or situations affecting equipment or generation unit availability due to human error, equipment failure, unintentional human action, external cause, etc. are reported in real time to the BA and other entities as required by other NERC Standards. Disturbance reporting should avoid the type of events that, for instance, would cause the total or partial loss of a generating unit under normal operational circumstances. There are a number of issues with the table in this regard. • For clarity, consider changing the table to identify for each event type "who" should be notified. This appears to be missing from the table overall. • Reportable Events, the meaning for the Event labeled "Destruction of BES equipment" is not clear. Footnote 1 adds the language "iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service." This language can be interpreted to mean that any damage to any BES equipment caused by human action, regardless of intention, must be reported within 1 hour of recognition of the event. This requirement will be overly burdensome. If this is not the intent of the definition of "Destruction of BES equipment", the footnote should be re-worded. As such, it is subjective and left open to interpretation. It should focus only on intentional actions to damage or interrupt BES functionality. It should not be worded as such that every item that trips a unit or every item that is damaged on a unit requires a report. That is where the language right now is not clear. There are and will continue to be unintentional human error that results in taking equipment out of service. This standard was meant to replace sabotage reporting. • Damage or destruction of Critical Asset per CIP-002 and Damage or destruction of a Critical Cyber Asset per CIP-002 should be removed from the table as Intentional Damage or Destruction of BES equipment would cover this as well. • Risk to BES

equipment should be removed from the table as it is very subjective and broad. At a minimum, the 1 hour reporting timeline should begin after recognition and assessment of the incident. As an example, a fire close to BES equipment may not truly be a threat to the equipment and will not be known until an assessment can be made to determine the risk. • Detection of a Reportable Cyber Security incident should be removed from the table as this is covered by CIP-008 requirements. Having this in two separate standards is double jeopardy and confusing to entities. • Generation Loss event reporting should only apply to the BA. These authorities have the ability and right to contact generation resources to supply necessary information needed for reporting. This would also eliminate redundant reporting by multiple entities for the same event. • Suggest that Generation Loss MW loss would match up with the 1500 MW level identified in CIP Version 4 or Version 5 for consistency between future CIP standards and this disturbance reporting standard. This would then cover CIP and significant MW losses that should be reported. • The Generation Loss MW loss amount needs to have a time boundary. Luminant would suggest a loss of 1500 MW within 15 minutes. • Unplanned Control Center evacuation should not apply to entities that have backup Control Centers where normal operations can continue without impact to the BES. • Loss of monitoring or all voice communication capability should be separated. Also the 24 hour reporting requirement may not be feasible if communications is down for longer than 24 hours. Luminant would suggest removal of the communication reporting event as there are a number of things that could cause this to occur for longer than the reporting requirement allows, thus putting entities at jeopardy of a potential violation that is out of their control. How does an entity report if all systems and communications are down for more than 24 hours? What about in instances of a partial or total blackout? These events could last much longer than 24 hours. All computer communication would likely also be down thus rendering electronic reporting unavailable.
Individual
Michael Moltane
ITC
Yes
Yes
No
See comments to Question #4
Footnote 1 and the corresponding Threshold For Reporting associated with the first Event in Attachment 1 are not consistent and thus confusing. Qualifying the term BES equipment through a footnote is inappropriate as it leads to this confusion. For instance, does iii under Footnote 1 apply only to BES equipment that meet i and ii or is it applicable to all BES equipment? The inclusion of equipment failure, operational error and unintentional human action within the threshold of reporting for “destruction” required in the first 3 Events listed in Attachment 1 is also not appropriate. It is clear through operational history that the intent of the equipment applied to the system, the operating practices and personnel training developed/delivered to operate the BES is to result in reliable operation of the BES which has been accomplished exceedingly well given past history. This is vastly different than for intentional actions and should be excluded from the first 3 events listed in Attachment. To the extent these issues are present in another event type they will be captured accordingly. Footnote 1 should be removed and the Threshold for Reporting associated with the first three events in Attachment 1 should be updated only to include intentional human action. This will also result in including all BES equipment that was intentionally damaged in the reporting requirement and not just the small subset qualified by the existing footnote 1. This provides a much better data sample for law enforcement to make assessments from than the smaller subset qualified by what we believe the intent of footnote 1 is.
Group
PacifiCorp
Sandra Shaffer
Yes
Yes

Yes
No comment.
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson
Yes
Yes
Yes
While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely “recognition” starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition.
Project 2008-06 proposes to withdraw the terms “Critical Asset” and “Critical Cyber Asset” from the NERC Glossary. In order to avoid a reliability gap when this occurs, we propose including High and Medium Impact BES Cyber Systems and Assets. The revised wording to add, “as appropriate” to R1.3 is a concern. We understand the SDT’s intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. R4 continues to be an onerous requirement for smaller entities. Verification was not part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1. Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3.
Individual
Tracy Richardson
Springfield Utility Board
Yes
Yes
Yes
• The Draft 3 Version History still lists the term “Impact Event” instead of “Event”. • Draft 3 of EOP-004-2 – Event Reporting does not provide a definition for the term “Event” nor does the NERC Glossary of Terms Used in Reliability Standards. SUB recommends that “Event” be listed and defined in “Definitions and Terms Used in the Standard” as well as the NERC Glossary, providing a framework and giving guidance to entities for how to determine what should be considered an “Event” (ex: sabotage, unusual occurrence, metal theft, etc.).
Individual
Kasia Mihalchuk
Manitoba Hydro
Yes

Yes
Yes
Attachment 1 - The term ‘Transmission Facilities’ used in Attachment 1 is capitalized, but it is not a defined term in the NERC glossary. The drafting team should clarify this issue. Attachment 2 - The inclusion of ‘Fuel supply emergency’ in Attachment 2 creates confusion as it infers that reporting a ‘fuel supply emergency’ may be required by the standard even though ‘fuel supply emergency’ is not listed in Attachment 1. On a similar note, it is not clear what the drafting team is hoping to capture by including a checkbox for ‘other’ in Attachment 2.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
Yes
Yes
1. EOP-004-2 R1.4 states entities must update their Operating Plans within 90 calendar days of incorporating lessons learned pursuant to R3. However, neither R3 nor Attachment 1 include a timeline for incorporating lessons learned. It is unclear when the “clock starts” on incorporating improvements or lessons learned. Within 90 days of what? 90 days of the event? 90 days from when management approved the lesson learned? Auditors need to know the trigger for the 90-day clock. 2. The Event Analysis classification includes Category 1C “failure or misoperation of the BPS SPS/RAS”. This category is not included in EOP-004-2’s Attachment 1. This event, “failure or misoperation of the BPS SPS/RAS”, needs to either be added to Attachment 1 or removed from the Event Analysis classification. It is important that EOP-004-2 Attachment 1 and the Event Analysis categories match up. Thank you for your work on this standard.
Individual
Kevin Conway
Intellibind
Yes
No
The language proposed is not clear and will continue to add confusion to entities who are trying to meet these requirements. It is not clear that the drafting team can put itself in the position of how the auditors will interpret and implement compliance against thithe R2 requirement. Requirements should be written to stand alone, not reference other requirements (or parts of the requirments. If the R1 parts 1.1, 1.2, 1.4 and 1.5 are so significant for this requirement, then they should be rewritten in R2.
Yes
Does this reporting conflict with reporting for DOE, and Regions? If so, what reporting requirements will the entity be held accountable to? Managing multiple reporting requirements for the multiple agencies is very problematic for entities and this standard should resolve those reporting requirments, as well as reduce the reporting down to one form and one submission. Reporting to ESISAC should take care of all reporting by the company. NERC should route all reports to the DOE, and regions through this mechanism.
I do not see that the rewrite of this standard is meeting the goal of clear reliability standards, and in fact the documents are looking more like legal documents. Though the original EOP-004 and CIP-001 was problematic at times, this rewrite, and the need to have such extensive guidance, attachments, and references for EOP-004-2 will create an even more difficult standard to properly meet to ensure

compliance during an audit. Though CIP-001 and EOP-004 were related, combining them in a single standard is not resolving the issues, and is in fact complicating the tasks. Requirements in this standard should deal with only one specific issue, not deal with multiple tasks. I am not sure how an auditor will consistently audit against R2, and how a violation will be categorized when an entity implements all portions of their Operating Plan, however fails to fully address all the requirements in R1, thereby not fully implementing R2, in strict interpretation. The drafting team should not set up a situation where an entity is in double jeopardy for missing an element of a requirement. I also suggest that EOP-004-2 be given a new EOP designation rather than calling it a revision. This way implementation can be better controlled, since most companies have written specific CIP-001 and EOP-004 document that will not simple transfer over to the new version. This standard is a drastic departure from the oringial versions. I appreciate the level of work that is going into EOP-004-2, it appears that significant time and effort has been going into the supporting documentation. It is my opinion that if this much material has to be created to state what the standard really requires, then the standard is flawed. When there are 21 pages of explanation for five requirements, especially when we have previously had 16 pages that originally covered 2 separate reliability standards, we need to reevaluate what we are really doing.
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
Yes
Yes
No comments
Individual
Chris Higgins / Jim Burns / Ted Snodgrass / Jeff Millennor / Russell Funk
Bonneville Power Administration
Yes
Yes
BPA believes the measures for R2 are unclear since they are similar to R3's reporting measures.
No
BPA believes that the first three elements in Attachment 1 are too generic and should be with only the intentional human criterion. The suspicious device needs to be determined as a threat (and not left behind tools) before requiring a report.
BPA believes that Attachment 1 has too many added reportable items because unintentional, equipment failure & operational errors are included in the first three items. A. Change to only "intentional human action". Otherwise, the first item "destruction of BES equipment" is too burdensome, along with its short time reporting time: i. - If a single transformer fails that shouldn't require a report. ii.- Emergency actions have to be taken for any failure of equipment, e.g. a loss of line reduces a path SOL and requires curtailments to reduce risk to the system. B. The item for "risk to BES" is not necessary until the suspicious object has been identified as a threat. If what turns out to be air impact wrench left next to BES equipment, that should not be a reportable incident as this current table implies. C. The nuclear "LOOP" should be only reported if total loss of off site source (i.e. 2 of 2 or 3 of 3) when supplying the plants load. If lightning or insulator fails causing one of the line sources to trip that's not a system disturbance especially if it is just used as a backup. It should only be a NRC process if they want to monitor that. The VRF/VSL: BPA believes that the VRF for R2 & R4 should be "Lower".
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.

Yes

No

Comments: • R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity: ["appropriate: - deleted] [otherwise it is not clear who determines what communication level is appropriate] • R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following ["within 90 calendar days of any" - deleted] change in assets or personnel (if the Operating Plan specifies personnel or assets) , ["other circumstances" - deleted] that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. • R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in "assets, personnel…. or incorporating lessons learned". This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis.

No

Comments: We have a number of comments on Attachment 1 and will make them here: • Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. • EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. • If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. • It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. • Event: "Risk to BES equipment" should be deleted. This is too vague and subjective. Will result in many "prove the negative" situations.' • Event: "Destruction of BES equipment" is again too vague. The footnote refers to equipment being "damaged or destroyed". There is a major difference between destruction and damage. • Event: "Damage or Destruction of a Critical Asset or Critical Cyber Asset" should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. • Event: "BES Emergency requiring public appeal for load reduction" should be modified to note that this does not apply to routine requests for customer conservation during high load periods.

Comments: • Requirement 4 does not specifically state details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit / enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. • R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. • The Purpose of the Standard should be revised because some of the events being reported on have no impact on the BES. Revise Purpose as follows: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of [add] "major system events." [delete - "with the potential to impact reliability and their causes, if known, by the Responsible Entities."]

Individual

David Burke

Orange and Rockland Utilities, Inc.

Yes

No

Comments: • R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity: ["appropriate: - deleted] [otherwise it is not clear who determines what communication level is appropriate] • R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following ["within 90 calendar days of any" - deleted] change in assets or personnel (if the Operating Plan specifies personnel or assets) , ["other circumstances" - deleted] that may no longer align with the Operating Plan; or incorporating lessons

learned pursuant to Requirement R3. • R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in “assets, personnel…. or incorporating lessons learned”. This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis.
No
• Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. • EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. • If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. • It is not clear what the difference is between a footnote and “Threshold for Reporting”. All information should be included in the body of the table, there should be no footnotes. • Event: “Risk to BES equipment” should be deleted. This is too vague and subjective. Will result in many “prove the negative” situations.’ • Event: “Destruction of BES equipment” is again too vague. The footnote refers to equipment being “damaged or destroyed”. There is a major difference between destruction and damage. • Event: “Damage or Destruction of a Critical Asset or Critical Cyber Asset” should be deleted. Disclosure policies regarding sensitive information could limit an entity’s ability to report. Unintentional damage to a CCA does not warrant a report. • Event: “BES Emergency requiring public appeal for load reduction” should be modified to note that this does not apply to routine requests for customer conservation during high load periods
Comments: • Requirement 4 does not specifically state details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit / enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. • R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. • The Purpose of the Standard should be revised because some of the events being reported on have no impact on the BES. Revise Purpose as follows: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of [add] "major system events.” [delete - “with the potential to impact reliability and their causes, if known, by the Responsible Entities.”]
Individual
Alice Ireland
Xcel Energy
Yes
No
Suggest modifying R3 to indicate this is related to R 1.3. Each Responsible Entity shall report events to entities specified in R1.3 and as identified as appropriate in its Operating Plan.
Yes
Group
BC Hydro
Patricia Robertson
Yes
Yes
No
As an event would be verbally reported to the RC, all the one hour requirements to submit a written report should be moved from one hour to 24 hours.
Attachment 1: Reportable Events: BC Hydro recommends further defining “BES equipment” for the

