Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Modifications to Address CIP Exceptional Circumstances
Comment Period Start Date:	2/10/2017
Comment Period End Date:	3/13/2017
Associated Ballots:	

There were 51 sets of responses, including comments from approximately 128 different people from approximately 97 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Southwest Power Pool, Inc. (RTO)	Charles Yeung	2	SPP RE	SRC CIP March	Charles Yeung	SPP	2	SPP RE
					Ben Li	IESO	2	NPCC
					Mark Holman	PJM	2	RF
					Matt Goldberg	ISONE	2	NPCC
					Lori Spence	MISO	2	MRO
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC

					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO

					Chuck Lawrence	American Transmission Company	1	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Stewart Dover	Lafayette Utilities System	2	SPP RE

					John Allen	City Utilities of Springfield, Missouri	4	SPP RE
					Tara Lightner	Sunflower	1	SPP RE
Public Service Enterprise Group	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

While the NSRF agrees with identifying those requirements impacted by CECs, we do not support revising the standards to add CEC exclusions as suggested. There is significant overhead to the Industry every time a standard is opened. It can also lead to more questions and additional standards changes to address questions raised by the Commission. There will also be additional work in the compliance arena as the RSAWS will likely ask to document all CEC events and whether they were properly assessed, or to provide proof that no CEC cases occurred.

In an effort to stabilize the CIP standards, we would recommend using NERC's new Compliance Guidance process. NERC should ask the CIPC to develop simple implementation guidance outlining how Registered Entities can document and report CECs to get Compliance Exception treatment. NERC should also draft a companion CMEP Practice Guide to enable expeditious Compliance Exception handling of access issues occurring during a CEC.

Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE recognizes there are instances where declaring a CIP Exceptional Circumstance (CEC) is appropriate and the Standard Drafting Team (SDT) did identify such circumstances. Given the definition of CEC, however, Texas RE recommends the SDT not extend the current application of CIP Exceptional Circumstances to the additional standards identified. The definition of CEC specifically includes situations that "involve[] or threaten[] to involve . . .an imminent or existing hardware, software, or equipment failure." That is to say, under the SDT proposal, an entity experiencing a hardware failure or system outage may declare a "CIP Exceptional Circumstance" and avoid Standard requirements that are expressly designed to encourage

redundant controls and backup systems precisely in such circumstances. As a result, the proposal appears designed solely to reduce compliance risk rather than encourage sound “defense-in-depth” practices.

Consider the proposal to extend the CEC language to CIP-006 R1, P1.8, concerning the logging of physical entry into a Physical Security Perimeter. Currently, registered entities routinely accomplish this logging function through electronic devices such as card readers. However, if these devices fail, entities are expected to deploy secondary physical controls to control access. In particular, registered entities routinely post security personnel at perimeters to log entry and exit during an outage. Under the SDT’s proposal, however, such entities would no longer be required to deploy such physical personnel to log access. Rather, they could declare a CEC during the duration of the hardware failure. The net effect is to reduce the overall protections for physical assets. The same logic extend to the retention of physical access logs and visitor logs under CIP-006 R1, P1.9 and CIP-006 R2, P.2.3, respectively.

A similar rationale applies to the extension of the CEC language to the CIP-004 R3, P. 3.5 Personal Risk Assessment (PRA) requirement. In Texas RE’s experience, the best practice for entities handling the PRA process is to ensure sufficient lead-time for PRA updates and other actions. Given the seven-year review window, entities should be encouraged to perform any and all reviews with sufficient lead time so that unforeseen circumstances and events do not result in a possible violation. Again, the SDT’s proposal reduces this incentive. Critically, the SDT’s proposal applies to all entity personnel and contractors. Given the potentially broad nature of an “imminent or existing hardware, software, or equipment failure,” an entity could avoid performing background diligence on any contractor entering its facilities to perform any unscheduled, non-routine maintenance. This appears overbroad and beyond the SDT’s intent. Texas RE has identified similar issues with CIP-007 and CIP-010 listed by the SDT above.

In the alternative, Texas RE recommends the SDT revise the definition of CEC to remove “an imminent or existing hardware, software, or equipment failure”. This properly aligns the focus of the CEC definition with the rationale statements provided by the SDT for the examples above.

Texas RE also recommends clarifying entities’ compliance expectations around CECs. In particular, Texas RE has encountered a number of entities that view a CIP Exceptional Circumstances declaration as exculpatory without more. Rather, if an entity declares a CIP Exceptional Circumstance, the entity must fully document and justify the scope and duration of the event, as well as establish that regular controls were in place and appropriate elements of its emergency response plan were implemented. This proceeding is an opportunity to clarify these expectations.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.

Likes 0	
Dislikes 0	

Response

Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2, Group Name SRC CIP March

Answer	No
Document Name	

Comment

While we agree with identifying those requirements impacted by CECs, we disagree with revising the standards to add CEC exclusions as suggested. There is significant overhead to the Industry every time a standard is opened. It can also lead to more questions and additional standards changes to address questions raised by the Commission. There will also be additional work in the compliance arena as the RSAWS will likely ask to document all CEC events and whether they were properly assessed, or to provide proof that no CEC cases occurred.

In an effort to stabilize the CIP standards, we would recommend using NERC's new Compliance Guidance process. NERC should ask the CIPC to develop simple Implementation Guidance outlining how Registered Entities can document and report CECs to get Compliance Exception treatment. NERC should also draft a companion CMEP Practice Guide to enable expeditious Compliance Exception handling of access issues occurring during a CEC.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees personnel risk assessments can’t be performed on first responders and some relevant vendors.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
It is impractical to refuse entry to an emergency responder or SME due to the lack of a PRA or have to wait to validate a PRA. This would potentially hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
CIP Exceptional Circumstance was approved for this requirement in previous versions. If there is an emergency situation as described by the definition of a CIP Exceptional Circumstance, there isn’t time to get a background check completed before allowing rescue/medical personnel in to assist.	

Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

AZPS respectfully requests that the addition of the existing CIP Exceptional Circumstance language be applied to CIP-004 R3, Parts 3.1 through 3.5 and be placed at the beginning of the opening phrase. AZPS believes that the performance of all Parts under Requirement R3 would not be feasible during a CIP Exceptional Circumstance, e.g., companies would not seek to confirm the identity of paramedics responding to the medical emergency of an employee.

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement parts. Specifically, it is important to highlight that for CIP-004-5, R3, the Personnel Risk Assessments (PRA) may not be able to be performed on first responders, whether they are entity personnel or external contractors, vendors or emergency personnel, within a reasonable period of time prior to authorizing unescorted physical access during a CIP exceptional circumstance.

CIP Exceptional Circumstances are declared in emergency situations to protect life, safety and the reliability of the BES. Entities are given the flexibility to design programs that articulate how to declare and respond to a CEC. That flexibility should extend to the entity’s ability to appoint or allow individuals with appropriate skills to assist with recovery to gain access as necessary to mitigate risk.

