Posting Document/Unofficial Comment Form

# Project 2016-02 Modifications to CIP Standards

Modifications to address CIP Exceptional Circumstances

**Do not** use this form for submitting comments. Use the [electronic form](https://sbs.nerc.net/) to submit comments  
on themodifications **to address CIP Exceptional Circumstances.** The electronic form must be   
submitted by **8 p.m. Eastern, March 13, 2017.**To minimize the number of posted documents, the Standard Drafting Team (SDT) included everything in this single document with the questions following the suggested approach and draft language.  
  
Additional information is available on the [project page](http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx). If you have questions, contact Senior Standards Developer, [Al McMeekin](mailto:al.mcmeekin@nerc.net) at (404) 446-9675.

**Introduction**

A CIP Exceptional Circumstance (CEC) is defined in the NERC Glossary of Terms Used in Reliability Standards as:

A situation that involves or threatens to involve one or more of the following, or similar,

conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil

unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security

Incident requiring emergency assistance; a response by emergency services; the enactment of

a mutual assistance agreement; or an impediment of large scale workforce availability.

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.

From the experience and knowledge gained in the on-going efforts to implement the CIP Version 5 standards, stakeholders requested in the SAR that the CIP Modifications Standard Drafting Team (SDT) review the entire suite of CIP standards to determine whether there are any additional requirements that could be impacted during a declared CEC, and if so, to recommend revisions to those requirements. The SDT reviewed the CIP Version 5 suite of standards and identified several more instances where including the phrase “except during CIP Exceptional Circumstances” is deemed appropriate. The SDT is proposing[[1]](#footnote-2) to retain the existing language in the currently approved CEC-related Requirements and add the same language to additional selected Requirements/Parts as outlined below.

**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, and may not be possible on relevant vendors. This 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 is damaged or destroyed. |
| 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, logging may not be possible if the facility is damaged or destroyed. |
| 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, 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, 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 event, security controls testing may impede recovery efforts. |
| 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 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. | This aligns to Requirement R3, Part 3.3. During the event, security controls testing may impede recovery efforts. |

Receiving thoughtful and constructive feedback from stakeholders is critical to the success of this plan. Submitting comments in advance of the deadline is welcomed and encouraged. The SDT thanks you for your participation.

# 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:

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-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:

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-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:

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

Yes

No

Comments:

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-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:

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-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:

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-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:

1. 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:

1. 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:

1. The SDT previously considered a second option to handle CIP Exceptional Circumstances which required the development of a formal CEC program that allowed for a CEC to be taken for any CIP requirement, based on need. Through additional review and input, the SDT determined that any CEC declared under the framework of a holistic CEC program would require treatment under the Compliance Monitoring and Enforcement Program as an instance of potential non-compliance. Consequently, the SDT dismissed this approach and is moving forward with a proposal based on the existing CEC paradigm. [↑](#footnote-ref-2)