events Destruction of BES equipment and Risk to BES equipment. Attachment 1: Reportable Events: BC Hydro recommends defining the Forced intrusion event as the wording is very broad and open to each entities interpretation. What would be a forced intrusion ie entry or only if equipment damage occurs?
Individual
Greg Rowland
Duke Energy
Yes
Yes
No
All events in Attachment 1 should have reporting times of no less than 24 hours. As stated on page 6 of the current draft of the standard: “The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.” We maintain that a report which is required to be made within one hour after an event is, in fact, a real time report. In the first hour or even several hours after an event the operator may appropriately still be totally committed to restoring service or returning to a stable bulk power system state, and should not stop that recovery activity in order to make this “after-the-fact” report.
1. Reporting under EOP-004-2 should be more closely aligned with Events Analysis Reporting. 2. Attachment 1 – Under the column titled “Entity with Reporting Responsibility”, several Events list multiple entities, using the phrase “Each RC, BA, TO, TOP, GO, GOP, DP that experiences…” or a similar phrase requiring that multiple entities report the same event. We believe these entries should be changed so that multiple reports aren’t required for the same event. 3. Attachment 1 – The phrase “BES equipment” is used several times in the Events Table and footnotes to the table. “Equipment” is not a defined term and lacks clarity. “Element” and “Facility” are defined terms. Replace “BES equipment” with “BES Element” or “BES Facility”. 4. Attachment 1 – The Event “Risk to BES equipment” is unclear, since some amount of risk is always present. Reword as follows: “Event that creates additional risk to a BES Element or Facility.” 5. Attachment 1 – The Threshold for Reporting Voltage deviations on BES Facilities is identified as “+ 10% sustained for > 15 continuous minutes.” Need to clarify + 10% of what voltage? We think it should be nominal voltage. 6. Attachment 1 - Footnote 1 contains the phrase “has the potential to”. This phrase should be struck because it creates an impossibly broad compliance responsibility. Similarly, Footnote 3 contains the same phrase, as well as the word “could” several times, which should be changed so that entities can reasonably comply. 7. Attachment 1 – The “Unplanned Control Center evacuation” Event has the word “potential” in the column under “Entity with Reporting Responsibility”. The word “potential” should be struck. 8. Attachment 2 – Includes “fuel supply emergency”, which is not listed on Attachment 1.
Group
Progress Energy
Jim Eckelkamp
(1) Attachment 1 lists “Destruction of BES Equipment” as a reportable event but then lists “equipment failure” as one of several thresholds for reporting, with a one hour time limit for reporting. It is simply not common sense to think of the simple failure of a single piece of equipment as “destruction of BES equipment”. Does the standard really expect that every BES equipment failure must be reported within one hour, regardless of cause or impact to BES reliability? What is the purpose of such extensive reporting? (2) The same comment as (1) above is applicable to the “Damage or destruction of Critical Asset” because one threshold is simple “equipment failure” as well. (3) Footnote 2 (page 20) says copper theft is not reportable “unless it effects the reliability of the BES”, but footnote 1 on the same page says copper theft is reportable if “it degrades the ability of equipment to operate

properly". In this instance, the proposed standard provides two different criteria for reporting one of the most common events on the same page. (4) Forced Intrusion must be reported if "you cannot determine the likely motivation", and not based on a conclusion that the intent was to commit sabotage or intentional damage. This would require reporting many theft related instances of cut fences and forced doors (including aborted theft attempts where nothing is stolen) which would consume a great deal of time and resources and accomplish nothing. This criteria is exactly the opposite of the existing philosophy of only reporting events if there is an indication of an intent to commit sabotage or cause damage. (5) "Risk to BES equipment…from a non-environmental physical threat" is reportable, but this is an example of a vague, open ended reporting requirement that will either generate a high volume of unproductive reports or will expose reporting entities to audit risk for not reporting potential threats that could have been reported. The standard helpfully lists train derailments and suspicious devices as examples of reportable events. The existing CAN for CIP-001 (CAN-0016) is already asking for a list of events that were analyzed so the auditors can determine if a violation was committed due to failure to report. I can envision the CAN for this new standard requiring a list of all "non-environmental physical threats" that were analyzed during the audit period to determine if applicable events were reported. This could generate a great deal of work simply to provide audit documentation even if no events actually occur that are reportable. It would also be easy for an audit team to second guess a decision that was made by an entity not to report an event (what is risk?...how much risk was present due to the event?...). Also, the reporting for this vague criteria must be done within one hour. Any event with a one hour reporting requirement should be crystal clear and unambiguous. (6) Transmission Loss…of three or more Transmission Facilities" is reportable. "Facility" is a defined term in the NERC Glossary, but "Transmission Facility" is not a defined term, which will lead to confusion when this criteria is applied. This requirement raises many confusing questions. What if three or more elements are lost due to two separate or loosely related events – is this reportable or not? What processes will need to be put in place to count elements that are lost for each event and determine if reporting is required? Why must events be reported that fit an arbitrary numerical criteria without regard to any material impact on BES reliability?
Individual
Rodney Luck
Los Angeles Department of Water and Power
No
The reporting time of within 1 hour of recognition for a "Forced Intrusion" (last event category on page 20 of Draft 3, dated October 25, 2011) when considered with the associated footnote "Report if you cannot reasonably determine likely motivation" is overly burdensome and unrealistic. What is "reasonably determine likely motivation" is too general and requires further clarity. For example, LADWP has numerous facilities with extensive perimeter fencing. There is a significant difference between a forced intrusion like a hole or cut in a property line fence of a facility versus a forced intrusion at a control house. Often cuts in fences, after further investigation, are determined to be cases of minor vandalism. An investigation of this nature will take much more than the allotted hour. The NERC Design Team needs to develop difference levels for the term "Force Intrusion" that fit the magnitude of the event and provide for adequate time to determine if the event was only a case of minor vandalism or petty thief. The requirement, as currently written, would unnecessarily burden an entity in reporting events that after given more time to investigate would more than likely not have been a reportable event.
Individual
Daniel Duff
Liberty Electric Power
No
Training should be left in the standard as an option, along with an actual event, drill or exercise, to demonstrate that operating personnel have knowledge of the procedure.
Yes

Yes
Group
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi
Mary Jo Cooper
Yes
Yes
Yes
We feel that the drafting team has done an excellent job of providing clarification and reasonable reporting requirements to the right functional entity. However we feel additional clarification should be made in the Attachment I Event Table. We suggest the following modifications: For the Event: BES Emergency resulting in automatic firm load shedding Modify the Entity with Reporting Responsibility to: Each DP or TOP that experiences the automatic load shedding within their respective distribution serving or Transmission Operating area. For the Event: Loss of Firm load for ≥ 15 Minutes Modify the Entity with Reporting Responsibility to: Each BA, TOP, DP that experiences the loss of firm load within their respective balancing, Transmission operating, or distribution serving area.
Individual
Lisa Rosintoski
Colorado Springs Utilities
Yes
No
The act of implementing the plan needs to include reporting events per R1, sub-requirement 1.3. R2 should simply state something like, “Each Responsible Entity shall implement the Operating Plan that meets the requirements of R1, as applicable, for an actual event or as specified.” Suggest eliminating R3 which, seems to create double jeopardy effect.
Yes
Agree with concept to combine CIP-001 into EOP-004. Agree with elimination of “sabotage” concept. Appreciate the attempt to combine reporting requirements, but it seems that in practice will still have separate reporting to DOE and NERC/Regional Entities. EOP-004-2 A.5. “Summary of Key Concepts” refers to Att. 1 Part A and Att. 1 Part B. I believe these have now been combined. EOP-004-2 A.5. “Summary of Key Concepts” refers to development of an electronic reporting form and inclusion of regional reporting requirements. It is unfortunate no progress was made on this front.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
No
We agree with the revision to R2 and R3, but assess that a requirement to enforce implementation of Part 1.3 in Requirement R1 is missing. Part 1.3 in Requirement R1 stipulates that: 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the following as appropriate: • Internal company personnel • The Responsible Entity’s Regional Entity • Law enforcement • Governmental or provincial agencies The implementation of Part 1.3 is not enforced by R2 or R3 or any other Requirements in the standard. Suggest to add another requirement or expand Requirement R4 (and M4) to require the implementation of this Part in addition to verifying the process.

Yes
1. Measures M1, M2 and M3: Suggest to achieve consistent wording among them by saying the leading part to “Each Responsible Entity shall provide….” 2. In our comments on the previous version, we suggested the SDT to review the need to include IA, TSP and LSE for some of the reporting requirements in Attachment 1. The SDT’s responded that it had to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, they will be subject to reporting. We accept this rationale. However, the revised Attachment 1 appears to be still somewhat discriminative on who needs to report an event. For example, the event of “Detection of a reportable Cyber Security Incident” (6th row in the table) requires reporting by a list of responsible entities based on the underlying requirements in CIP-008, but the list does not include the IA, TSP and LSE. We again suggest the SDT to review the need for listing the specific entities versus leaving it general by saying: “Applicable Entities under CIP-008” for this particular item, and review and establish a consistent approach throughout Attachment 1. 3. VSLs: a. Suggest to not list all the specific entities, but replace them with “Each Responsible Entity” to simplify the write-up which will allow readers to get to the violation condition much more quickly. b. For R1, it is not clear whether the conditions listed under the four columns are “OR” or “AND”. We believe it means “OR”, but this needs to be clarified in the VSL table. 4. The proposed implementation plan conflicts with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by appending to the implementation plan wording, after “applicable regulatory approval” in the Effective Dates Section on P. 2 of the draft standard and P. 1 of the draft implementation plan, to the following effect: “, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.”
Individual
John Bee on Behalf of Exelon
Exelon
Yes
Yes
Why is the reference to R1.3 missing from EOP-004-2 Requirement R2?
No
Due to the size of the service territories in ComEd and PECO it’s difficult to get to some of the stations within in an hour to analyze an event which causes concern with the 1 hour criteria. It is conceivable that the evaluation of an event could take longer then one hour to determine if it is reportable. Exelon cannot support this version of the standard until the 1 hour reporting criteria is clarified so that the reporting requirements are reasonable and obtainable. Exelon has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. We would like a better understanding when the 1 hour clock starts please consider using the following clarifying statement, in the statements that read, “recognition of events” please consider replacing the word “recognition” with the word “confirmation” as in a “confirmed event”
1. Please replace the text “Operating Plan” with procedure(s). Many companies have procedure(s) for the reporting and recognition of sabotage events. These procedures extend beyond operating groups and provide guidance to the entire company. 2. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, as Exelon has previously commented, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Exelon understands that the DSR SDT evaluated the use of the word “source” but dismissed the use in favor of “supply” with the justification “[that] ‘supply’ encompasses all sources”. Exelon again suggests that the word “source” is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to “one or more” Exelon believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of “one or more” will ensure that all potential events (regardless of configuration of off-site

power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs. As previously suggested, Exelon again proposes that the loss of an off-site power source be revised to an “unplanned” loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance. Although the loss of one off-site power source may not result in a nuclear generating unit trip, Exelon agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows: Event: Unplanned loss of any off-site power source to a Nuclear Power Plant Entity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements. Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. 3. Attachment 1 Generation loss event criteria Generation loss The ≥ 2000 MW/≥ 1000 MW generation loss criteria do not provide a time threshold or location criteria. If the 2000 MW/1000 MW is intended to be from a combination of units in a single location, what is the time threshold for the combined unit loss? For example, if a large two unit facility in the Eastern Interconnection with an aggregate full power output of 2200 MW (1100 MW per unit) trips one unit (1100 MW) [T=0 loss of 1100 MW] and is ramping back the other unit from 100% power and 2 hours later the other unit trips at 50% power [550 MW at time of trip]. The total loss is 2200 MW; however, the loss was sustained over a 2 hour period. Would this scenario require reporting in accordance with Attachment 1? What if it happened in 15 minutes? 1 hour? 24 hours? Exelon suggests the criteria revised to include a time threshold for the total loss at a single location to provide this additional guidance to the GOP (e.g., within 15 minutes to align with other similar threshold conditions). Threshold for Reporting ≥ 2,000 MW unplanned total loss at a single location within 15 minutes for entities in the Eastern or Western Interconnection ≥ 1000 MW unplanned total loss at a single location within 15 minutes for entities in the ERCOT or Quebec Interconnection 4. Exelon appreciates that the DSR SDT has added the NRC to the list of Stakeholders in the Reporting Process, but does not agree with the SDT response to FirstEnergy’s comment to Question 17 [page 206] that stated “NRC requirements or comments fall outside the scope of this project.” Quite the contrary, this project should be communicated and coordinated with the NRC to eliminate confusion and duplicative reporting requirements. There are unique and specific reporting criteria and coordination that is currently in place with the NRC, the FBI and the JTTF for all nuclear power plants. If an event is in progress at a nuclear facility, consideration should be given to coordinating such reporting as to not duplicate effort, introduce conflicting reporting thresholds, or add unnecessary burden on the part of a nuclear GO/GOP who’s primary focus is to protect the health and safety of the public during a potential radiological sabotage event (as defined by the NRC) in conjunction with potential impact to the reliability of the BES. 5. Attachment 1 Detection of a reportable Cyber Security Incident event criteria The threshold for reporting is “that meets the criteria in CIP-008”. If an entity is exempt from CIP-008, does that mean that this reportable event is therefore also not applicable in accordance with EOP-004-2 Attachment 1?
Individual
Public Utility District No. 1 of Snohomish County
John D. Martinsen
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won’t be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards

Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. Related to "Reportable Events" of Attachment 1: 1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term "Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal "Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. Reporting Thresholds 1. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for ≥ 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. Firm Demand 1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a reliability issue. Clarification of Firm Demand would be helpful
Group
MRO NSRF
WILL SMITH
Yes
Yes
Yes
: The MRO NSRF wishes to thank the SDT for incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy's OE 417 reporting form.
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
Yes
Yes
Results-based standards should include, within each requirement, the purpose or reason for the requirement. The requirements of this standard, while we support the requirements, do not include the goal or proupose of meeting each stated requirement. The Measures all include language stating "the responsible entity shall provide…". During a quality review of a WECC Regional Reliability Standard we were told that the "shall provide" language is essentially another requirement to provide something. If it is truly necessary to provide this it should be in the requirements. It was suggested to us that we drop the "shall provide" language and just start each Measure with the "Evidence may include but is not limited to…".
Individual