Additionally, during a major BES Cyber System event there may be a need to provide access to the vendor to address the system issue where obtaining a PRA for electronic access would prohibit addressing maintaining reliability. The seven (7) year criminal history checks may may require searches across multiple jurisdictions for a single individual based on resident history. Jurisdications are not required to respond to requests for criminal history information within a specified service level agreement (SLA). In addition, some jurisdications require fingerprinting or other means to authenticate the criminal history of an individual, which would extend the amount of time required to complete the PRA.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

Recommend changing the order of the wording to:

“Process to ensure, except during CIP Exceptional Circumstances, that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.”

Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

Requirement 3 of CIP-004-6 Guidelines and Technical Basis already referenced CEC:”Each Responsible Entity shall ensure a personnel risk assessment … except for program specified exceptional circumstances”.

Can a requirement be suspended for CEC even if it does not allow CEC explicitly?

What if the G&TB makes a reference to CEC but not the requirement?

What should be the procedure for reporting the CEC in a case where CEC is not explicitly mentioned in the requirement?

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this is consistent with CIP-004 R2, Part 2.2. This exception is needed to address instances where first responders or others providing assistance in a CEC require access. In the event of a CEC, obtaining a personnel risk assessment prior to allowing access may cause risk to life or property. Additionally, in the event of a CEC, obtaining a PRA for vendors involved with restoration may not be practical. ERCOT also suggests the SDT consider revising the language to further clarify that the exception applies to the need to conduct a PRA, and not to the period covered by the PRA. This could be addressed as follows: "Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years. The requirement to complete a personnel risk assessment does not apply during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Agree with SDT rationale	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-004 R3, Part 3.5. Compliance with this requirement should not hinder first responders efforts to respond to emergency situations.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
During CEC the process is it not feasible to ensure individals with authorized electronic or authorized unescorted physical access have a personnel risk assessment completed.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
To provide consistency between the two major pre-requisites contained within CIP-004-6 R2 (Training) and CIP-004-6 R3 (PRA), the CEC langauge could be added where if Training is not required during a CEC prior to allowing emergency access, the requirements for R3 should allow for the same. Additionally, it could also be considered that CEC exemptions under R2 and R3 are not necessary based on the CEC exemption under CIP-004-6 R4.1, which allows an Entity to forego "authorizing access based on need" during a CEC. For example - if emergency responders are responding to a fire in a PSP, there would be no intention to "authorize" those personnel for unescorted access (which would require background checks and training) because they would be considered visitors, and the exemption under CIP-004-6 R4.1 should be sufficient. CIP-006-6 R2 also allows a CEC exemption to allow an Entity to forego escorting and logging visitors into a PSP during a CEC.	
Likes 0	

Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

Southern supports the inclusion of a CEC exemption under R1.8, but also provides the following for consideration under CIP-006: Under CIP-006-6 R1.4 and R1.6 – 'Monitor for unauthorized access' is a requirement where your ability to monitor constantly, 24x7, may be impacted by the onset of a CEC. For example – if a tornado or flood renders your ability to perform 24x7 monitoring unavailable until you can dispatch personnel or implement alternative means of monitoring – are you in violation of not performing 24x7 monitoring during the period you are convening and dispatching personnel to perform human observation and monitoring? What if, due to flooding, the PSP access points (or PACS assets) are inaccessible and monitoring communications circuits are down – removing your ability to dispatch personnel? Shouldn't R1.4 and R1.6 provide the ability to respond to and address monitoring when it has been impacted by a CEC? Similarly, if you are unable to monitor due to the onset of a CEC, you are likely also unable to issue an alarm or alert during that CEC. Consider, under CIP-006-6 R1.5 and 1.7 – 'Issue an alert in response to detected unauthorized access,' should be included as requirements that need a CEC exemption; otherwsie, are you in violation if a tornado or flood has taken out your standard implementation of alarm issuance during the period you are implementing back-up measures?	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-006 R1, Part 1.8. AECI agrees with the SDT's assertion that during certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	

Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Agree with SDT rationale although it is harder to envision a scenario where we wouldn't want to log entry of authorized personnel in some manner, even someone with a clipboard taking notes.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to CIP-006 R2, Part 2.2. During certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
This makes the requirement consistent with that for visitors in Part 2.2. However, I believe some measure of control is needed to ensure that, even during CIP Exceptional Circumstances, carte blanche access is not provided to all. This provides a potential secondary attack vector to those who	

otherwise might not have access. While perhaps full-fledged logging may not be required, some access list verification (including "approved visitors" needed for addressing the emergency is required.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Authorized unescorted physical access is logged automatically, or manually in the event that the automated system is unavailable. If a facility is damaged or destroyed, it may not be possible to control access via the automated system. Having resources to manually log individuals with authorized unescorted physical access to PSPs during a declared CEC may compromise the safety of the personnel logging access. Additionally, the amount of time to manually log entry could hinder recovery efforts resulting in increased risk to the BES. CIP Exceptional Circumstances are declared in emergency situations to protect life, safety and the reliability of the BES. Entities are given the flexibility to design programs that articulate how to declare and respond to a CEC. That flexibility should extend to the entity’s ability to appoint or allow individuals with appropriate skills to assist with recovery to gain physical access as necessary to mitigate reliability risks.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Under some circumstances when a CIP Exception Circumstance is allowed, it may or may not be possible to capture log this information manually. Entities should do their best, but CIP Exceptional Circumstance will still be needed in some of the possible scenarios.	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Depending on the nature of the incident, the RE makes every effort to maintain logs of physical attendance; however, this process should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	

Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See comments on Question No. 1	
Likes 0	
Dislikes 0	
Response	

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Because logging may not be occurring during a CIP Exceptional Cirumstance, there may be no logs to actually retain pursuant to this requirement. Further, if logging is ocurring, there is no need for a CIP Exceptional Circumstance to be applied to the log retention requirements. Thus, AZPS recommends that, relative to retention requirements, the phrase 'except during a CIP Exceptional Circumstance' be modified to state 'except if such logs are adversely impacted or destroyed as a result of a CIP Exceptional Circumstance'.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	
The rationale that is listed is not valid for this requirement. While I agree that logging may not be possible during periods when the facility is damaged and destroyed, it's not that logging can't be perfromed. It's that the log repository may be destroyed and rendered unusable.	
Likes 0	
Dislikes 0	
Response	

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	

Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	
Comment	
Depending on the nature of the incident, the RE should make every reasonable effort to maintain logs of physical attendance; however, this process should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
If a log is not created as required by Part 1.8 due to CIP Exceptional Circumstance, it logically follows that it won't be possible to retain it due to CIP Exceptional Circumstance.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon supports the addition of "except during CIP Exceptional Circumstance" to the Requirement part. As discussed in the response to question 2, it was noted that logging of authorized unescorted physical access could increase risks to personal safety and the reliability of the BES. During CECs where logging is not possible or practical, logs would not exist to retain for 90 days. Further, It is understood that for CECs where logging of authorized unescorted physical access took place, the entity would adhere to the 90 day retention requirement to the best of its ability. There may be situations where databases or manual records have gaps despite the fact that authorized unescorted physical access was granted as a result of the circumstances pertaining to the declared CEC. Additionally, where automation is used to record and retain the historical records of physical access logs, depending on the circumstances of the declared CEC, it is possible those records could have been partially or completely lost due to events of the declared CEC.	

Exelon recommends that the SDT add language to the Guidelines and Technical Basis that provide brief discussion about examples of scenarios where the ability to retain physical access logs for 90 days may not be possible as a result of a declared CEC.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
What if the physical access logs are damaged during a CEC, should they still be retained?	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes this aligns with 1.8.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
As noted in the rationale, this aligns to CIP-007-6 R4, Part 4.3. During certain events, logging may not be possible if the facility is damaged or destroyed. If the events are not logged due to a failure of CIP-006 R1, Part 1.8, the logs cannot be retained for ninety calendar days. Also, the current phrasing of the exception could suggest that the retention obligation does not apply during a CEC; however, ERCOT assumes the intent of the exception is that there should be no obligation to retain information that wasn't logged in the first place due to a CEC, consistent with the exception in part 1.8. In keeping with this purpose, ERCOT suggests modifying the sentence as follows: "…for at least ninety calendar days, except for any entry that was not logged due to a CIP Exceptional Circumstance."

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	

Comment
In cases were we don't log (Part 1.8) or logs are destroyed, it is impossible to retain what we don't have.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	

Comment
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-006 R1, Part 1.9. As stated in the AECI's previous response, during certain events, logging may not be possible if the facility is damaged or destroyed.

Likes 0	

Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC if the system storing the logs is impacted.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
As an extension to the justification under CIP-006-6 R1.8, if due to a CEC you are unable to log, you are also unable to retain logs that don't exist. Therefore, to provide consistency with the proposed modifications under R1.8, a CEC exemption should be added to R1.9 as well.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See comments on Question No. 1	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	
The rationale that is listed is not valid for this requirement. While I agree that logging may not be possible during periods when the facility is damaged and destroyed, it's not that logging can't be perfromed. It's that the log repository (in this case, perhaps the manual visitor log book) may be destroyed and otherwise unreadable.	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	

Comment	
Because logging may not be occurring during a CIP Exceptional Cirumstance, there may be no logs to actually retain pursuant to this requirement. Further, if logging is ocurring, there is no need for a CIP Exceptional Circumstance to be applied to the log retention requirements. Thus, AZPS recommends that, relative to retention requirements, the phrase ‘except during a CIP Exceptional Circumstance’ be modified to state ‘except if such logs are adversely impacted or destroyed as a result of a CIP Exceptional Circumstance’	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
As an extension to the justification under CIP-006-6 R1.8 and R1.9, if due to a CEC you are unable to log, you are also unable to retain logs that don't exist. Therefore, to provide consistency with the proposed modifications under R1.8 and R1.9, a CEC exemption should be added to R2.3 as well.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-006 R2, Part 2.3. During certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Again, if logs are destroyed, can't retain.	
Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to CIP-007-6 R4, Part 4.3. During certain events, logging may not be possible if the facility is damaged or destroyed. If the events are not logged due to a failure of CIP-006 R2, Part 2.2, the logs cannot be retained for ninety calendar days. Also, ERCOT notes that the current exception language could be read to apply to the duration of retention, and not to the underlying obligation to retain visitor logs that weren't created in the first place due to a CEC. ERCOT therefore suggests that the SDT consider the following clarification: "…for at least ninety calendar days, except for any visitor entry that was not logged due to a CIP Exceptional Circumstance."	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
What if the physical access logs are damaged during a CEC, should they still be retained?	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Vistors are manually logged by site personnel. Manually logging individuals who are visitors during CECs may compromise the safety of the personnel logging access. Additionally, the amount of time to manually log entry could hinder recovery efforts resulting in increased risk to the BES.

CIP Exceptional Circumstances are declared in emergency situations to protect life, safety and the reliability of the BES. Entities are given the flexibility to design programs that articulate how to declare and respond to a CEC. That flexibility should extend to the entity’s ability to appoint or allow individuals with appropriate skills to assist with recovery to gain access as necessary to mitigate risk.

Just as with the physical access log retention, there may be situations where databases or manual records have gaps despite the fact that physical access for visitors was granted. Additionally, where automation is used to record and retain the historical records of physical access logs for visitors, depending on the circumstances of the declared CEC, it is possible those records could have been partially or completely lost as a result of the events pertaining to the declared CEC event.

Exelon recommends that the SDT add language to the Guidelines and Technical Basis that provide brief discussion about examples of scenarios where the ability to retain physical access logs for visitors for 90 days may not be possible as a result of a declared CEC.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	Yes
Document Name	

Comment

CIP Exceptional Circumstances exists for CIP-006 R2, Part 2.2 regarding logging visitors. It logically follows that it won’t be possible to retain visitor logs if they weren’t created due to CIP

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

Depending on the nature of the incident, the RE should make every reasonable effort to maintain logs of physical attendance; however, this process should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
By stating “per BES Cyber Asset/System capability” this additional language does not seem necessary. In the event of an exceptional circumstance that causes damage to a device, it would seem reasonable to assume that capability is not present during that time period.	
Likes 0	
Dislikes 0	
Response	

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Depending on the nature of the event and/or condition of the cyber asset collecting the logs, log events may not be available. CIP Exceptional Circumstance language would then apply.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	

Comment	
Logging events may not be possible due to equipment failure.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully submits that the complex software and tool sets utilized to log events for malicious code may also be utilized to generate alerting for such events. Therefore, if such software and tool sets are impacted during a CIP Exceptional Circumstance and are unable to log, they may also be unable to generate alerts. Accordingly, we recommend the addition of the existing CIP Exceptional Circumstance language to Part 4.2.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Event logging at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) may not be possible during certain CECs if a facility is damaged or destroyed. For some operational technology devices where a replacement device is a new device type, it may be necessary to develop custom log parsing settings in order to obtain and import the logs to an automated log management solution as a result of the declared CEC.	
Likes 0	
Dislikes 0	
Response	

Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
If the device is destroyed due to hardware failure, fire, water damage, or other, and the only logging capability is local to the device, the entity should be able to follow their CIP Exceptional Circumstances process. This might be the case for devices that are serial only and do not have the capability/connections to send logs to a SIEM tool.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The circumstances associated with the declaration of CIP Exceptional Circumstances may have damaged or destroyed monitoring and logging systems such that event logs cannot be retained.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-007 R4, Part 4.1. During certain events, logging may not be possible if the facility is damaged or destroyed.	

Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments in response to #1.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
As noted in the rationale, this aligns to CIP-006 R2, Part 2.2. During certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	
Dislikes 0	

Response

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
During CIP Exceptional Circumstance (CEC), in the interest of restoring the BES, there may not be time to determine required cyber security controls that may be impacted by the change. If this is done, due to CEC, then it logically follows that CIP Exceptional Circumstances should be applied to all parts of CIP-010 R1, Part 1.4 because they are tied together. Therefore, add the phrase at the Part 1.4 level. For example, “Except during CIP Exceptional Circumstances, for a change that deviates from the existing baseline configuration: 1.4.1……, 1.4.2…… and 1.4.3……”	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

All of CIP-010-2 R1 should allow for CEC exemption. CIP-010-2 R1 and each of its sub-requirements all constitute "documentation" exercises that, when responsing to a CEC, may be required to be postponed or would be considered secondary to restoring power. Without similar caveats that are found in R1.3 allowing for documentation updates to be completed within 30 days, a CEC exemption is necessary for R1.1, R1.2, R1.4, and R1.5 when commissioning new devices needed in responding to a CEC.