RoLynda Shumpert
South Carolina Electric and Gas
Yes
Yes
Yes
In terms of receiving reports, is it the drafting teams expectation that separate reports be developed by both the RC and the TOP, GO, BA, etc. for an event that occurs on a company's system that is within the RC's footprint? One by the RC and one by the TOP, GO, BA, etc. In terms of meeting reporting thresholds, is it the drafting teams expectation that the RC aggregate events within its RC Area to determine whether a reporting threshold has been met within its area for the quantitative thresholds?
Individual
Kathleen Goodman
ISO New England
No
Please see further comments; we do not believe R4 is a necessary requirement in the standard and suggest it be deleted.
No
In accordance with the results-based standards concept, all that is required, for the “what” is that company X reported on event Y in accordance with the reporting requirements in attachment Z of the draft standard. Therefore, we proposed the only requirement that is necessary is R3, which should be re-written to read… "Each Responsible Entity shall report to address the events listed in Attachment 1."
Yes
Attachment 1should be revisited. “Equipment Damage” is overly vague and will also potentially result in reporting on equipment failures which may simply be related to the age and/or vintage of equipment.
Group
Imperial Irrigation District
Jesus Sammy Alcaraz
Yes
Yes
Yes
IID strongly believes the reporting flowchart should not be part of a standard. The suggestion is to replace it with a more clear, right to the point requirement.
Individual
Curtis Crews
Texas Reliability Entity
Substantive comments: 1.ERO and Regional Entities should not be included in the Applicability of this standard. Just because they may be subject to some CIP requirements does not mean they also have to be included here. The ERO and Regional Entities do not operate equipment or systems that are

integral to the operation of the BES. Also, none of the VSLs apply to the ERO or to Regional Entities. 2.The first entry in the Events Table should say “Damage or destruction of BES equipment.” Equipment may be rendered inoperable without being “destroyed,” and entities should not have to determine within one hour whether damage is sufficient to cause the equipment to be considered “destroyed.” Footnote 1 refers to equipment that is “damaged or destroyed.” 3.In the Events Table, consider whether the item for “Voltage deviations on BES facilities” should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator and power system stabilizer) could have a similar impact on the BES as other reportable items. 4.In the Events Table, under Transmission Loss, does this item require that at least three Facilities owned by one entity must be lost to trigger the reporting requirement, or is the reporting requirement also to be triggered by loss of three Facilities during one event or occurrence that are owned by two or three different entities? 5.In the Events Table, under Transmission Loss, it is unclear how Facilities are to be counted to determine when “three or more” Facilities are lost. In the NERC Glossary, Facility is ambiguously defined as “a set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In many cases, a “set of electrical equipment” can be selected and counted in different ways, which makes this item ambiguous. 6.In the Events Table, under Transmission Loss, it appears that a substation bus failure would only count as a loss of one Facility, even though it might interrupt flow between several transmission lines. We believe this type of event should be reported under this standard, and appropriate revisions should be made to this entry. 7.In the Events Table, under Transmission Loss, consider including generators that are lost as a result of transmission loss events when counting Facilities. For example, if a transmission line and a transformer fail, resulting in a generator going off-line, that should count as a loss of “three or more” facilities and be reportable under this standard. 8.In the Events Table, under “Unplanned Control Center evacuation” and “Loss of monitoring or all voice communication capability,” GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. 9.In the Events Table, under “Loss of monitoring or all voice communication capability,” we suggest adding that if there is a failure at one control center, that event is not reportable if there is a successful failover to a backup system or control center. 10.“Fuel supply emergency” is included in the Event Reporting Form, but not in Attachment 1, so there is no reporting threshold or deadline provided for this type of event. Clean-up items: 1.In R1.5, capitalize “Responsible Entity” and lower-case “process”. 2.In footnote 1, add “or” before “iii)” to clarify that this event type applies to equipment that satisfies any one of these three conditions. 3.In the Event Reporting Form, “forced intrusion” and “Risk to BES equipment” are run together and should be separated. VSLs: 1.We support the substance of the VSLs, but the repeated long list of entities makes the VSLs extremely difficult to read and decipher. The repeated list of entities should be replaced by “Responsible Entities.” 2.If the ERO and Regional Entities are to be subject to requirements in this standard (which we oppose), they need to be added to the VSLs.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
Yes
Yes
ATC appreciates the work of the SDT in incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy’s OE 417 reporting form.
Individual
Anthony Jablonski
ReliabilityFirst

ReliabilityFirst thanks the SDT for their effort on this project. ReliabilityFirst has a number of concerns/questions related to the draft EOP-004-2 standard which include the following: 1. General Comment - The SDT should consider any possible impacts that could arise related to the applicability of Generator Owners that may or may not own transmission facilities. This will help alleviate any potential or unforeseen impacts on these Generator Owners 2. General Comment – Though the rationale boxes contain useful editorial information for each requirement, they should rather contain the technical rationale or answer the question “why is this needed” for each requirement. The rationale boxes currently seem to contain suggestions on how to meet the requirements. ReliabilityFirst suggests possibly moving some of the statements in the “Guideline and Technical Basis” into the rationale boxes, as some of the rationale seems to be contained in that section. 3. General comment – The end of Measure M4 is incorrectly pointing to R3. This should refer to R4. 4. General Comment – ReliabilityFirst recommends the “Reporting Hierarchy for Reportable Events” flowchart should be removed from the “Background” section and put into an appendix. ReliabilityFirst believes the flowchart is not really background information, but an outline of the proposed process found in the new standard. 5. Applicability Comment – ReliabilityFirst questions the newly added applicability for both the Regional Entity (RE) and ERO. Standards, as outlined in many, if not all, the FERC Orders, should have applicability to users, owners and operators of the BES and not to the compliance monitoring entities (e.g. RE and ERO). Any requirements regarding event reporting for the RE and ERO should be dealt with in the NERC Rules of Procedure and/or Regional Delegation Agreements. It is also unclear who would enforce compliance on the ERO if the ERO remains an applicable entity. 6. Requirement Comment - ReliabilityFirst believes the process for communicating events in Requirement R1, Part 1.3 should be all inclusive and therefore include the bullet points. Bullet points are considered to be “OR” statements and thus ReliabilityFirst believes they should be characterized as sub-parts. Listed below is an example: 1.3. A process for communicating events listed in Attachment 1 to the following: 1.3.1 Electric Reliability Organization, 1.3.2 Responsible Entity’s Reliability Coordinator 1.3.3 Internal company personnel 1.3.4 The Responsible Entity’s Regional Entity 1.3.5 Law enforcement 1.3.6 Governmental or provincial agencies 7. Requirement Comment – ReliabilityFirst questions why Requirement R1, Part 1.1 and Part 1.2 are not required to be verified when performing a drill or exercise in Requirement R4? ReliabilityFirst believes that performing a drill or exercise utilizing the process for identifying events (Part 1.1) and the process for gathering information (Part 1.2) are needed along with the verification of the process for communicating events as listed in Part 1.3. 8. Compliance Section Comment – Section 1.1 states “If the Responsible Entity works for the Regional Entity…” and ReliabilityFirst questions the intent of this language. ReliabilityFirst is unaware of any Responsible Entities who work for a Regional Entity. Also, if the Regional Entity and ERO remain as applicable entities, in Section 1.1 of the standard, it is unclear who will act as the Compliance Enforcement Authority (CEA). 9. Compliance Section Comment – ReliabilityFirst recommends removing the second, third and fourth paragraphs from Section 1.2 since ReliabilityFirst believes entities should retain evidence for the entire time period since their last audit. 10. Compliance Section Comment – ReliabilityFirst recommends modifying the fifth paragraph from Section 1.2 as follows: “If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or until a data hold release is issued by the CEA.” ReliabilityFirst believes, as currently stated, the CEA would be required to retain information for an indefinite period of time. 11. Compliance Section Comment – ReliabilityFirst recommends removing the sixth paragraph from Section 1.2 since the requirement for the CEA to keep the last audit records and all requested and submitted subsequent audit records is already covered in the NERC ROP. 12. Attachment 1 Comment – It is unclear what the term/acronym “Tv” is referring to. It may be beneficial to include a footnote clarifying what the term “Tv” stands for. 13. VSL General Comment – although ReliabilityFirst believes that the applicability is not appropriate, as the REs and ERO are not users, owners, or operators of the Bulk Electrcic System, the Regional Entity and ERO are missing from all four sets of VSLs, if the applicability as currently written stays as is. If the Regional Entity and ERO are subject to compliance for all four requirements, they need to be included in the VSLs as well. Furthermore, for consistency with other standards, each VSL should begin with the phrase “The Responsible Entity…” 14. VSL 4 Comment - The second “OR” statement under the “Lower” VSL should be removed. By not verifying the communication process in its Operating Plan within the calendar year, the responsible entity completely missed the intent of the requirement and is already covered under the “Severe” VSL category.
Individual
Don Schmit

Nebraska Public Power District
Yes
Yes
Yes
Although 24 hours is a vast improvement, one business day would make more sense for after the fact reporting.
Individual
Dennis Sismaet
Seattle City Light
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won’t be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. Related to “Reportable Events” of Attachment 1: 1. A reportable event is stated as, “Risk to the BES”, the threshold for reporting is, “From a non-environmental physical threat”. This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. 2. A reportable event is stated as, “Damage or destruction of Critical Asset per CIP-002”. The term “Damage” would have to be defined in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. One could argue that normal “Damage” can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. Reporting Thresholds 1. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for ≥ 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. Firm Demand 1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a reliability issue. Clarification of Firm Demand would be helpful
Individual
John Seelke
PSEG
Yes

Yes
Yes
We have several comments: 1. The “Law Enforcement Reporting” section on p. 6 is unclearly written. The first three sentences are excerpted here: “The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement.” The outages described prior to the last sentence are “vandalism and terrorism.” The next sentence states “Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES.” If the SDT intended to only have events reported to law enforcement that could to Cascading, it should state so clearly and succinctly. But other language implies otherwise. a. The footnote 1 on Attachment 1 (p. 20) states: “Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).” Rendering a relay inoperative may or may not lead to Cascading. b. With regard to “forced intrusion,” footnote 2 on Attachment 1 states: “Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES.” The criterion, or criteria, for reporting an event to law enforcement needs to be unambiguous. The SDT needs to revise this “Law Enforcement Section” so that is achieved. The “law enforcement reporting” criterion, or criteria, should also be added to the flow chart on p. 9. We suggest the following as a starting point for the team to discuss: there should be two criteria for reporting an event to law enforcement: (1) BES equipment appears to have been deliberately damaged, destroyed, or stolen, whether by physical or cyber means, or (2) someone has gained, or attempted to gain, unauthorized access by forced or unauthorized entry (e.g., via a stolen employee keycard badge) into BES facilities, including by physical or cyber means. 2. The use of the terms “communicating events” in R1.3, and the use of the term “communication process” are confusing because in other places such as R3 the term “reporting” is used. If the SDT intends “communicating” to mean “reporting” as that later term is used in R3, it should use the same “reporting” term in lieu of “communicating” or “communication” elsewhere. Inconsistent terminology causes confusion. PSEG prefers the word “reporting” because it is better understood. 3. Attachment 1 needs to more clearly define what is meant by “recognition of an event.” a. When equipment or a facility is involved, it would better state within “X” time (e.g., 1 hour) of “of confirmation of an event by the entity that either owns or operates the Element or Facility.” b. Other reports should have a different specification of the starting time of the reporting deadline clock. For example, in the requirement for reporting a “BES Emergency requiring public appeal for load reduction,” it is unclear what event is required to be reported - the “BES Emergency requiring public appeal” or “public appeal for load reduction.” If the later is intended, then the event should be reported within “24 hours after a public appeal for load reduction is first issued.” These statements need to be reviewed and customized for each event by the SDT so they are unambiguous. In summary, the starting time for the reporting clock to start running should be made clear for each event. This will require that the SDT review each event and customize the starting time appropriately. The phrase “recognition of an event” should not be used because it is too vague. 4. When EOP-004-2 refers to other standards, it frequently omits the version of the standard. Example: see the second and third row of Attachment 1 that refers to “CIP-002.” Include the version on all standards referenced.
Group
Compliance & Responsbility Office
Silvia Parada Mitchell
Yes
See comments in response to Question 4.
Yes
See comments in response to Question 4.
Yes
See comments in response to Question 4.
NextEra Energy, Inc. (NextEra) appreciates the DSR SDT revising proposed EOP-004-2, based on the

previous comments of NextEra and the stakeholders. NextEra, however, believes that EOP-004-2 needs additional refinement prior to approval. R1.3 In R1.3, NextEra is concerned that the term "internal company personnel" is unclear and may be misinterpreted. For example, NextEra does not believe this term should include all company or corporate personnel, or even all personnel in the Responsible Entity's company or business unit. Instead, the definition of personnel should be limited to those who could be directly impacted by the event or are working on the event. Thus, NextEra suggests that the language in R1.3 be revised to read: "Internal Responsible Entity personnel whose tasks require them to take specific actions to mitigate, stop the spread and/or normalize the event, or personnel who are directly impacted by the event." NextEra is concerned that R1.3, as written, will be interpreted differently from company to company, region to region, auditor to auditor, and, therefore, may result in considerable confusion during actual events as well as during the audits/stop checks of EOP-004-2 compliance. Also, in R1.3, NextEra is concerned that many of the events listed in Attachment A already must be reported to NERC under its trial (soon to be final) Event Analysis Reporting requirements (Event Analysis). NextEra believes duplicative and different reporting requirements in EOP-004-2 and the Event Analysis rules will cause confusion and inefficiencies during an actual event, which will likely be counterproductive to promoting reliability of the bulk power system. Thus, NextEra believes that any event already covered by NERC's Event Analysis should be deleted from Attachment 1. Events already covered include, for example, loss of monitoring or all voice, loss of firm load and loss of generation. If this approach is not acceptable, NextEra proposes, in the alternative, that the reporting requirements between EOP-004-2 and Event Analysis be identical. For instance, in EOP-004-2, there is a requirement to report any loss of firm load lasting for more than 15 minutes, while the Event Analysis only requires reporting the of loss of firm load above 300 megawatts and lasting more than 15 minutes. Similarly, EOP-004-2 requires the reporting of any unplanned control center evacuation, while the Event Analysis only requires reporting after the evacuation of the control center that lasted 30 minutes or more. Thus, NextEra requests that either EOP-004-2 not address events that are already set forth in NERC's Event Analysis, or, in the alternative, for those duplicative events to be reconciled and made identical, so the thresholds set forth in the Event Analysis are also used in EOP-004-2. In addition, NextEra believes that a reconciliation between the language "of recognition" in Attachment 1 and "process to identify" in R1.1 is necessary. NextEra prefers that the language in Attachment 1 be revised to read " . . . of the identification of the event under the Responsible Entity's R1.1 process." For instance, the first event under the "Submit Attachment 2 . . . ." column should read: "The parties identified pursuant to R1.3 within 1 hour of the identification of an event under the Responsible Entity's R1.1 process." This change will help eliminate confusion, and will also likely address (and possibly make moot) many of the footnotes and qualifications in Attachment 1, because a Responsible Entity's process will likely require that possible events are properly vetted with subject matter experts and law enforcement, as appropriate, prior to identifying them as "events". Thus, only after any such vetting and a formal identification of an event would the one hour or twenty-four hour reporting clock start to run. R1.4, R1.5, R3 and R4 NextEra is concerned with the wording and purpose of R1.4, R1.5, R3 and R4. For example, R1.4 requires an update to the Operating Plan for ". . . any change in assets, personnel, other circumstances . . . ." This language is much too broad to understand what is required or its purpose. Further, R1.4 states that the Operating Plan shall be updated for lessons learned pursuant to R3, but R3 does not address lessons learned. Although there may be lessons learned during a post event assessment, there is no requirement to conduct such an assessment. Stepping back, it appears that the proposed EOP-004-2 has a mix of updates, reviews and verifications, and the implication that there will be lessons learned. Given that EOP-004-2 is a reporting Standard, and not an operational Standard, NextEra is not inclined to agree that it needs the same testing and updating requirements like EOP-005 (restoration) or EOP-008 (control centers). Thus, it is NextEra's preference that R1.4, R1.5 and R4 be deleted, and replaced with a new R1.4 as follows: R1.4 A process for ensuring that the Responsibly Entity reviews, and updates, as appropriate its Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews. If the DSR SDT does not agree with this approach, NextEra, in the alternative, proposes a second approach that consolidates R1.4, R1.5 and R4 in a new R1.4 as follows: R1.4 A process for ensuring that the Responsibly Entity tests and reviews its Operating Plan at least annually (once each calendar year) with no more than 15 months between a test and review. Based on the test and review, the Operating Plan shall be updated, as appropriate, within 90 calendar days. If an actual event occurs, the Responsible Entity shall conduct a post event assessment to identify any lessons learned within 90 calendar days of the event. If the Responsible Entity identifies any lessons learned in post event assessment, the lessons