Likes 0	
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

From an industry perspective, SCE agrees.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-0010 R1, Part 1.4.1. During a CEC event, cyber security control testing may hinder the Responsible Entitiy's recovery efforts.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	Yes
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The "return to normal operations" following CIP Exceptional Circumstances should include a validation that appropriate controls have not been impacted. Requiring this effort during CIP Exceptional Circumstances does not appear to add value and may impede restoration efforts.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to R3, Part 3.3. During the event, security controls testing may impede recovery efforts. Security controls should be examined on the production system following the conclusion of the declared CEC.	
Likes 0	
Dislikes 0	

Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Agree in concept but judgment still needs to be applied to verify the intended outcome is achieved without compromising security controls. Perhaps the verification of controls occurs after the emergency has ended and the facility and/or assets is again functioning in a normal capacity.	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
In the event of a CEC such as a natural disaster (hurricane/tornado) or an event that requied mutual assistance for restoration, an entity might need to rebuild/restore equipment without documenting the potential changes to cyber security controls. The restoration of the BES functionality in a safe and secure manner would be first priority. Security controls could be verified after the fact to ensure that appropriate controls are in place.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Entity change controls require a rigorous approval and testing process for changes to a BES Cyber Asset or BES Cyber System. In the event of a CEC, existing processes may not afford enough flexibility to conduct recovery in a way that rapidly mitigates the risk to the reliability of the BES.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS respectfully asserts that the entirety of Requirement R1.4 is what comprises security control testing, and, as such, recommends the addition of the CIP Exceptional Circumstances language to the opening phrase of Requirement R1.4.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

Depending on the nature of the incident, the RE should make every reasonable effort to determine impacted cyber security controls; however, this process should not hinder recovery/response efforts.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
SRP agrees that during a CIP Exceptional Circumstance, security controls testing may impede recovery efforts.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that during a CIP Exceptional Circumstance, security controls testing may impede recovery efforts.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Depending on the nature of the incident, the RE should make every reasonable effort to test changes in a test environment; however, this should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
If CEC is used for CIP-010 R1, Part 1.4, it logically follows that CEC should be allowed for testing the changes. The wording works, but the CEC phrase could be added only once at the CIP-010 R1 Part 1.5 level to cover both sub-parts with one phrase.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully asserts that the entirety of Requirement R1.5 should be subject to CIP Exceptional Circumstances. Accordingly, AZPS recommends that the addition of the CIP Exceptional Circumstances language to the opening phrase of Requirement R1.5.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Entity change controls require a rigorous approval and testing process for changes to a BES Cyber Asset or BES Cyber System. In the event of a CEC, existing processes may not afford enough flexibility to conduct recovery in a way that rapidly mitigates the risk to the reliability of the BES.

For clarity, Exelon suggests moving the “except during CIP Exceptional Circumstances” phrase closer to the front of 1.5.1 and 1.5.2 as noted below. This ensures that the phrase applies to the entire Requirement Part, and not just the last clause of the text.

1.5.1. Prior to implementing any change in the production environment, **except during CIP Exceptional Circumstances,** test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and

1.5.2. Except during CIP Exceptional Circumstances, document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Likes 0	
Dislikes 0	
Response	

Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

In the event of a CEC such as a natural disaster (hurricane/tornado) or an event that requied mutual assistance for restoration, an entity might need to rebuild/restore equipment without testing cyber security controls and documenting the test. The restoration of the BES functionality in a safe and secure manner would be first priority. Security controls could be verified after the fact to ensure that appropriate controls are in place.

Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Agree in concept but judgment still needs to be applied to verify the intended outcome is achieved without compromising security controls. Perhaps the verification of controls occurs after the emergency has ended and the facility and/or assets is again functioning in a normal capacity.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to R3, Part 3.3. During the event, security controls testing may impede recovery efforts. Security controls should be examined on the production system following the conclusion of the declared CEC.	

ERCOT also suggests moving the exception to the beginning of the language, as follows:

1.5.1 Except during a CIP Exceptional Circumstance, and prior to implementing any change in the production environment…"

And

"1.5.2 Except during a CIP Exceptional Circumstance, document the results of the testing…"

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF

Answer	Yes
Document Name	

Comment

Having the exceptional circumstances language in both subparts ensures that there is no question whether it is applicable to both subparts.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	Yes
Document Name	

Comment

Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-010 R1, Part 1.5.1 and 1.5.2. During a CEC event, cyber security control testing may hinder the Responsible Entitiy's recovery efforts.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

All of CIP-010-2 R1 should allow for CEC exemption. CIP-010-2 R1 and each of its sub-requirements all constitute "documentation" exercises that, when responsing to a CEC, may be required to be postponed or would be considered secondary to restoring power. Without similar caveats that are found in R1.3 allowing for documentation updates to be completed within 30 days, a CEC exemption is necessary for R1.1, R1.2, R1.4, and R1.5 when commissioning new devices needed in responding to a CEC.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Include the electronic and physical security controls required by CIP-003 R2 Attachment 1, sections 2 and 3. This would meet the same rational as used for the inclusion of CEC for CIP-004 and CIP-006.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
No additional requirements identified as applicable.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	

When considering Requirements against the elements of the CEC Definition, the view often focuses on time limited events measured in minutes, hours, or a day. We encourage a wider view. For example: An impediment of large scale workforce availability conceivably affects Requirements with time periods of multiple days, weeks, even months. This view stems from an entity's priority of operating the BES which may replace its ability to complete administrative efforts dedicated to program updates—while important—they fall out of the active operation of the BES to maintain reliability in emergency circumstances.

It is in consideration of this type of scenario we offer the following additional Requirements:

Rationale: Difficult to Adhere to Short Time-Based Requirements if During A CEC:

CIP-004-6 R5.1 (24-hour termination);

CIP-004-6 R5.3 (1-day termination to CII Repository);

CIP-004-6 R5.4 (30-day termination to shared accounts);

CIP-007-6 R2.2 (35-day patch evaluation);

CIP-007-6 R2.3 (35-day patch implementation/mitigation);

CIP-007-6 R4.4 (15-day logged event review);

CIP-010-2 R1.3 (30-day baseline configuration update after the change);

CIP-010-2 R2.1 (35-day baseline configuration monitoring);

Rationale: Similar Rationale As Other Requirements Added By SDT FOR CIP-010 R1, Part 1.4.1: CIP-010-2 R1.2 (authorize & document changes that deviate from the baseline configuration); Rationale: Similar Rationale As Other Requirements Added By SDT FOR CIP-007-4: CIP-007-6 R4.2 (security event alerting); CIP-004-6 R4.2 (quarterly access review) depending on timing of CEC.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Please see above responses where reference to additional requirements for consideration have been addressed.	
Likes 0	
Dislikes 0	
Response	

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Any requirement that requires real-time or near real-time alerting and response should include the CEC phrase. For example, CIP-004 R5, that addresses access revocations. In the case of CEC, response to a termination action or reassignment could be significantly delayed.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
CIP-004-6, R5, Part 5.1 - The Responsible Entity may not be able to remove an individual's ability for unescorted physical access and Interactive Remote Access if an asset is damaged or destroyed during a CEC. CIP-006-6, R1, Parts 1.2 – 1.7, & 1.10 – During a CEC, Physical Access Control Systems may be damaged or destroyed, preventing the Responsible Entity from strict adherence to these requirements. CIP-007-6, R4 Part 4.2 - The Responsible Entity may not be able to generate alerts for applicable security events if logging is not functional in accordance with CIP-007-6 R4 Part 4.1. CIP-007-6, R4 Part 4.4 – During a CEC, logging may not be functional if the facility is damaged or destroyed. CIP-010-2 R1, Parts 1.1 – 1.3 – Change management controls may impede recovery efforts during a CEC.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per standard/requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
All standards, requirements, and parts related to reliability and safety should include the CIP Exceptional Circumstance language.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Yes- if a facility is significantly damanged or destroyed all CIP requrements and sub requirements should be considered for CEC. For Example, Update of the Recovery Plan required by CIP-009-5 R3, Part 3.1 if the CEC lasts for more than 90 days.	

Update of the CIP Cyber Asset list required by CIP-002.

Testing of the recovery plan required by CIP-009-5 R2 Part 2.3 if the CEC is occurring during the planned testing date.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

- CIP-004-6 R5.1 Consider – In the case of a CEC, it may not be possible to complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). The ability to remove access may be impeded because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.1 Consider – In the case of a CEC, all applicable Cyber Assets connected to a network via a routable protocol may not reside within a defined ESP.

ESP might not be defined in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.3 Consider – In the case of a CEC, it may not be possible to have inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. Access permissions might not be defined in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.4 Consider – In the case of a CEC, it may not be possible to perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets. Performing authentication, when establishing Dial-up Connectivity with applicable Cyber Assets, might not be possible in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.5 Consider – In the case of a CEC, it may not be possible to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Having a method for detecting known or suspected malicious communications for both inbound and outbound communications, might not be possible in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.2 Consider – In the case of a CEC, it may not be possible to utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access. In the event of a failure of a PACS, it may not be possible to have 1 factor for access control.

- CIP-006-6 R1.3 Consider – In the case of a CEC, it may not be possible to utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access. In the event of a failure of a PACS, it may not be possible to have two factor access controls.

- CIP-006-6 R1.4 Consider – Monitoring unauthorized access through a physical access point into a Physical Security Perimeter may not be possible in the case that the logging and/or monitoring system is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.5 Consider – Issuing an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection may not be possible in the case that the logging and/or monitoring system, required to detected unauthorized access, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.6 Consider – Monitoring each Physical Access Control System for unauthorized physical access to a Physical Access Control System may not be possible in the case that the logging and/or monitoring system, required to monitor unauthorized physical access to PACS, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.7 Consider – Issuing an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection may not be possible in the case that the logging and/or monitoring system, required to detected unauthorized access to PCAS, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-007-6 R2.3 Consider – It may not be possible to apply applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, if the asset to be patched is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-007-6 R4.2 Consider – Generating alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, to detected malicious code from Part 4.1 and detected failure of Part 4.1 event logging, may not be possible in the case that the system to

detect malicious code and/or the system required to detect event logging failure, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-007-6 R4.4 Consider – Reviewing a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents, may not be possible in the case that the system required to log events, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-008-5 R2.1 Consider – It may not be possible to test each Cyber Security Incident response plan(s) at least once every 15 calendar months, by responding to an actual Reportable Cyber Security Incident, with a paper drill or tabletop exercise of a Reportable Cyber Security Incident or with an operational exercise of a reportable Cyber Security Incident. The ability to test the plan may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoke for that requirement in the case of a Cyber Security incident that mobilize the same staff required to test the Cyber Security response plan)

- CIP-008-5 R2.3 Consider – It may not be possible to retain records related to Reportable Cyber Security Incidents in the case that the records are damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-008-5 R3.1 Consider – No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, it may not be possible to document any lessons learned or document the absence of any lessons learned, to update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan and to notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned. The ability to document any lessons learned, update the plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike)

- CIP-008-5 R3.2 Consider – No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan, it may not be possible to update the Cyber Security Incident response plan(s) and notify each person or group with a defined role in the Cyber Security Incident response plan of the updates. The ability to update the plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike)

- CIP-009-6 R2.1 Consider – It may not be possible to test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months, by recovering from an actual incident, with a paper drill or tabletop exercise or with an operational exercise. The ability to test the recovery plan may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike)

- CIP-009-6 R2.2 Consider – It may not be possible to test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. The ability to test a

representative sample of information used to recover BES Cyber System functionality may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike).

- CIP-009-6 R2.3 Consider – It may not be possible to test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. The ability to test the recovery plans may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike).

- CIP-009-6 R3.1 Consider – No later than 90 calendar days after completion of a recovery plan test or actual recovery, it may not be possible to document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned, to update the recovery plan based on any documented lessons learned associated with the plan and to notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned. The ability to document any lessons learned, update the recovery plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoke for that requirement in the case of a general strike)

- CIP-009-6 R3.2 Consider – No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan, it may not be possible to update the recovery plan and notify each person or group with a defined role in the recovery plan of the updates. The ability to update the recovery plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoke for that requirement in the case of a general strike)

- CIP-011-1 R2.1 Consider – Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), it may not be possible that the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media in the case that the applicable Cyber Asset is no longer available because of an event triggering a CIP exceptional circumstance. (Example: A Cyber Asset containing BES Cyber System Information was stolen during a physical intrusion by terrorist)

- CIP-011-1 R2.2 Consider – Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, it may not be possible that the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media in the case that the applicable Cyber Asset or the data storage media is no longer available because of an event triggering a CIP exceptional circumstance. (Example: A Cyber Assets containing BES Cyber System Information was stolen during a physical intrusion by terrorist)

- Attachment 1, Section 2 (Physical Security Controls for low impact)

Consider – Control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any, may not be possible in the case that the physical control in place is damaged or destroyed because of an event triggering a CIP exceptional circumstance. (Example: emergency services destroyed physical lock that controls access in order to give assistance)

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Include the electronic and physical security controls required by CIP-003 R2 Attachment 1, sections 2 and 3. This would meet the same rational as used for the inclusion of CEC for CIP-004 and CIP-006.	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
CIP-003-6 Attachment 1 Section 2 should have the CIP Exceptional Circumstance language for physical security relative to the clause “shall control physical access, based on need.” While an entity could use language in their CIP-003 R2 Attachment 1 Section 2 to indicate that first responders have a “need,” it would be preferable to use the same program used for CIP-006 for consistency across all locations.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	

IPC would like the following CIP requirements added to the CEC list of requirements:

CIP-005-5 R1, Parts R1.1 to R1.5—There may be times during a CEC when a Responsible Entity will be in a position where holding their ESP intact is not feasible, possible, or will extend an operational outage or issue creating additional reliability concerns. A Responsible Entity should be provided with a high degree of latitude to address a CEC and be provided the tools necessary to address reliability concerns without concurrent compliance concerns.