learned shall be incorporated in the Operating Plan within 90 calendar days of the date of the final post event assessment. NextEra purposely did not add language regarding “any change in assets, personnel etc,” because that language is not sufficiently clear or understandable for purposes of a mandatory requirement. Although it may be argued that it is a best practice to update an Operating Plan for certain changes, unless the DST SDT can articulate specific, concrete and understandable issues that require an updated Operating Plan prior to an annual review, NextEra recommends that the concept be dropped. Nuclear Specific Concerns EOP-004-2 identifies the Nuclear Regulatory Commission (NRC) as a stakeholder in the Reporting Process, but does not address the status of reporting to the NRC in the Event Reporting flow diagram on page 9. Is the NRC considered Law Enforcement as is presented in the diagram? Since nuclear stations are under a federal license, some of the events that would trigger local/state law enforcement at non-nuclear facilities would be under federal jurisdiction at a nuclear site. There are some events listed in Attachment 1 that seem redundant or out of place. For example, a forced intrusion is a one hour report to NERC. However, if there is an ongoing forced intrusion at a nuclear power plant, there are many actions taking place, with the NRC Operations Center as the primary contact which will mobilize the local law enforcement agency, etc. It is unclear that reporting to NERC in one hour promotes reliability or the resolution of an emergency in progress. Also, is there an ability to have the NRC in an emergency notify NERC? The same concerns related to cyber security events. Procedures versus Plan NextEra also suggests replacing "Operating Plan" with "procedures". Given that EOP-004-2 is a reporting Standard and not an operational Standard, it is typical for procedures that address this standard to reside in other departments, such as Information Management and Security. In other words, the procedures needed to address the requirements of EOP-004-2 are likely broader than the NERC-defined Operating Plan. Clean-Up Items In Attachment 1, Control Centers should be capitalized in all columns so as not to be confused with control rooms. Also, the final product should clearly state that the process flow chart that is set forth before the Standard is for illustrative purposes, so there is no implication that a Registered Entity must implement multiple procedures versus one comprehensive procedure to address different reporting requirements.

Individual

Barry Lawson

NRECA

1. Please ensure that the work of the SDT is done in close coordination with Events Analysis Process (EAP) work being undertaken by the PC/OC and BOT, and with any NERC ROP additions or modifications. NRECA is concerned that the EAP work being done by these groups is not closely coordinated even though their respective work products are closely linked -- especially since the EAP references information in EOP-004. 2. The SDT needs to be consistent in its use of "BES" and "BPS" – boths acronyms are used throughout the SDT documents. NRECA strongly prefers the use of "BES" since that is what NERC standards are written for. 3. Under “Purpose” section of standard, 3rd line, add “BES” between “impact” and “reliability.” Without making this change the "Purpose" section could be misconstrued to refer to reliability beyond the BES. 4. In the Background section there is reference to the Events Analysis Program. Is that the same thing as the Events Analysis Process? Is it something different? Is it referring to a specific department at NERC? Please clarify in order to reduce confusion. Also in the Background section there is reference to the Events Analysis Program personnel. Who is this referring to -- NERC staff in a specific department? Please clarify. 5. In M1 please be specific regarding what “dated” means. 6. In M3 please make it clear that if there wasn’t an event, this measure is not applicable 7. In R4 it is not clear what “verify” means. Please clarify. 8. In Attachment 1 there are references to Critical Asset and Critical Cyber Asset. These terms will likely be eliminated from the NERC Glossary of Terms when CIP V5 moves forward and is ultimately approved by FERC. This could create future problems with EOP-004 if CIP V5 is made effective as currently drafted. 9. In Attachment 1 the one hour timeframe for submitting data for the first 7 items listed is very tight. Other than being required by the EOE)E-417 form, NRECA requests that the SDT provide further support for this timeframe. If there are not distinct reasons why 1 hour is the right timeframe for this, then other timeframes should be explored with DOE. 10. While including Footnote 1 is appreciated, NRECA is concerned that this footnote will create confusion in the compliance and audit areas and request the SDT to provide more definitive guidance to help explain what these "Events"

refer to. NRECA has the same comment on Footnote 2 and 3. Specifically in Footnote 3, how do you clearly determine and audit from a factual standpoint something that “could have damaged” or “has the potential to damage the equiment?” 11. In the Guideline and Technical Basis section, in the 1st bullet, how do you determine, demonstrate and audit for something that “may impact” BES reliability? 12. On p. 28, first line, this sentence seems to state that NERC, law enforcement and other entities – not the responsible entity – will be doing event analysis. My understanding of the current and future Event Analysis Process is that the responsible entity does the event analysis. Please confirm and clarify.
Individual
Terry Harbour
MidAmerican Energy
Yes
Yes
No
MidAmerican Energy agrees with the direction of consolidating CIP-001, EOP-004 and portions of CIP-008. However, we have concerns with some of the events included in Attachment 1 and reporting timelines. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. Based on our understanding of Attachment 1, the category of “damage or destruction of a critical cyber asset” will result in hundreds or thousands of small equipment failures being reported to NERC and DOE, with no improvement to security. For example, hard drive failures, server failures, PLC failures and relay failures could all meet the criteria of “damage or destruction of a critical cyber asset.” We recommend replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. Reporting timelines and reporting form FERC Order 706, paragraph 676, directed NERC to require a responsible entity to “at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.” In paragraph 674, FERC stated that the Commission agrees that, in the “aftermath of a cyber attack, restoring the system is the utmost priority.” They clarified: “the responsible entity does not need to initially send a full report of the incident…To report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever useful preliminary information is available at the time. This could be accomplished by a phone call or another method.” While FERC did not order completion of a full report within one hour in Order 706, the draft EOP-004 Attachment 1 appears to require submittal of formal reports within one hour for six of the categories, unless there have been “certain adverse conditions” (in which case, as much information as is available must be submitted at the time of notification). The Violation Severity Levels are extreme for late submittal of a report. For example, it would be a severe violation to submit a report more than three hours following an event for an event requiring reporting in one hour. MidAmerican Energy suggests incorporating the language from FERC Order 706, paragraph 674, into the EOP-004 reporting requirement to allow preliminary reporting within one hour to be done through a phone call or another method to allow the responsible entity to focus on recovery and/or restoration, if needed. MidAmerican Energy agrees with the use of DOE OE-417 for submittal of the full report of incidents under EOP-004 and CIP-008. We would note there are two parts to this form -- Schedule 1-Alert Notice, and Schedule 2-Narrative Description. Since OE-417 already requires submittal of a final report that includes Schedule 2 within 48 hours of the event, MidAmerican Energy believes it is not necessary to include a timeline for completion of the final report within the EOP-004 standard. We would note that Schedule 2 has an estimated public reporting burden time of two hours so it is not realistic to expect Schedule 2 to be completed within one hour. Events included in Attachment 1: MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. The categories listed in Attachment 1 with one-hour reporting timelines cause the greatest concern. None

of these categories are listed in OE-417, and all but the last row would not be considered a Cyber Security Incident under CIP-008, unless there was malicious or suspicious intent.
MidAmerican proposes eliminating the phrase “with no more than 15 months between reviews” from R1.5. While we agree this is best practice, it creates the need to track two conditions for the review, eliminates flexibility for the responsible entity and does not improve security to the Bulk Electric System. There has not been a directive from FERC to specify the definition of annual within the standard itself. In conjunction with this comment, the Violation Severity Levels for R4 should be revised to remove the references to months.
Group
ACES Power Marketing Standards Collaborators
Jean Nitz
No
We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard, in particular to requirement R4. The use of the words “or through a drill or exercise” still implies that training is required if no actual event has occurred. When you conduct a fire “drill” you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually.
No
Requirement R2 requires Responsible Entities to implement the various sub-requirements in R1. We believe it is unnecessary to state that an entity must implement their Operating Plan in a separate requirement. Having a separate requirement seems redundant. If the processes in the Operating Plan are not implemented, the entity is non-compliant with the standard. There doesn’t need to be an extra requirement saying entities need to implement their Operating Plan.
Yes
For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting.
Individual
Thad Ness
American Electric Power
Yes
No
AEP prefers to avoid requirements that are purely administrative in nature. Requirements should be clear in their actions of supporting of the BES. For example, we would prefer requirements which state what is to be expected, and allowing the entities to develop their programs, processes, and procedures accordingly. It has been our understanding that industry, and perhaps NERC as well, seeks to reduce the amount to administrative (i.e. document-based) requirements. We are confident that the appropriate documentation and administrative elements would occur as a natural course of implementing and adhering to action-based requirements. In light of this perspective, we believe that that R1 and R2 is not necessary, and that R3 would be sufficient by itself. Our comments above notwithstanding, AEP strongly encourages the SDT to consider that R2 and R3, if kept, be merged into a single requirement as a violation of R2 would also be a violation of R3. Two violations would then occur for what is essentially only a single incident. Rather than having both R2 and R3, might R3 be sufficient on its own? R2 is simply a means to an end of achieving R3. If there is a need to explicitly reference implementation, that could be addressed as part of R1. For example, R1 could

state “Each Responsible Entity shall implement an Operating Plan that includes...” R1 seems disjointed, as subparts 1.4 and 1.5 (updating and reviewing the Operating Plan) do not align well with subparts 1.1 through 1.3 which are process related. If 1.4 and 1.5 are indeed needed, we recommend that they be a part of their own requirement(s). Furthermore, the action of these requirements should be changed from emphasizing provision(s) of a process to demonstrating the underlying activity. 1.4: AEP is concerned by the vagueness of requiring provision(s) for updating the Operating Plan for “changes”, as such changes could occur frequently and unpredictably.

Yes

M4: Recommend removing the text “for events” so that it instead reads “The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan created pursuant to Requirement R1, Part 1.3.” R4: It is not clear to what extent the verification needs to be applied if the process used is complex and includes a variety of paths and/or tasks. The draft team may wish to consider changing the wording to simply state ”each Responsible Entity shall test each of the communication paths in the operating plan”. We also recommend dropping “once per calendar year” as it is inconstant with the measure itself which allows for 15 months.

Individual

Guy Andrews

Georgia System Operations Corporation

Yes

Yes

Yes

The ERO and the Regional Entity should not be listed as Responsible Entities. The ERO and the Regional Entity should not have to meet the requirements of this standard, especially reporting to itself. Attachment 1 (all page numbers are from the clean draft): Page 20, destruction of BES equipment: part iii) of the footnote adds damage as an event but the heading is for destruction. Is it just for destruction? Or is it for damage or destruction? Page 21, Risk to BES equipment: Footnote 3 gives an example where there is flammable or toxic cargo. These are environmental threats. However, the threshold for reporting is for non-environmental threats. Which is it? Page 21, BES emergency requiring public appeal for load reduction: A small deficient entity within a BA may not initiate public appeals. The BA is typically the entity which initiates public appeals when the entire BA is deficient. The initiating entity should be the responsible entity not the deficient entity. Page 21, BES emergency requiring manual firm load shedding: If a RC directs a DP to shed load and the DP initiates manually shedding its load as directed, is the RC the initiating entity? Or is it the DP? Page 22, system separation (islanding): a DP does not have a view of the system to see that the system separated or how much generation and load are in the island. Remove DP. Attachment 2 (all page numbers are from the clean draft): Page 25: fuel supply emergencies will no longer be reportable under the current draft. Miscellaneous typos and quality issues (all page numbers are from the clean draft): Page 5, the last paragraph: There are two cases where Parts A or B are referred to. Attachment 1 no longer has two parts (A & B). Page 27, Discussion of Event Reporting: the second paragraph has a typo at the beginning of the sentence.