CIP-006-6 R1, Parts R1.2 to R1.7—Although it is ideal to maintain Parts R1.2 to R1.7 in every circumstance, during a CEC, it may not be feasible for a Responsible Entity to utilize two-factor access controls, monitor physical access points, or issue alarms. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-007-6 R1, Parts R1.1 & R1.2—Although it is ideal to maintain Parts R1.1 and R1.2 in every circumstance, during a CEC, a Responsible Entity may not have time to document and protect every port. While port security is important, a Responsible Entity should have the flexibility to document and protect the applicable ports when the CEC has been corrected. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-007-6 R4, Part 4.2—If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, generating alerts for security events for Part 4.1 would most likely be unavailable as well. A Responsible Entity should be given the flexibility to determine what they are able to keep in place based on the event taking place and suspend those requirements that are either ineffective or non-functioning based on the situation.

CIP-007-6 R4, Part 4.4—If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, reviewing logs would not be possible for the time the logging system is down during the CEC, which may exceed 15 calendar days.

CIP-007-6 R5, Parts R5.1 to R5.3—Although it is ideal to maintain Parts R5.1 to R5.3 in every circumstance, during a CEC, a Responsible Entity may not have time to identify and enforce certain system access controls. While authentication, inventories of all generic accounts, and lists of those who can access shared accounts is important, it may not be necessary to have this documentation updated during a CEC where new devices are being implemented or old devices are being wiped and rebuilt. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-010-2 R1, Parts 1.1 to R1.4, including R1.4.2 & R1.4.3—Change management is a critical piece of day-to-day operations to maintain good process controls and practices. However, rigid change management processes and baseline documentation could just as easily be a hindrance to recovery efforts during a CEC. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-010-2, Attachment 1, Section 1.1 to 1.5—Although it is ideal to maintain Sections 1.1 to 1.5 in every circumstance, during a CEC, it may not feasible for a Responsible Entity to use only those devices that are designated as a TCA. Some instances may require additional resources from within a Responsible Entity that would not be approved TCAs. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning

CIP-010-2, Attachment 1, Section 2.1 to 2.3—Although it is ideal to maintain Sections 2.1 to 2.3 in every circumstance, during a CEC, it may not be feasible for a Resonsible Entity to mitigate software vulnerabilities and malicious code for TCAs managed by a party other that the Responsible Entity. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-010-2, Attachment 1, Section 3.1 to 3.2—Although it is ideal to maintain Sections 3.1 to 3.2 in every circumstance, during a CEC, it may not be feasible for a Responsible Entity to use only those devices that are designated as a RM. Some instances may require additional resources from within a

Responsible Entity that would not be approved RM. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-011-2 R1, Part R1.2—Although it is ideal to maintain Part R1.2 in every circumstance, during a CEC, it may not be feasible for a Responsible Entity to maintain adherence to a Responsible Entity's Information Protection Program. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon suggests also adding CIP Exceptional Circumstance language in these requirements:

1. CIP-010-2, R1, Part 1.1 Develop Baseline
2. CIP-010-2, R1, Part 1.2 Authorize changes to the baseline
3. CIP-010-2, R1, Part 1.3 Update baseline

The same justification that was used for CIP-010-2, R1, Part 1.5 could be applied to these three requirments.

It is a general practice that the baseline must be created prior to the Cyber Asset being put into production. If during a declared CIP Exceptional Circumstance, a new Cyber Asset type for which an existing baseline configuration does not exist must be deployed, the development of the baseline may hinder recovery and addressing BES reliability.

Additionally, where a major system outage has occurred that qualifies as a declared CIP Exceptional Circumstance, it is possible that in the interest of restoring the reliability function a new firmware version or version of software needs to be installed on the Cyber Asset outside of the traditional rigor of the change and configuration managmenet processes.

Lastly, during a declared CIP Exceptional Circumstance it may not be practical to update the baseline within 30 days while resources are addressing the CIP Exceptional Circumstance event.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully recommends that the SDT consider the addition of the CIP Exceptional Circumstances language to the following requirements: CIP-006, R1.4 – 1.7; (may be unable to perform under CEC, i.e., if the facility is destroyed); CIP-010-2, R1.1 (may impede recovery to the detriment of restoration of a reliable BES).	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy recommends that the CIP Exceptional Circumstance language be implemented across the entire suite of CIP standards and requirements. CEC(s) are implemented in situations where safety or reliability of the BES is concerned. In these most important instances, we believe it is appropriate to address the immediate safety or reliability issue first, without concern for the compliance implications that could result. Having CEC(s) as an option for all CIP requirements would eliminate the potential for an entity to take time to rationalize, and deliberate on compliance implications, prior to mitigating a safety or reliability issue. Mitigating concerns for safety and the reliability of the BES should always be first, and an entity having the ability to claim a CEC when necessary for all CIP requirements would help reinforce this way of thinking. Duke Energy recognizes that the SDT considered a holistic approach but abandoned it since it would require CMEP changes such that it wouldn't be considered as a non-compliant event. However, Duke Energy recommends that this could be solved by simply including the phrase "except during CIP Exceptional Circumstances" at the conclusion of each individual CIP requirement.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	

Comment
In addition to the Parts identified, we recommend adding the “except during CIP Exceptional Circumstances” language to the following Parts of the CIP Standards. • CIP-003-7 (i) R2 Attachement 1, section 2 – In a catastrophic event, physical access controls may be affected or altered temporarily. (e.g. Katrina) • CIP-004-6 Parts 4.2, 4.3, 4.4 – Scheduled quarter, annual, or 15 month reviews may not be delayed or not possible in the event of a catastrophic event. • CIP-04-6, Parts 5.2, 5.3, 5.4, 5.5 – In a catastrophic event, termination and access revocation activitities may be affected. • CIP-006-6 – 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.10, 3.1 – In a catastrophic event, physical access controls may be affected or altered temporarily (e.g., damage to gate cause by debris, or first responders entering facility). • CIP-010 Part 1.3 – The timing of being able to update the baseline within 30 days may not be able to be completed after a catastrophic event. • CIP-010 Part 1.4.2 – Although the timing of the testing of the cybersecurity controls isn’t addressed in the language of the requirement, there appears to be an expectation that testing occur soon after the change. In a catastrophic event, the timing of the actual testing needs to be prioritized after the recovery process is completed. • CIP-010 Part 2.1 -- The timing of being able to update the baseline within 30 days may not be able to be completed after a catastrophic event. • CIP-010 Parts 3.1, 3.2 – The timing of scheduled vulnerability assessments (paper or active) may be affected in the event of a catastrophic event. • CIP-011 Part 2.2 – In a catastrophic event, the cyber asset may not be able to be found (e.g., picked up by a tornado)

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	

Comment
CIP-004-6, R5, Part 5.1 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. During certain events, the ability to remove access may not be possible if a system is damaged or destroyed.

CIP-006-6, R1, Part 1.2 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event of a failure of a PACS, it may not be possible to have 1 factor for access control.