Group

Florida Municipal Power Agency

Frank Gaffney

No

First, we wish to thank the SDT for their hard work and making significant progress in significant improvements in the standard. We commend the direction that the SDT is taking. There are; however, a few unresolved issues that cause us to not support the standard at this time. An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states “the following as appropriate”. Who has the authority to deem what is appropriate? The requirements should be clear that the Responsible Entity is the decision maker of

who is appropriate, otherwise there is opportunity for conflict between entities and compliance. In addition, 1.4 is onerous and burdensome regarding the need to revise the plan within 90 days of "any" change, especially considering the ambiguity of "other circumstances". "Other circumstances" is open to interpretation and a potential source of conflict.
No
Both requirements are to implement the Operating Plan. Hence, R3 should be a bullet under R2 and not a separate requirement. In addition, for R2, the phrase "actual event" is ambiguous and should mean: "actual event that meets the criteria of Attachment 1" We suggest the following wording to R2 (which will result in eliminating R3) "Each Responsible Entity shall implement its Operating Plan: • For actual events meeting the threshold criteria of Attachment 1 in accordance with Requirement R1 parts 1.1, 1.2 and 1.3 • For review and updating of the Operating Plan in accordance with Requirement R1 parts 1.4 and 1.5" Note that we believe that if the SDT decides to not combine R2 and R3, then we disagree with the distinction between the two requirements. The division of implementing R1 through R2 and R3 as presented is "implementing" vs. "reporting". We believe that the correct division should rather be "implementation" of the plan (which includes reporting) vs. revisions to the plan.
No
The times don't seem aggressive enough for some of the Events related to generation capacity shortages, e.g., we would think public appeal, system wide voltage reduction and manual firm load shedding ought to be within an hour. These are indicators that the BES is "on the edge" and to help BES reliability, communication of this status is important to Interconnection-wide reliability.
The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. In R4, it might be worth clarifying that, in this case, implementation of the plan for an event that does not meet the criteria of Attachment 1 and going beyond the requirements R2 and R3 could be used as evidence. Consider adding a phrase as such to M4, or a descriptive footnote that in this case, "actual event" may not be limited to those in Attachment 1. Comments to Attachment 1 table: On "Damage or destruction of Critical Asset" and "… Critical Cyber Asset", Version 5 of the CIP standards is moving away from the binary critical/non-critical paradigm to a high/medium/low risk paradigm. Suggest adding description that if version 5 is approved by FERC, that "critical" would be replaced with "high or medium risk", or include changing this standard to the scope of the CIP SDT, or consider posting multiple versions of this standard depending on the outcome of CIP v5 in a similar fashion to how FAC-003 was posted as part of the GO/TO effort of Project 2010-07. On "forced intrusion", the phrase "at BES facility" is open to interpretation as "BES Facility" (e.g., controversy surrounding CAN-0016) which would exclude control centers and other critical/high/medium cyber system Physical Security Perimeters (PSPs). We suggest changing this to "BES Facility or the PSP or Defined Physical Boundary of critical/high/medium cyber assets". This change would cause a change to the applicability of this reportable event to coincide with CIP standard applicability. On "Risk to BES equipment", that phrase is open to too wide a range of interpretation; we suggest adding the word "imminent" in front of it, i.e., "Imminent risk to BES equipment". For instance, heavy thermal loading puts equipment at risk, but not imminent risk. Also, "non-environmental" used as the threshold criteria is ambiguous. For instance, the example in the footnote, if the BES equipment is near railroad tracks, then trains getting derailed can be interpreted as part of that BES equipment's "environment", defined in Webster's as "the circumstances, objects, or conditions by which one is surrounded". It seems that the SDT really means "non-weather related", or "Not risks due to Acts of Nature". On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? Should LSE be an applicable entity to "loss of firm load"? As proposed, the DP is but the LSE is not. In an RTO market, will a DP know what is firm and what is non-firm load? Suggest eliminating DP from the applicability of "system separation". The system separation we care about is separation of one part of the BES from another which would not involve a DP. On "Unplanned Control Center Evacuation", CIP v5 might add GOP to the applicability, another reason to add revision of EOP-004-2 to the scope of the CIP v5 drafting team, or in other ways coordinate this SDT with that SDT. Consider posting a couple of versions of the standard depending on the outcome of CIP v5 in a similar fashion to the multiple versions of FAC-003 posted with the Go/TO effort of

Project 2010-07.
Individual
Ed Davis
Entergy Services
Entergy agrees with and supports comments submitted by the SERC OC Standards Review group.
Individual
Margaret McNaul
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency
The first three incident categories designated on Attachment 1 as reportable events should be modified. As the Standard is current drafted, each incident category (i.e., destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets) requires reporting if the event was due to unintentional human action. For example, under the reporting criteria as drafted, inadvertently dropping and damaging a piece of computer equipment designated as a Critical Cyber Asset while moving or installing it would appear to require an event report within an hour of the incident. MDEA requests that the Drafting Team consider modifying footnote 1 and each of the first three event categories to reflect that reportable events include only those that (i) affect an IROL; (ii) significantly affect the reliability margin of the system; or (iii) involve equipment damage or destruction due to intentional human action that results in the removal of the BES equipment, Critical Assets, and/or Critical Cyber Assets, as applicable, from service. Footnote 2 (which now pertains only to the fourth incident category – forced intrusions) should also apply to the first three event categories. Specifically, responsible entities should report intentional damage or destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets if either the damage/destruction was clearly intentional or if motivation for the damage or destruction cannot reasonably be determined and the damage or destruction affects the reliability of the BES. Attachment 1 is also unclear to the extent that the incident category involving reports for the detection of reportable Cyber Security Incidents includes a reference to CIP-008 as the reporting threshold. While entities in various functional categories (i.e., RCs, BAs, TOPs/TOs, GOPs/GOs, and DPs) are listed as being responsible for the reporting of such events, some entities in these functional categories may not currently be subject to CIP-008. If it is the Drafting Team's intent to limit event reports for Cyber Security Incidents to include only registered entities subject to CIP-008, that clarification should be incorporated into the listing of entities with reporting responsibility for this incident category in Attachment 1.
Group
Santee Cooper
Terry L. Blackwell
Yes
Yes
Yes
The on-going development of the definition of the BES could have significant impacts on reporting requirements associated with this standard. The event titled "Risk to the BES" appears to be a catch-all event and more guidance needs to be provided on this category. The event titled "Damage or Destruction of a Critical Asset or Critical Cyber Asset per CIP-002" is ambiguous and further guidance is recommended. Ambiguity in a standard leaves it open to interpretation for all involved.
Group

Sacramento Municipal Utility District (SMUD)
Joe Tarantino
Yes
Yes
Yes
SMUD and BANC agree with the revised language in EOP-004-1 requirements, but we have identified the following issues in A-1: We commend the SDT for properly addressing the sabotage issue. However, additional confusion is caused by introducing term "damage". As "damage" is not a defined term it would be beneficial for the drafting team to provide clarification for what is meant by "damage". The threshold for reporting "Each public Appeal for load reduction" should clearly state the triggering is for the BES Emergency as routine "public appeal" for conservation could be considered a threshold for the report triggering. Regarding the SOL Violations in Attachment 1 the SOL Violations should only be those that affect the WECC paths. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
IMEA agrees with the removal of the training requirement, but also believes verification is not a necessary requirement for this standard; therefore, R4 is not necessary and should be removed.
No
R2 is not necessary, and should be removed. Subrequirement R1.4 is also not necessary and should be removed.
Yes
With the understanding this is within 24 hrs., and good professional judgment determines the amount of time to report the event to appropriate parties.
IMEA appreciates this opportunity to comment. IMEA appreciates the SDT's efforts to simplify reporting requirements by combining CIP-001 with EOP-004. [IMEA encourages NERC to continue working towards a one-stop-shop to simplify reporting on ES-ISAC.] IMEA supports, and encourages SDT consideration of, comments submitted by APPA and Florida Municipal Power Agency.
Individual
Kirit Shah
Ameren
No
The current language in the parenthesis of R4 suggests that the training requirement was actually not removed, in that "a drill or exercise" constitutes training. As documented in the last sentence of the Summary of Key Concepts section, "The proposed standard deals exclusively with after-the-fact reporting." We feel that training, even if it is called drills or exercises is not necessary for an after-the-fact report.
No
(1) The new wording while well intentioned, effectively does not add clarity and leads to confusion. From our perspective, R1, which requires and Operating Plan, which is defined by the NERC glossary as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." (2) Is not a proper location for an after-the-fact reporting standard? In fact it could be argued that after-the-fact reports in and of themselves do not affect the reliability of the bulk

electric system. (3) But considering the proposed standard as written with the Operating Plan in requirement R1, and implementation of the Operating Plan in requirement R2 (except the actual reporting which is in R3) and then R3 which requires implementing the reporting section R1.3, it is not clear how these requirements can be kept separate in either implementation nor by the CEA. (4) The second sentence in the second paragraph of “Rationale for R1” states: “The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report.” This is crucial for a Standard like this that is intended to mandate actions for events that are frequently totally unexpected and beyond normal planning criteria. This language needs to be added to Attachment 1 by the DSR SDT as explained in the rest of our comments
No
(1)By our count there are still six of the nineteen events listed with a one hour reporting requirement and the rest are all within 24 hour after the occurrence (or recognition of the event). This in our opinion, is reporting in real-time, which is against one of the key concepts listed in the background section:"The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting." (2)We believe the earliest preliminary report required in this standard should at the close of the next business day. Operating Entities, such as the RC, BA, TOP, GOP, DP, and LSE should not be burdened with unnecessary after-the-fact reporting while they are addressing real-time operating conditions. Entities should have the ability to allow their support staff to perform this function during the next business day as needed. We acknowledge it would not be an undue burden to cc: NERC on other required governmental reports with shorter reporting timeframes, but NERC should not expand on this practice. (3)We agree with the extension in reporting times for events that now have 24 hours of reporting time. As a GO there are still too many potential events that still require a 1 hour reporting time that is impractical, unrealistic and could lead to inappropriate escalation of normal failures. For example, the sudden loss of several control room display screens for a BES generator at 2 AM in the morning, with only 1 hour to report something, might be mistakenly interpreted as a cyber-attack. The reality is most likely something far more mundane such as the unexpected failure of an instrument transformer, critical circuit board, etc.
Yes. We have the other comments as follow: (1) The "EOP-004 Attachment 1: Events Table" is quite lengthy and written in a manner that can be quite subjective in interpretation when determining if an event is reportable. We believe this table should be clear and unambiguous for consistent and repeatable application by both reliability entities and a CEA. The table should be divided into sections such as: 9a) Events that affect the BES that are either clearly sabotage or suspected sabotage after review by an entity's security department and local/state/federal law enforcement.(b) Events that pose a risk to the BES and that clearly reach a defined threshold, such as load loss, generation loss, public appeal, EEAs, etc. that entities are required to report by the end of the next business day.(c) Other events that may prove valuable for lessons learned, but are less definitive than required reporting events. These events should be reported voluntarily and not be subject to a CEA for non-reporting.(d)Events identified through other means outside of entity reporting, but due to their nature, could benefit the industry by an event report with lessons learned. Requests to report and perform analysis on these type of events should be vetted through a ERO/Functional Entity process to ensure resources provided to this effort have an effective reliability benefit. (2)Any event reporting shall not in any manner replace or inhibit an Entity's responsibility to coordinate with other Reliability Entities (such as the RC, TOP, BA, GOP as appropriate) as required by other Standards, and good utility practice to operate the electric system in a safe and reliable manner. (3) The 1 hour reporting maximum time limit for all GO events in Attachment 1 should be lengthened to something reasonable – at least 24 hours. Operators in our energy centers are well-trained and if they have good reason to suspect an event that might have serious impact on the BES will contact the TOP quickly. However, constantly reporting events that turn out to have no serious BES impact and were only reported for fear of a violation or self-report will quickly result in a cry wolf syndrome and a great waste of resources and risk to the GO and the BES. The risk to the GO will be potential fines, and the risk to the BES will be ignoring events that truly have an impact of the BES.(4)The 2nd and 3rd Events on Attachment 1 should be reworded so they do not use terms that may have been deleted from the NERC Glossary by the time FERC approves this Standard. (5) The terms “destruction” and “damage” are key to identifying reportable events. Neither has been defined in the Standard. The term

destruction is usually defined as 100% unusable. However, the term damage can be anywhere from 1% to 99% unusable and take anywhere from 5 minutes to 5 months to repair. How will we know what the SDT intended, or an auditor will expect, without additional information? (6)We also do not understand why “destruction of BES equipment” (first item Attachment 1, first page) must be reported < 1 hour, but “system separation (islanding) > 100 MW” (Attachment 1, page 3) does not need to be reported for 24 hours. (7)The first 2 Events in Attachment 1 list criteria Threshold for Reporting as “…operational error, equipment failure, external cause, or intentional or unintentional human action.” The term “intentional or unintentional human action” appears to cover “operational error” so these terms appear redundant and create risk of misreporting. Can this be clarified? (8)The footnote of the first page of Attachment 1 includes the explanation “…ii) Significantly affects the reliability margin of the system…” However, the GO is prevented from seeing the system and has no idea what BES equipment can affect the reliability margin of the system. Can this be clarified by the SDT? (9) The use of the term “BES equipment” is problematic for a GO. NERC Team 2010-17 (BES Definition) has told the industry its next work phase will include identifying the interface between the generator and the transmission system. The 2010-17 current effort at defining the BES still fails to clearly define whether or not generator tie-lines are part of the BES. In addition, NERC Team 2010-07 may also be assigned the task of defining the generator/transmission interface and possibly whether or not these are BES facilities. Can the SDT clarify the use of this term? For example, does it include the entire generator lead-line from the GSU high-side to the point of interconnection? Does it include any station service transformer supplied from the interconnected BES?
Individual
Linda Jacobson-Quinn
FEUS
Yes
Yes
No
The OE-417 requires several of the events listed in Attachment 1 be reported within 1 hour. FEUS recommends the drafting team review the events and the OE-417 form and align the reporting window requirements. For example, public appeals, load shedding, and system seperation have a 1 hour requirement in OE-417.
R4 requires verification through a drill or exercise the communication process created as part of R1.3. Clarification of what a drill or exercise should be considered. In order to show compliance to R4 would the entity have to send a pseudo event report to Internal Personnel, the Regional Entity, NERC ES-ISAC, Law Enforcement, and Governmental or provincial agencies listed in R1.3 to verify the communications plan? It would not be a burden on the entity so much, however, I’m not sure the external parties want to be the recipient of approximately 2000 psuedo event reports annually. Attachment 1: BES equipment is too vague – consider changing to BES facility and including that reduces the reliability of the BES in the footnote. Is the footnote an and or an or? Attachment 1: Version 5 of CIP Requirements remove the terms Critical Asset and Critical Cyber Asset. The drafting team should consider revising the table to include BES Cyber Systems. Clarify if Damage or Destruction is physical damage (aka – cyber incidents would be part of CIP-008.) Attachment 1: Unplanned Control Center evacuation – remove “potential” from the reporting responsibility Attachment 2 – 3: change to, “Did the event originate in your system?” The requirement only requires reporting for Events – not potential events. Attachment 2 4: “Damage or Destruction to BES equipment” should be “Destruction of BES Equipment” like it is in Attachment 1 and “forced intrusion risk to BES equipment” remove “risk”
Individual
Tom Foreman
Lower Colorado River Authority
Yes
Yes

Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards. Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. Related to “Reportable Events” of Attachment 1: 1. The “Purpose” section of the Standard indicates it is designed to require the reporting of events “with the potential to impact reliability” of the BES. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because s plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting. 3. The word “Significantly” in item ii) of footnote 1 introduces an element of subjectivity. What is “significant” to one person may not be significant to someone else. 4. The word “unintentional” in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to “Damage or destruction of BES equipment” (2) removing the footnote and (3) replacing the existing “Threshold for Reporting” with the following language: “Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)” 5. One reportable event is, “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. 6. One reportable event is, “Damage or destruction of Critical Asset per CIP-002.” The SDT should define the term “Damage” in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. Normal “damage” can occur on a CA that should not be reportable (e.g. the screwdriver example, above). 7. For the event called “BES Emergency requiring public appeal for load reduction,” the SDT should make it clear who should report such an event. For example, in the ERCOT Region, there is a requirement that ERCOT issue public appeals for load reduction (See ERCOT Protocols Section 6.5.9.4). As the draft of EOP-004-2 is currently written, every Registered Entity in the ERCOT Region would have to file a report when ERCOT issues such an appeal. Such a requirement is overly burdensome and does not enhance the reliability of the BES. The Standard should require that the Reliability Coordinator file a report when it issues a public appeal to reduce load. Reporting Thresholds 1. See Paragraph 1 in the “Related to “Reportable Events” of Attachment 1” section, above. 2. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for “Damage or destruction to Critical Assets …” and “Damage or destruction of a [CCA]” to “Initial Indication the event was due to external cause or intentional human action.” 3. We support the SDT’s attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding” of ≥ 100 MW or “Loss of Firm load for ≥ 15 Minutes” that is ≥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Demand 1. The use of the term “Firm load” in the context of the

draft Standard seems inappropriate. “Firm load” is not defined in the NERC Glossary (although “Firm Demand” is defined). If the SDT intended to use “Firm Demand,” they should revise the draft Standard. If the SDT wishes to use the term “Firm load” they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as “Emergency Interruptible Load Service” (EILS). If the SDT intends that “Firm load” means load other than load which has agreed to be dropped, it should make that fact clear.] Comments to Attachment 2 1. The checkbox for “fuel supply emergency” should be deleted because it is not listed as an Event on Attachment 1. 2. There should be separation between “forced intrusion” and “Risk to BES equipment.” They are separate Events on Attachment 1. Comments to Guideline and Technical Basis The last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form “may be included or attached to the NERC report.” If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified.
Individual
Richard Salgo
NV Energy
Yes
Thankyou for responding to the stakeholder comments on this issue.
No
On my read of the Standard, R2 and R3 appear to be duplicative, and I can't really distinguish the difference between the two. The action required appears to be the same for both requirements. Even the Measures for these two sound similar. It is not clear to me what it means to "implement" other than to have evidence of the existence and understanding of roles and responsibilities under the "Operating Plan." I suggest elimination of R2 and inclusion of a line item in Measure 1 calling for evidence of the existence of an "Operating Plan" including all the required elements in R1.
Yes
Attachment 1 includes an item "Detection of a reportable cyber security incident." The reporting requirement is a report via Attachment 2 or the OE417 report form submittal. However, under CIP-008, to which this requirement is linked, the reporting is accomplished via NERC's secure CIPIS reporting tool. This appears to be a conflict in that the entity is directed to file reporting under CIP-008 that differs from this subject standard. Attachment 1 also includes a provision for reporting the "loss of firm load greater than or equal to 15 minutes in an amount of 200MW (or 300MW for peaks greater than 3000MW). This appears to be a rather low threshold, particularly in comparison with the companion loss of generation reporting threshold elsewhere in the attachment. The volume of reports triggered by this low threshold will likely lead to an inordinate number of filed reports, sapping NERC staff time and deflecting resources from more severe events that require attention. I suggest either an increase in the threshold, or the addition of the qualifier "caused by interruption/loss of BES facilities" in this reporting item. This qualifier would therefore exclude distribution-only outages that are not indicative of a BES reliability issue.
Group
SPP Standards Review Group
Robert Rhodes
Yes
Yes
No
The purpose of the reporting requirement should be clear either in the text of the requirements or through an explanation that is embodied in the language of the approved set of standards. This would be consistent with a “Results-based” architecture. What is lacking in the proposed language of this standard is recognition that registered entities differ in size and relevance of their impact on the Bulk Electric System. Also, events that are reportable differ in their impact on the registered entity. A “one-size fits all” approach to this standard may cause smaller entities with low impact on the grid to

take extraordinary measures to meet the reporting/timing requirements and yet be too “loose” for larger more sophisticated and impacting entities to meet the same requirements. Therefore, we believe language of the standard must clearly state the intent that entities must provide reports in a manner consistent with their capabilities from a size/reliability impact perspective and from a communications availability perspective. Timing requirements should allow for differences and consider these variables. Also, we would suggest including language to specifically exclude situations where communications facilities may not be available for reporting. For example, in situations where communications facilities have been lost, initial reports would be due within 6 hours of the restoration of those communication facilities. We would also suggest that Attachment 1 be broken into two distinct parts such that those events which must be reported within 1 hour standout from those events that have to be reported within 24 hours.

The inclusion of optional entities to which to report events in R1.3 introduces ambiguity into the standard that we feel needs to be eliminated. We propose the following replacement language for R1.3: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the Responsible Entity’s Regional Entity. We would also propose to incorporate the law enforcement and governmental or provincial agencies mentioned in R1.3 in Attachment 1 by adding them to the existing language for each of the event cells. For example, the first cell in that column would read: The parties identified pursuant to R1.3 and applicable law enforcement and governmental or provincial agencies within 1 hour of recognition of event. Similarly, the phrase ‘…and applicable law enforcement and governmental or provincial agencies…’ should be inserted in all the remaining cells in the 4th column.

Individual

Nathan Mitchell

American Public Power Association

Yes

APPA agrees that removal of the training requirement was an appropriate revision to limit the burden on small registered entities. However, APPA requests clarification from the SDT on the current draft of R4. If no event occurs during the calendar year, a drill or exercise of the Operating Plan communication process is required. APPA believes that if this drill or exercise is required, then it should be a table top verification of the internal communication process such as verification of phone numbers and stepping through a Registered Entity specific scenario. This should not be a full drill with requirements to contact outside entities such as law enforcement, NERC, the RC or other entities playing out a drill scenario. This full drill would be a major burden for small entities.

Yes

No

APPA echoes the comments made by Central Lincoln: We do not believe the SDT has adequately addressed the FERC Order to “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely “recognition” starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. APPA recommends the SDT evaluate a less burdensome requirement for smaller entities with reporting requirements in Attachment 1. This exception needs to address the fact that not all entities have 24 hour 7 day a week operating personnel. However, APPA cautions the SDT that changes to this standard may expose entities to reporting violations on DOE-OE-417 which imposes civil and criminal penalties on reporting events to the Department of Energy. APPA recommends that the SDT reach out to DOE for clarification of reporting requirements for DOE-OE-417 for small entities, asking DOE to change their reporting requirement to match EOP-004-2. If DOE cannot change their reporting requirement the SDT should provide an explanation in the guidance section of Reliability Standard EOP-004-2 that addresses these competing FERC/DOE directives.

Requirement R1: 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the following as appropriate: • Internal company personnel • The Responsible Entity’s Regional Entity • Law enforcement • Governmental or provincial agencies APPA believes that including the list of other

entities needing to be included in a process for communicating events under 1.3 may open this requirement up for interpretation. APPA requests that the SDT remove from the requirement the listing of; “Internal company personnel, The Responsible Entity’s Regional Entity, Law enforcement & Governmental or provincial agencies” and include these references in a guidance document. The registered entities need to communicate with the ERO and the RC if applicable for compliance with this standard and to maintain the reliability of the BES. Communication with other entities such as internal company personnel, law enforcement and the Regional Entity are expected, but do not impact the reliability of the BES. This will simplify the reporting structure and will not be burdensome to registered entities when documenting compliance. If this is not an acceptable solution, APPA suggests revising 1.3 to remove the wording “the following as appropriate” and add “other entities as determined by the Responsible Entity. Examples of other entities may include, but are not limited to:” Then it is clear that the list is examples and should not be enforced by the auditor. 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. APPA understands that the SDT is following the FERC order requiring a 90 day limit on updates to any changes to the plan. However, APPA believes that “updating the Operating Plan within 90 calendar days of any change…” is a very burdensome compliance documentation requirement. APPA reminds the SDT that including DPs in this combined standard has increased the number of small Responsible Entities that will be required to document compliance. APPA requests that the SDT combine requirement 1.4 and 1.5 so the Operating Plan will be reviewed and updated with any changes on a yearly basis. If this is not an acceptable solution, APPA suggests that the “Lower VSL” exclude a violation to 1.4. The thought being, a violation of 1.4 by itself is a documentation error and should not be levied a penalty. Attachment 1: Events Table APPA believes that the intent of the SDT was to mirror the DOE OE-417 criteria in reporting requirements. With the inclusion of DP in the Applicability, however, APPA believes the SDT created an unintended excessive reporting requirement for DPs during insignificant events. APPA recommends that a qualifier be added to the events table. In DOE OE-417 local electrical systems with less than 300MW are excluded from reporting certain events since they are not significant to the BES. APPA believes that the benefit of reporting certain events on systems below this value would not outweigh the compliance burden placed on these small systems. Therefore, APPA requests that the standard drafting team add the following qualifier to the Events Table of Attachment 1: “For systems with greater than 300MW peak load.” This statement should be placed in the Threshold for Reporting column for the following Events: BES Emergency requiring appeal for load reduction, BES Emergency requiring system-wide voltage reduction, BES Emergency requiring manual firm load shedding, BES Emergency resulting in automatic firm load shedding. This will match the DOE OE-417 reporting criteria and relieve the burden on small entities. Definition of “Risk to BES equipment”: The SDT attempted to give examples of the Event category “Risk to BES equipment” in a footnote. This footnote gives the Responsible Entity and the Auditor a lot of room for interpretation. APPA suggests that the SDT either define this term or give a triggering mechanism that the industry would understand. One suggestion would be “Risk to BES equipment: An event that forces a Facility Owner to initiate an unplanned, non-standard or conservative operating procedure.” Then list; “Examples include train derailment adjacent to BES Facilities that either could have damaged the equipment directly or has the potential to damage the equipment…” This will allow the entity to have an operating procedure linked to the event. If this suggestion is taken by the SDT then the Reporting column of Attachment 1 needs to be changed to: “The parties identified pursuant to R1.3 within 1 hour of initiating conservative operating procedures.”
Individual
Angela Summer
Southwestern Power Administration
Yes
No
One hour is not enough time to make these assessments for all of the six items in attachment 1. All timing requirements should be made the same in order to simplify the reporting process.
Individual

Michelle R D'Antuono
Ingleside Cogeneration LP
Yes
: Yes. Ingleside Cogeneration LP agrees that training on an incident reporting operations plan should be at the option of the entity. However, we recommend that a statement be included in the “Guideline and Technical Basis” section that encourages drills and exercises be coincident with those conducted for Emergency Operations. Since front-line operators must send out the initial alert that a reportable condition exists, such exercises may help determine how to manage their reporting obligations during the early stages of the troubleshooting process. This is especially true where a notification must be made within an hour of discovery – a very short time period.
No
Attachment 1 and requirement R3 are written in a manner which would seem to indicate that internal personnel and law enforcement personnel would have to be copied on the submitted form – either Attachment 2 or OE-417. We believe the intent is to submit such forms to the appropriate recipients only (e.g.; the ERO and the DOE). The requirement should be re-written to clarify that this is the case.
Yes
Yes. Any reporting that is mandated during the first hour of an event must be subject to close scrutiny. Many of the same resources that are needed to troubleshoot and stabilize the local system will be engaged in the reporting – which will impair reliability if not carefully applied. We believe that the ERO should reassess the need for any immediate reporting requirements on a regular basis to confirm that it provides some value to the restoration process.
We are encouraged that the 2009-01 project team has eliminated duplicate reporting requirements from multiple organizations and governmental agencies. Ingleside Cogeneration LP believes that there are further improvements that can be made in this area – as the remaining overlap seem to be a result of legalities and preferences, not technical issues. We would like to see an ongoing commitment by NERC for a single process that will consolidate and automate data entry, submission, and distribution.
Individual
Tim Soles
Occidental Power Services, Inc. (OPSI)
Yes
No
Attachment 1 and R3 require event reports to be sent to the ERO and the entity’s RC and to others “as appropriate.” Although this gives the entity some discretion, it might also create some “Monday morning quarterbacking” situations. This is especially true for the one hour reporting situations as personnel that would be responding to these events are the same ones needed to report the event. OPSI suggests that the SDT reconsider and clarify reporting obligations with the objective of sending initial reports to the minimum number of entities on a need-to-know basis.
Yes
Load Serving Entities that do not own or operate BES assets should not be included in the Applicability. In current posting, the SDT states that it includes LSEs based on CIP-002; however, if the LSE does not have any BES assets, CIP-002 should also not be applicable, because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Section 460 and 461; however, Section 461 also states “Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.” A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own or operate BES assets would seem appropriate. The proposed CIP-002 Version V has such a qualifier in that it applies to a “Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or Regional Reliability Standard • A UVLS program required by a NERC or Regional Reliability

Standard" The SDT should consider the same wording in the Applicability section of EOP-004-2 on order to be consistent with what will become the standing version of CIP-002 (Version 5).
Group
Dominion
Connie Lowe
Yes
Yes
Yes
Dominion appreciates the changes that have been made to increase the 1 hr reporting time to 24 hours.
There is still inconsistency in Attachment 1 vs. the DOE OE-417 form; in future changes, Dominion suggests align/rename events similar to that of the 'criteria for filing' events listed in the DOE OE-417, by working in coordination with the DOE. Minor comment; in the Background section, the drafting team refers to bulk power system (redline page 5; 1st paragraph and page 7; 2nd paragraph) rather than bulk electric system. The note in Attachment 1 states in part that "the affected Responsible Entity shall notify parties per R1 and …" Dominion believes the correct reference to be R3. In addition, capitalized terms "Event" and "Event Report" are used in this note. Dominion believes the terms should be non-capitalized as they are not NERC defined terms. Attachment 1 – "Detection of a reportable Cyber Security Incident – That meets the criteria in CIP-008". This essentially equates the criteria to be defined by the entity in its procedures as required by CIP-008 R1.1., additional clarification should be added in Attachment 1 to make this clear. The last sentence in Attachment 2 instructions should clarify that the email, facsimile and voice communication methods are for ERO notification only. Dominion continues to believe that the drill or exercise specified in R4 is unnecessary. Dominion suggests deleting this activity in the requirement.
Individual
Michael Lombardi
Northeast Utilities
Yes
Yes
Yes
- Incorporate NERC Event Analysis Reporting into this standard. Make the requirements more specific to functional registrations as opposed to having requirements applicable to "Responsible Entities". - The description of a Transmission Loss Event in Attachment 1 should be clarified to indicate that this only pertains to the loss of three or more BES elements due to a discrete event at a single point in time as opposed to a storm/weather event which may last 24 hours or more and cause the loss of three or more transmission facilities over the course of the weather event.
Group
Southern Comnpany
Antonio Grayson
No
Southern agrees with removing the training requirement of R4 from the previous version of the standard. However, Southern suggests that drills and exercises are also training and R4 in this revised standard should be removed in its entirety
No
These requirements as drafted in this revised standard potentially create a situation where an entity could be deemed non-compliant for both R2 and R3. For example, if a Responsible Entity included a reporting obligation in its Operating Plan, and failed to report an event, the Responsible Entity could