CIP-006-6, R1, Part 1.3 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event of a failure of a PACS, it may not be possible to have 2 factors for access control.

CIP-006-6, R1, Part 1.4 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In certain events, monitoring may not be possible if the facility is damaged or destroyed.

CIP-006-6, R1, Part 1.5 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event monitoring is unavailable, alerting may not be possible.

CIP-006-6, R1, Part 1.6 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In certain events, monitoring may not be possible if the facility is damaged or destroyed.

CIP-006-6, R1, Part 1.7 Rationale – This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event monitoring is unavailable, alerting may not be possible.

CIP-007-6, R2 Part 2.2 Rationale - This is similar to CIP-007-6 R4, Part 4.1. Security Patch Management timeline may be unattainable if there is failure of the patch assessment system during the event.

CIP-007-6, R4 Part 4.2 Rationale - This aligns to CIP-007 R4, Part 4.1. In the event monitoring under Part 4.1 is unavailable, alerting may not be possible.

CIP-007-6, R4 Part 4.4 Rationale - This aligns to CIP-007 R4, Part 4.1. In certain events, logging may not be possible if asset or a facility is damaged or destroyed.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

CIP Exceptional Circumstances should be applied to Attachment 1, Section 3 Electronic Access Controls. Electronic access controls applied to Low BES Cyber Systems (BCS) may need temporarily bypassing due to a CIP Exceptional Circumstance. Examples are where a firewall or data diode used for Low BCS Electronic Access Controls must be temporarily bypassed to resolve the CIP Exceptional Circumstance.

Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

Seattle City Light would like to see CIP Exceptional Circumstances added to CIP-003 R2, Attachment 1, Section 2 (and Section 5, as proposed).

For Section 2, the revision would read: "***Except during CIP Exceptional Circumstances***, each Respnosbile Entity shall control physical access,…"

The rationale for this addition is similar to that for requirements associated with CIP-004 and CIP-006, in that for during certain events, access controls may not be possible if the facility is damaged or destroyed.

For Section 5, the rationale would be the same as for CIP-010 R4, extended from Transient Cyber Assets and Removable Media at High and Medium location to those at Low locations.

Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP would like the following CIP requirements to be added to the CEC list of requirements:

- CIP CIP-007-6 R4, Part 4.2: If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, generating alerts for security events for Part 4.1 would most likely be unavailable as well.
- CIP-007-6 R4, Part 4.4: If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, reviewing logs would not be possible for the time the logging system is down during the CEC, which may exceed 15 calendar days.

Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Recommend adding the CIP Exceptional Circumstances language to the following Requirement in addition to those already identified: **CIP-006 R1, Part 1.1 – 1.9: Implementation of all Parts would be impacted by a CIP Exceptional Circumstance.**	
Likes 0	
Dislikes 0	

Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
CIP-006 R1 Parts 1.4 (Monitor PSP), 1.5 (Alarm within 15 minutes), 1.6 (Monitor PACS), 1.7 (Alarm within 15 minutes). Achieving compliance for these requirements depends greatly on hardware availability, including power supply. Whereas CIP-007 monitoring and logging requirements cannot be achieved in the event of a power outage to an ESP because there is no traffic flowing and without power there essentially is no ESP, the CIP-006 requires monitoring of the PSP which exists and can be accessed regardless of power outage/hardware failure/ natural disaster. Alarms cannot be generated, badge logs collected, or camera footage recorded in the event a site or system goes dark. It may be best practice for an entity to dispatch a security guard or other personnel to a site to perform manual monitoring and/or logging for some small scale events that would meet CIP Exceptional Circumstances. However, during major event such as a hurricane affecting dozens of sites across a large geographical area, it may not be feasible or within an entities safety policy to dispatch security personnel. Entities should implement compensating measures, such as fail-secure doors, for events that would affect the systems that meet compliance with these requirements during normal operations. However, it is unreasonable to expect entities to monitor and alarm at sites without appropriate support from technical solutions. Using the NERC language above, “During certain events,” physical alarming and/or monitoring “may not be possible if the facility is damaged or destroyed.”	
Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
CIP-007-6 part 2.2: If a security patch gets released 34 days after your assessment of the most recent previous patch, an entity would have one day (or possible less) to evaluate the patch. If you patch assessment system has a hardware failure (i.e. CEC) during this time, as it is now written this would be a violation. Strongly suggest adding this to the CEC list of requirements. CIP-007-6 part 4.2: If CEC is available for part 4.1 "logging of events" then it would, by inference, necessitate to have CEC available for part 4.2 since generation of alerts is probably based on logging of the events. CIP-007-6 part 4.4: Additionally for the same reason part 4.4 reviewing a summarization or sampling of logs would not be possible if all logging was offline during the CEC event, and the CEC event lasted more that 15 calendar days.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4

Answer	
Document Name	

Comment
When possible, consider adding the CIP Exceptional Circumstances language at the Requirement level rather than each of the individual Parts.

Likes 0	
Dislikes 0	

Response
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	
Document Name	

Comment
n/a

Likes 0	
Dislikes 0	

Response
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment
Seattle asks that the Standards Drafting Team consider simplifying the application of CIP Exceptional Circumstances to parts of CIP-006 by applying CIP Exceptional Circumstance language to R1 and R2, rather than to various parts and sub-parts.

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
A Reliability Standard must not hinder REs in responding to situations that endanger human life and/or adversely impact system restoration. It is possible to devise a circumstance where every one of the NERC CIP Reliability Standards may be violated while responding to a CIP Exceptional Circumstance. Instead of the proposed piecemeal approach, it is more reasonable to add a single requirement giving REs flexibility to respond to CIP Exceptional Circumstances that covers all NERC CIP requirements. NERC CIP-003 is a logical location for such a requirement. Embedding one universally applicable CIP Exceptional Circumstances requirement provides an approach that resolves the immediate dilemma of requirements for which an RE cannot possibly comply. During the normal course of standards revisions, legacy individual CIP Exceptional Circumstance clauses could be organically phased out so as not to induce a flurry of undue burden in otherwise unsubstantive procedure revisions.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	
Document Name	
Comment	
Documentation requirements associated with “documenting” the results of a previous Part, such as CIP-010 Part 3.4, should not require CEC language provided the language is afforded to the Parts subject to CEC treatment. In this example, CIP-010 Parts 3.1, 3.2, 3.3. However, if CEC is not extended to all of the Parts (CIP-010 Parts 3.1, 3.2, 3.3), then it should be considered for the documentation requirement (in Part 3.4).	
Likes 0	
Dislikes 0	
Response	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	
Document Name	
Comment	
Not at this time.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	2016-02_CIP_CEC_Unofficial_Comment_AZPS.docx
Comment	
AZPS would like clarification on the following statement: “CEC are included in a Responsible Entity’s cyber security policy from CIP-003 which describes how the entity would declare and respond to a CEC. During a declared CEC, the entity is allowed exception(s) to adhering to the specific reliability objective of the requirement(s); however, the entity is still compliant with the requirement(s) if the entity properly declares and responds to the CEC and adheres to its applicable cyber security policies”. The last phrase appears to contradict the concept or philosophy being expressed in the previous phrase in that it appears to require the entity to remain compliant with the requirement even if such requirement is impacted by a CEC. This would be contrary to the intent of a CIP Exceptional Circumstance	

wherein it is recognized that a responsible entity's ability to be compliant may be impacted as a result of a CEC, e.g., if a facility is substantially destroyed, a physical security perimeter may no longer be intact. AZPS requests that the SDT clarify the statement to ensure that the effect of declaring a CEC is clear and that all responsible entities understand what their continuing obligations are once a CEC is declared. Addtionally, AZPS has attached a document with recommendations to the Rationale in the table titled List of Additional Requirements for Consideration on Page 2-4 of the Unofficial Comment Form.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Consider simplifying the application of CEC in CIP-006 by applying the term to R1 and R2 and not to the sub-sections.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments in response to #1.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	