be deemed non-compliant for R2 for not “implementing” its plan and for R3 for not reporting the event to the appropriate entities. A potential solution to address this would be to add Requirement 1, Part 1.3 to Requirement 2 and remove Requirement 3 in its entirety. We also request clarification on Measure M3. Which records should have “dated and time-stamped transmittal records to show that the event was reported”? Some of the communication is handled via face-to-face conversation or through telephone conversation.
No
Southern request clarification on one of the entries in Attachment 1. The concern is with the last row on page 21 of Draft 3. What is the basis for “Voltage deviations”? The Threshold is ±10% sustained for ≥ 15 minutes. Is the voltage deviation based on the Voltage Schedule for that particular timeframe, or is it something else (pre-contingency voltage level, nominal voltage, etc.)? In addition, the second row of Attachment 1 lists “Damage or destruction of a Critical Cyber Asset per CIP-002” as a reportable event. The threshold includes “…intentional or unintentional human action” and gives us 1 hour to report. The term “damage” may be overly broad and, without definition, is not limited in any way. If a person mistypes a command and accidentally deletes a file, or renames something, or in any way changes anything on the CCA in error, then this could be considered “damage” and becomes a reportable event. The SDT should consider more thoroughly defining what is meant by “damage”. Should it incorporate the idea that the essential functions that the CCA is performing must be adversely impacted? Lastly, no event should have a reporting time shorter than at the close of the next business day. Any reporting of an event that requires a shorter reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity.
Southern has the following comments: (1) In Requirement R1.4, we request the SDT to clarify what is meant by the term “assets”? (2) If requirement 4 is not deleted, should we have to test every possible event described in our Operating Plan or each event listed in Attachment 1 to verify communications? (3) In the last paragraph of the “Summary of Key Concepts” section on page 6 of Draft 3, there is a statement that “Real-time reporting is achieved through the RCIS…” The only reporting required on RCIS by the Standards is for EEAs and TLRs. Please review and modify this language as needed. (4) Evidence Retention (page 12 of Draft 3): The 3 calendar year reference has no bearing on a Standard that may be audited on a cycle greater than 3 years. (5) In the NOTE for Attachment 1 (page 20 of Draft 3), what is meant by “periodic verbal updates” and to whom should the updates be made? (6) There are Prerequisite Approvals listed in the Implementation Plan. Is it appropriate to ask industry to vote on this Standard Revision that has a prerequisite approval of changes in the Rules of Procedure that have not been approved? (7) We believe the reporting of the events in Attachment 1 has no reliability benefit to the Bulk Electric System. We suggest that Attachment 1 should be removed.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5 could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards. Additionally, it is debatable whether the destruction of, for example, one relay would be a

reportable incident given the proposed language. Related to “Reportable Events” of Attachment 1: 1. The “Purpose” section of the Standard indicates it is designed to require the reporting of events “with the potential to impact reliability” of the BES. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting. 3. The word “Significantly” in item ii) of footnote 1 introduces an element of subjectivity. What is “significant” to one person may not be significant to someone else. 4. The word “unintentional” in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to “Damage or destruction of BES equipment” (2) removing the footnote and (3) replacing the existing “Threshold for Reporting” with the following language: “Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)” 5. One reportable event is “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. 6. One reportable event is “Damage or destruction of Critical Asset per CIP-002.” The SDT should define the term “Damage” in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. Normal “damage” can occur on a CA that should not be reportable (e.g. the screwdriver example, above). 7. For the event called “BES Emergency requiring public appeal for load reduction,” the SDT should make it clear who should report such an event. For example, in the ERCOT Region, there is a requirement that ERCOT issue public appeals for load reduction (See ERCOT Protocols Section 6.5.9.4). As the draft of EOP-004-2 is currently written, every Registered Entity in the ERCOT Region would have to file a report when ERCOT issues such an appeal. Such a requirement is overly burdensome and does not enhance the reliability of the BES. The Standard should require that the Reliability Coordinator file a report when it issues a public appeal to reduce load. Reporting Thresholds 1. See Paragraph 1 in the “Related to 'Reportable Events' of Attachment 1” section, above. 2. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for “Damage or destruction of Critical Asset…” and “Damage or destruction of a [CCA]” to “Initial Indication the event was due to external cause or intentional human action.” 3. We support the SDT’s attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding” of ≥ 100 MW or “Loss of Firm load for ≥ 15 Minutes” that is ≥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Load 1. The use of the term “Firm load” in the context of the draft Standard seems inappropriate. “Firm load” is not defined in the NERC Glossary (although “Firm Demand” is defined). If the SDT intended to use “Firm Demand,” they should revise the draft Standard to use that language. If the SDT wishes to use the term “Firm load” they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as “Emergency Interruptible Load Service” (EILS). If the SDT intends that “Firm load” means load other than load which has agreed to be dropped, it should make that fact clear.] Comments to Attachment 2 1. The checkbox for “fuel supply emergency” should be deleted because it is not listed as an Event on Attachment 1. 2. There should be separation between “forced intrusion” and “Risk to BES equipment.” They are separate Events on Attachment 1. Comments to Guideline and Technical Basis The last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form “may be included or attached to the NERC report.” If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified.

Group
FirstEnergy

Sam Ciccone
Yes
FirstEnergy supports this removal and thanks the drafting team.
Yes
Yes
Although we agree with the timeframes for reporting, we have other concerns as listed in our response to Question 4.
1. Attachment 1 – Regarding the 1st event listed in the table, “Destruction of BES Equipment” and its accompanying Footnote 1, we believe that this event should be broken into two separate events that incorporate the specifics in the footnote as follows: a. “Destruction of BES equipment that associated with an IROL per FAC-014-2.” Regarding the 1st event we have proposed – We have proposed this be made specific to IROL as stated in Footnote 1 part i. Also, we believe that only the RC and TOP would have the ability to quickly determine and report within 1 hour if the destruction is associated with an IROL. The other entities listed would not necessarily know if the event affects and IROL. Therefore, we also propose that the Entities with Reporting Responsibilities (column 2) be revised to only include the RC and TOP. b. "Destruction of BES equipment that removes the equipment from service.” Regarding the 3rd event we have proposed – We have proposed this be made specific to destruction of BES equipment that removes the equipment from service as stated in Footnote 1 part iii. Also, the other part of footnote 1 part iii which states “Damaged or destroyed due to intentional or unintentional human action” is not required since it is covered in the threshold for reporting. Also the term “Damaged” in this part iii is not appropriate since these events are limited to equipment that has been destroyed. We also propose that the Entities with Reporting Responsibilities (column 2) for this event would remain the same as it states now since any of those entities may observe out of service BES equipment. Regarding part ii of footnote 1, we do not believe that this event needs to be separated. Regarding the phrase “significantly affects the reliability margin of the system be clarified so that it is not left up to the entity to interpret a “significant” affect. Lastly, since we have incorporated parts i and iii into the two separate events and removed part ii as proposed above, the only statement that needs to be left in the Footnote 1 is: “Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).” 2. Attachment 1 – We ask that the team add an “Event #” column to the table so that each of the events listed can be referred to by #, such as Event 1, Event 2, etc. 3. Attachment 1 – Event titled “Damage or destruction of a Critical Cyber Asset per CIP-002”, the proposed threshold for reporting seems incomplete. We suggest the threshold for this event match the threshold for the Critical Asset event which states: “Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.” 4. Attachment 1 – Events titled “Damage or destruction of a Critical Assets per CIP-002” and “Damage or destruction of a Critical Cyber Asset per CIP-002” seem ambiguous due to the term “damage”. We suggest removal of “damage” or clarity as to what is considered a damaged asset. 5. VSL Table – Instead of listing every entity, it may be more efficient to simply say “The Responsible Entity” in the VSL for each requirement. 6. Guideline and Technical Basis section – This section does not provide guidance on each of the requirements of the standard. We suggest the team consider adding guidance for the requirements.
Group
PPL Electric Utilities and PPL Supply Organizations`
Annette M. Bannon
Yes
Yes
Our comments center around the footnotes and events 'Destruction of BES equipment' and 'Loss of Off-site power to a nuclear generating plant'. We request the SDT consider adding a statement to the standard that acknowledges that not all registered entities have visibility to the information in the footnotes. E.G. Destruction of BES equipment. A GO/GOP does not necessarily know if loss of specific

BES equipment would affect any IROL and therefore would not be able to consider this criteria in its reporting decision. Loss of BES equipment would be reported to the BA/RC and the BA/RC would know of an IROL impact and the BA/RC is the appropriate entity to report. We request the SDT consider the information in the footnotes for inclusion in the table directly. Consider Event 'Destruction of BES equipment'. Is footnote 1 a scoping statement? Is it part of the threshold? Is it the impact? Is it defining Destruction? If the BES equipment was destroyed by weather and does not affect an IROL, then is no report is needed? Alternatively, do you still apply the threshold and say it was external cause and therefore report? We suggest including a flowchart on how to use Attachment 1 with an example. The flowchart would explain the order in which to consider the event and the threshold, and footnotes if they remain. Regarding Attachment 1 Footnote 1 'do not report copper theft...unless it degrades the ability of equipment to operate correctly.', is this defining destruction as not operating correctly ? or is the entirety of footnote 1 a definition of destruction? Regarding Attachment 1 Footnote 1, iii, we request this be changed for consistency with the Event and suggest removing damage from the footnote. i.e. The event is 'destruction' whereas the footnote says 'damaged or destroyed'. The standard does not provide guidance on damage vs destruction which could lead to differing reporting conclusions. Is the reporting line out of service, beyond repair, or is it timeframe based? Regarding Attachment 1 Footnote 2 ' to steal copper... unless it affects the reliability of the BES', is affecting the reliability of the BES a consideration in all the events? PPL believes this is the case and request this statement be made. This could be included in the flowchart as a decision point. Regarding Event 'Loss of Off-site power to a nuclear generating plant', the threshold for reporting does not designate if the off-site loss is planned and/or unplanned – or if the reporting threshold includes the loss of one source of off-site power or is the reporting limited to when all off-site sources are unavailable. PPL recommends the event be 'Total unplanned loss of offsite power to a nuclear generating plant (grid supply)' Thank you for considering our comments.
Group
CenterPoint Energy
John Brockhan
Yes
No
CenterPoint Energy believes the current R2 is unnecessary and duplicative. Upon reporting events as required by R3, entities will be implementing the relevant parts of their Operating Plan that address R1.1 and R1.2. This duplication is clear when reading M2 and M3. Acceptable evidence is an event report. R2 should be modified to remove this duplicative requirement.
No
CenterPoint Energy agrees with the revision that allows more time for reporting some events; however, some 1 hour requirements remain. The Company does not agree with this timeframe for any event.
CenterPoint Energy appreciates the SDT's consideration of comments and removal of the term, Impact Event. However, the Company still suggests removing the phrase "with the potential to impact" from the purpose as it is vast and vague. An alternative purpose would be "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events that impact reliability and their causes if known". The focus should remain on those events that truly impact the reliability of the BES. CenterPoint Energy remains very concerned about the types of events that the SDT has retained in Attachment 1 as indicated in the following comments: Destruction of BES Equipment – The loss of BES equipment should not be reportable unless the reliability of the BES is impacted. Footnote 5, iii should be modified to tie the removal of a piece of equipment from service back to reliability of the BES. Risk to BES equipment: This Event is too vague to be meaningful and should be deleted. The Event should be modified to "Detection of an imminent physical threat to BES equipment". Any reporting time frame of 1 hour is unreasonable; Entities will still be responding to the Event and gathering information. A 24 hour reporting time frame would be more reasonable and would still provide timely information. System Separation: The 100 MW threshold is too low for a reliability impact. A more appropriate threshold is 500 MW. Loss of Monitoring or all voice communication capability: The two elements of this Event should be separated for clarity as follows: "Loss of monitoring of Real-Time conditions" and "Loss of all voice communication capability."

Individual
James Sauceda
Energy Northwest - Columbia
Yes
Yes
No
Energy Northwest - Columbia (ENWC) has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. ENWC would like the word "recognition" in the statement that reads, "recognition of events," be replaced by "confirmation" as in "confirmed event." Also, we would like clarification as to when the 1 hour clock starts. Please consider changing recognition in "within 1 hour of recognition of event" and incorporating in "confirmation."
1. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Energy Northwest understands that the DSR SDT evaluated the use of the word “source” but dismissed the use in favor of “supply” with the justification “[that] ‘supply’ encompasses all sources”. Energy Northwest suggests that the word “source” is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to “one or more” Energy Northwest believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of “one or more” will ensure that all potential events (regardless of configuration of off-site power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs. Energy Northwest proposes that the loss of an off-site power source be revised to an “unplanned” loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance. Although the loss of one off-site power source may not result in a nuclear generating unit trip, Energy Northwest agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows: Event: Unplanned loss of any off-site power source to a Nuclear Power Plant Entity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements. Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. 2. Please consider changing "Operating Plan" with "Procedure(s)". Procedures extend beyond operating groups and provide guidance to the entire company.
Group
Electric Compliance
Tom McElhinney
Yes
Yes
Yes
The concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards and so this may cause confusion. Recommend modifying to be in accordance with Version 5. Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. We recommend modifying the language to insure

nuisance reporting is minimized. One reportable event is, “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope. For example, a fan on a transformer can be destroyed because a technician drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. Proposed Footnote: BES equipment that become damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service that i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii). Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). The word “Significantly” in item ii) of footnote 1 and “as appropriate” in section 1.3 introduces elements of subjectivity. What is “significant” or “appropriate” to one person may not be to someone else. In section 1.4, we believe that revising the plan within 90 days of “any” change should be changed to 180 days or else classes of events should be made so that only substantial changes are required to made within the 90 day timeframe.
Individual
Scott Berry
Indiana Municipal Power Agency
No
IMPA does not believe that R4 is necessary. In addition, if a drill or exercise is used to verify the communication process, some of the parties listed in R1.3 may not want to participate in the drill or exercise every 15 months, such as law enforcement and governmental agencies. IMPA would propose a contacting these agencies every 15 months to verify their contact information only and updating their information in the plan as needed, without performing a drill or exercise.
No
Both requirements seem to be implementing the Operating Plan which means R3 should be a bullet under R2 and not a separate requirement. IMPA supports making R2 and R3 one requirement and eliminating the current R3 requirement. In addition, R2 needs to be clarified when addressing an actual event. IMPA recommends saying “an actual event that meets the criteria of Attachment 1.”
No
IMPA believes that some of the times may not be aggressive enought that are related to generation capacity shortages. In addition, IMPA believes clarity needs to be added when saying within 1 hour of recognition of event. For example, A fence cutting may not be discovered for days at a remote substation and then a determination has to be made if it was “forced intrusion” – Does that one hour apply once the determination is made that is was “forced intrusion” or from the time the discovery was made? Some of the 1 hour time limits can be expanded to allow for more time, such as forced intrusion, destruction of BES equipment, Risk to BES equipment, etc.
Many of the items listed in Attachment 1 are onerous and burdensome when it comes to making judgments or determinations. What one may consider “Risk to BES equipment” another person may not make the same determination. Clarity needs to be added to make the events easier to determine and that will result in less issues when it comes to compliance audits. IMPA does not understand the usage of the terms Critical Asset and Critical Cyber Asset as they will be retired with CIP version 5. IMPA believes the data retention requirements are way too complicated and need to be simplified. It seems like it would be less complicated if one data retention period applied to all data associated with this standard. On “public appeal”, in the threshold, the descriptor “each” should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event?
Individual
Maggy Powell

Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.
Yes
Yes, we support removal of the training requirement.
Yes
While we support the delineation of the different activities associated with implementation and reporting, further clarification would be helpful. R1. 1.3: As currently written, it is somewhat confusing, in particular the use of the qualifier “as appropriate”. In addition, the use of the word “communicating” to capture both reporting to reliability authorities and notifying others may leave the requirement open to question. Below is a proposed revision: 1.3 A process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and for communicating to others as defined in the Responsible Entity’s Operating Plan, such as: • Internal company personnel • The Responsible Entity’s Regional Entity • Law Enforcement • Government or provincial agencies R1, 1.4: the last phrase of the requirements seems to be leftover from an earlier version. The requirement should end after the word “Plan”. R1, 1.5: “Process” should not be capitalized. While we understand the intent of the draft language and appreciate the effort to streamline the requirements, we propose an adjusted delineation below that we feel tracks more cleanly to the structure of a compliance program. Proposed revised language: R2. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.1 and 1.2 for an actual event(s). M2. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event. Evidence may include, but is not limited to, an submitted event report form (Attachment 2) or a submitted OE-417 report, operator logs, or voice recording. R3. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.4 and 1.5. M3. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.4 and 1.5. Evidence may include, but is not limited to, dated documentation of review and update of the Operating Plan. R4. Each Responsible Entity shall verify (through implementation for an actual event, or through a drill, exercise or table top exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification. M4. The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill, exercise, or table top exercise may be used as evidence to meet this requirement. The time period between verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification.
Yes
We agree with the change to the reporting times in Attachment 1. While this is an improvement, other concerns with the language in the events table language remain. Please see additional details below: General items: • All submission instructions (column 4 in Events Table) should qualify the recognition of the event as “of recognition of event as a reportable event.” • Is the ES-ISAC the appropriate contact for the ERO given that these two entities are separate even though they are currently managed by NERC? In addition, are the phone numbers in the Attachment 1 NOTE accurate? Is it possible they will change in a different cycle than the standard? Specific Event Language: • Destruction of BES Equipment, footnote: Footnote 1, item iii confuses the clarification added in items i. and ii. Footnote 1 should be modified to state BES equipment that (i) an entity knows will affect an IROL or has been notified the loss affects an IROL; (ii) significantly affects the reserve margin of a Balancing Authority or Reserve Sharing Group. Item iii should be dropped. • Damage or destruction of Critical Asset per CIP-002: Within the currently developing revisions to CIP-002 (version 5), Critical Asset will be retired as a glossary term. As well as addressing the durability of this event category, additional delineation is needed regarding which asset disruptions are to be reported. A CA as currently defined incorporates assets in a broad perspective, for instance a generating plant may be a Critical Asset. As currently written in Attachment 1, reporting may be required for unintended events, such as a boiler leak that takes a plant offline for a minor repair. Event #1 – Destruction of BES Equipment – captures incidents at the relevant equipment regardless of whether they are a Critical Asset or not. We recommend dropping this event. However, if reference

to CIP-002 assets remains, it will be important to capture reporting of the events relevant to reliability and not just more events. • Damage or destruction of a Critical Cyber Asset per CIP-002: Because CCAs are defined at the component level, including this trigger is appropriate; however, as with CAs, the CCA term is scheduled to be retired under CIP-002 version 5. • Forced Intrusion: The footnote confuses the goal of including this event category. In addition, “forced” doesn’t need to define the incident. Constellation proposes the following to better define the event: Intrusion that affects or attempts to affect the reliable operation of the BES (1) (1) Examples of "affecting reliable operation of the BES are": (i) device operations, (ii) protective equipment degradation, (iii) communications systems degradation including telemetered values and device status. • Risk to BES equipment: This category is too vague to be effective and the footnote further complicates the expectations around this event. The catch all concept of reporting potential risks to BES equipment is problematic. It’s not clear what the reliability goal of this category is. Risk is not an event, it is an analysis. How are entities to comply with this “event”, never mind within an hour? It appears that the information contemplated within this scenario would be better captured within the greater efforts underway by NERC to assess risks to the BES. This event should be removed from the Attachment 1 list in EOP-004. • BES Emergency requiring system-wide voltage reduction: the Entity with Reporting Responsibility should be limited to RC and TOP. • Voltage deviations on BES Facilities: The Threshold for Reporting language needs more detail to explain +/- 10% of what? Proposed revision: ± 10% outside the voltage schedule band sustained for ≥ 15 continuous minutes • IROL Violation (all Interconnections) or SOL Violation (WECC only): Should “Interconnections” be capitalized? • Transmission loss: The reporting threshold should provide more specifics around what constitutes Transmission Facilities. One minor item, under the Threshold for Reporting, “Three” does not need to be capitalized.
Background Section: The background section in this revision of EOP-004 reads more like guidance than a background of the development of the event reporting standard. Because of the background remains as part of the standard, the language raises questions as to role it plays relative to the standard language. For instance, the Law Enforcement Reporting section states:”Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES.” It’s not clear how “potential to impact to a wider area of the BES” is defined and where it fits into the standard. As well, and perhaps more problematic, is the Reporting Hierarchy for Reportable Events flow chart. While the flow chart concept is quite useful as a guidance tool, the flow chart currently in the Background raises questions. For instance, the Procedure to Report to Law Enforcement sequence does not map to language in the requirements. Further, Entities would not know about the interaction between law enforcement agencies. Please see additional recommended revisions to the requirement language and to the Events Table in the Q2 and Q3 responses. Attachment 2: Event Reporting Form: The review of the form is one of the many aspects to compare with the developments within the Events Analysis Process (EAP) developments. We support the effort to create one form for submissions. The recent draft EAP posted as part of Planning Committee and Operating Committee agendas includes a form requiring a few bits of additional relevant information when compared to the EOP-004 form. This may be a valuable approach to avoid follow up inquiries that may result if the form is too limited. We suggest that consideration be given to the proposed EAP form. One specific note on the Proposed EOP-004 Attachment 2: The “Potential event” box in item 3 should be eliminated to track with the removal of the “Risk to the BES” category.
Group
Salt River Project
Brenton Lopez
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the NERC Event Analysis process, but there is some duplication of efforts. EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be

duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards. Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. Related to “Reportable Events” of Attachment 1: 1. The “Purpose” section of the Standard indicates it is designed to require the reporting of events “with the potential to impact reliability” of the BES. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting. 3. The word “Significantly” in item ii) of footnote 1 introduces an element of subjectivity. What is “significant” to one person may not be significant to someone else. 4. The word “unintentional” in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to “Damage or destruction of BES equipment” (2) removing the footnote and (3) replacing the existing “Threshold for Reporting” with the following language: “Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)” 5. One reportable event is, “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. 6. One reportable event is, “Damage or destruction of Critical Asset per CIP-002.” The SDT should define the term “Damage” in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. Normal “damage” can occur on a CA that should not be reportable (e.g. the screwdriver example, above). Reporting Thresholds 1. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for “Damage or destruction to Critical Assets …” and “Damage or destruction of a [CCA]” to “Initial Indication the event was due to external cause or intentional human action.” 2. We support the SDT’s attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding” of ≥ 100 MW or "Loss of Firm load for ≥ 15 Minutes” that is ≥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Demand 1. The use of the term “Firm load” in the context of the draft Standard seems inappropriate. “Firm load” is not defined in the NERC Glossary (although “Firm Demand” is defined). If the SDT intended to use “Firm Demand,” they should revised the draft Standard. If the SDT wishes to use the term “Firm load” they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as “Emergency Interruptible Load Service” (EILS). If the SDT intends that “Firm load” means load other than load which has agreed to be dropped, it should make that fact clear.] Comments to Attachment 2 1. The checkbox for “fuel supply emergency” should be deleted because it is not listed as an Event on Attachment 1. 2. There should be separation between “forced intrusion” and “Risk to BES equipment.” They are separate Events on Attachment 1. Comments to Guideline and Technical Basis The last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form “may be included or attached to the NERC report.” If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified.
Individual

Michael Brytowski
Great River Energy
No
We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard, in particular to requirement R4. The use of the words “or through a drill or exercise” still implies that training is required if no actual event has occurred. When you conduct a fire “drill” you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually.
No
Requirement R2 requires Responsible Entities to implement the various subrequirements in R1. We believe it is unnecessary to state that an entity must implement their Operating Plan in a separate requirement. Having a separate requirement seems redundant. If the processes in the Operating Plan are not implemented, the entity is non-compliant with the standard. There doesn’t need to be an extra requirement saying entities need to implement their Operating Plan.
Yes
For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting.
Individual
Christine Hasha
Electric Reliability Council of Texas, Inc.
Yes
Yes
No
Destruction of BES equipment: 1. Request that the term “destruction” be clarified. Damage or destruction of Critical Asset per CIP-002: 1. Request that the terms “damage” and “destruction” be clarified. 2. Is the expectation that an entity report each individual device or system equipment failure or each mistake made by someone administering a system? 3. Request that “initial indication of the event” be changed to “confirmation of the event”. Event monitoring and management systems may receive many events that are determined to be harmless and put the entity at no risk. This can only be determined after analysis of the associated events is performed. Damage or destruction of a Critical Cyber Asset per CIP-002: 1. Request that the terms “damage” and “destruction” be clarified. 2. Is the expectation that an entity report each individual device or system equipment failure or each mistake made by someone administering a system? 3. Request that “initial indication of the event” be changed to “confirmation of the event”. Event monitoring and management systems may receive many events that are determined to be harmless and put the entity at no risk. This can only be determined after analysis of the associated events is performed. Risk to BES equipment: Request that the terms “risk” be clarified.
Individual
Darryl Curtis
Oncor Electric Delivery Company LLC
Yes

No

NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting.

Yes

NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting.

Group

Kansas City Power & Light

Michael Gammon

Yes

No

Requirement R1.1 is confusing regarding the “process for identifying events listed in Attachment 1”. Considering Attachment 1, the Events Table, already identifies the events required for reporting, please clearly describe in the requirement what the “process” referred to in requirement R1.1 represents.

No

The reportable events listed in Attachment 1 can be categorized as events that have had a reliability impact and those events that could have a reliability impact. The listed events that could have a reliability impact should have a 24 hour reporting requirement and the events that have had a reliability impact are appropriate at a 1 hour reporting. The following events with a 1 hour report requirement are recommended to change to 24 hour: Forced Intrusion and Risk to BES Equipment. In addition, the Attachment 1 Events Table is incomplete as many of the listed events are incomplete regarding reporting time requirements and event descriptions. Also recommend removing (ii) from note 5 with event “Destruction of BES equipment” as this part of the note is already described in the event description and insinuates reporting of equipment losses that do not have a reliability impact. The events, “Damage or destruction of Critical Asset per CIP-002” and “Damage or destruction of a Critical Cyber Asset per CIP-002”, does not have sufficient clarity regarding what that represents. A note similar in nature to Note 5 for BES equipment is recommended.

The implementation plan indicates that much of CIP-008 is retained. The reporting requirements in CIP-008 and the required reportable events outlined in Attachment 1 are an overlap with CIP-008-3 R1.1 which says “Procedures to characterize and classify events as reportable Cyber Security Incidents” and CIP-008-3 R1.3 which requires processes to address reporting to the ES-ISAC. There is also a NERC document titled, Security Guideline for the Electricity Sector: Threat and Incident Reporting, which is a guideline to “assist entities to identify and classify incidents for reporting to the ES-ISAC”. The SDT should consider the content of the Security Guideline for the Electricity Sector: Threat and Incident Reporting when considering the reporting requirements proposed EOP-004. The efforts to incorporate CIP-008 into EOP-004 are insufficient and will result in serious confusion between proposed EOP-004 and CIP-008 and reporting expectations. Considering the complexity CIP incident reporting and the interests of ES-ISAC, it may be beneficial to leave CIP-008 out of the proposed EOP-004 and limit EOP-004 to the reporting interests of NERC. The flowchart states, “Notification Protocol to State Agency Law Enforcement”. Please correct this to, “Notification to State, Provincial, or Local Law Enforcement”, to be consistent with the language in the background section part, “A Reporting Process Solution – EOP-004”. Measure 4 is not clear enough regarding the extent to which drills should be performed. Does the measure mean that all events in the events list need to be drilled or is drilling a subset of the events list sufficient? Please clearly indicate the extent of drilling that is required or clearly indicate in the requirement the extent of the drills to be performed is the responsibility of the Responsible Entity to identify in their “processes”. Evidence Retention – it is not clear what the phrase “prior 3 calendar years” represents in the third paragraph of this section

regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of “since the last audit for 3 calendar years” for R1 and M1? VSL for R2 under Severe regarding R1.1 may require revision considering the comment regarding R1.1 in item 2 previously stated. In addition, the VRF for R2 is MEDIUM. R2 is administrative regarding the implementation of the requirements specified in R1. Documentation and maintenance should be considered LOWER. There is no VSL for R4 and a VSL for R4 needs to be proposed.

Additional Comments Received:

Southwestern Power Administration's Comments for Project 2009-1
Submitted by Angela Summer

"Attachment 1 contains elements that do not need to be included, and redundant elements such as:

Forced intrusion at BES Facility - A facility break-in does not necessarily mean that the facility has been impacted or has undergone damage or destruction.

Detection of a reportable Cyber Security Incident per CIP-008 - If entities are addressing this requirement in CIP-008, why do so again in
EOP-004 (Attachment 2-EOP-004, Reporting Requirement number 5)?

Transmission Loss: Each TOP that experiences transmission loss of three or more facilities - This element should be removed or rewritten so that it only applies when the loss includes a contingent element of an IROL facility."