Answer	
Document Name	
Comment	

AEP recognizes the considerable effort of the SDT to establish an expansion of CIP requirements subject to exception during a CEC. AEP is concerned that like Versions 5 and 6 it will later be found that additional requirements should be subject to exception during a CEC. A more general rule for exceptions to CIP requirements would allow entities additional flexibility to manage its response during a CEC and future proof the CIP Standards in this area. The flexibility should come with a requirement to justify anyexceptions to requirements taken at specific locations or regions as they are impacted by a CEC. This or similar language could be placed in the “Exceptions” section of each CIP Reliability Standard: “4.2.3.5. A Responsible Entity may temporarily suspend compliance activities associated with CIP requirements for affected assets, BES Cyber Systems and individuals during a period when it has declared a CIP Exceptional Circumstance”. And, language could be added to the existing policy requirements of CIP-003-7 as follows: R1 1.1.9. and 1.2.6 **“**Declaring, justifying and responding to CIP Exceptional Circumstances”.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	

ERCOT supports the drafting team’s position in adding the CEC language to additional requirement parts. Although a formal CEC program would have been beneficial to entities in allowing coverage for all requirements, introducing compliance that derived from the approach would be burdensome to have all instances of invoking a CEC result in potential non-compliance.

Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	
Document Name	
Comment	

CIP Exceptional Circumstances include both a Bulk Electric System emergency when the responsible entity is delayed in, or prevented from, performing or carrying out any compliance activity required by CIP-002 through CIP-014 by reason of or through any cause reasonably beyond its control and not attributable to its neglect .

During the threat and after the impact of a CIP Exceptional Circumstance, ITC's priorities are the safety of its' employees and customers, environment compliance and the restoration of service.

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF

Answer	
Document Name	

Comment

Consider whether any changes to the definition of CIP Exceptional Circumstances are needed to accommodate potential government (Executive, DOE, etc.) orders which may require us to behave in a manner that appears to be out of compliance with one or more requirement(s) which provides for CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	
Document Name	

Comment

Basin Electric Power Cooperative agrees with the discussion surrounding the identification of typical standards/requirement/parts likely to be affected by a CIP Exceptional Circumstance. However, Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per standard/requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.

Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends clarification on what evidence will be required for a CIP Exceptional Circumstance.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
Consider simplifying the application of CEC in CIP-006 by applying the term to R1 and R2 and not to the sub-sections.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

Compliance with many additional CIP requirements could be impacted by a CIP Exceptional Event. Any requirement with an established timeframe (24 hours, 30 days, 15 months, or 7 years) could be impacted if a compliance requirement is slated for completion near the end of the time period and a CIP Exceptional Event were to occur.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	

Additional comments received by Vivian Vo of APS (Q9)

List of Additional Requirements for Consideration

Standard	Requirement	Rationale
CIP-004	Requirement R3, Part 3.5 Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	This is similar to the CIP-004-5 Requirement R2, Part 2.2 training requirement. A personnel risk assessment cannot be performed on first responders, would not be possible in emergency circumstances, and may not be possible on relevant vendors. Thus, this requirement should be subject to CIP Exceptional Circumstances for both ~~is would cover~~ the entity's personnel as well as contractors and service vendors
CIP-006	Requirement R1, Part 1.8 Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	This aligns to CIP-006-6 Requirement R2, Part 2.2. During certain events, logging may not be possible if the facility in which the logging and/or supporting hardware, software, or communication networks reside is damaged or destroyed. Thus, this requirement should be subject to CIP Exceptional Circumstances.
CIP-006	Requirement R1, Part 1.9 Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	This aligns to CIP-007-6 Requirement R4, Part 4.3. During certain events, a facility where the logging and/or supporting software, hardware, or communications reside may be damaged or destroyed. As a result, records already recorded for retention may also be adversely impacted and new logging may not be possible ~~if the facility is damaged or destroyed~~. Thus, this requirement should be subject to CIP Exceptional Circumstances.
CIP-006	Requirement R2, Part 2.3 Retain visitor logs for at least ninety calendar days.	This aligns to CIP-007-6 Requirement R4, Part 4.3. During certain events, a facility where the logging and/or supporting software, hardware, or communications reside may be damaged or destroyed. As a result, records already recorded for retention may also be adversely

Standard	Requirement	Rationale
		impacted and new logging may not be possible. Thus, this requirement should be subject to CIP Exceptional Circumstances.~~During certain events, logging may not be possible if the facility is damaged or destroyed.~~
CIP-007	Requirement R4, Part 4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	This aligns to CIP-006-6 Requirement R2, Part 2.2. During certain events, if the facility in which hardware, software, or communication networks utilized to support logging of events resides is damaged or destroyed, the ability to log events could be adversely impacted. Thus, this requirement should be subject to CIP Exceptional Circumstances.~~During certain events, logging may not be possible if the facility is damaged or destroyed.~~
CIP-010	Requirement R1, Part 1.4.1 Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	This aligns to Requirement R3, Part 3.3. During ~~the~~ an event, security controls identification and testing may impede recovery efforts necessary to restore the reliable operation of the BES. Thus, this requirement should be subject to CIP Exceptional Circumstances.
CIP-010	Requirement R1, Part 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and	This aligns to Requirement R3, Part 3.3. During an event, security controls identification and testing may impede recovery efforts necessary to restore the reliable operation of the BES. Thus, this requirement should be subject to CIP Exceptional Circumstances.~~During the event, security controls testing may impede recovery efforts.~~

Standard	Requirement	Rationale
	CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	

Additional comments received from Nathan Mitchell of APPA

Questions

Note: The new (revised) language is shown in red text.

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

   ☒ Yes

   ☐ No

   Comments:

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

   ☒ Yes

   ☐ No

   Comments:

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

☒ Yes

☐ No

Comments:

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

   ☒ Yes

   ☐ No

   Comments:

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

   ☒ Yes

   ☐ No

   Comments:

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

   ☒ Yes

   ☐ No

   Comments:

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

☒ Yes

☐ No

Comments:

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.

   ☒ Yes

   ☐ No

   Comments:

   Include the electronic and physical security controls required by CIP-003 R2 Attachment 1, sections 2 and 3. This would meet the same rational as used for the inclusion of CEC for CIP-004 and CIP-006.

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.

   Comments:

   Consider simplifying the application of CEC in CIP-006 by applying the term to R1 and R2 and not to the sub-sections.