

**Note: an Interpretation cannot be used to change a standard.**

Request for an Interpretation of a Reliability Standard	
<b>Date submitted:</b>	02/06/09
<b>Contact information for person requesting the interpretation:</b>	
<b>Name:</b>	Daniel Marvin
<b>Organization:</b>	PacifiCorp
<b>Telephone:</b>	503.813.5375
<b>E-mail:</b>	daniel.marvin@pacificorp.com
<b>Identify the standard that needs clarification:</b>	
<b>Standard Number (include version number):</b>	CIP-006-1.R1.1
<b>Standard Title:</b>	CIP-006-1 --Cyber Security -- Physical Security
<b>Identify specifically what needs clarification</b> (If a category is not applicable, please leave it blank):	
<b>Requirement Number and Text of Requirement:</b>	CIP-006-1 R1.1
<p><b>R1.1</b> Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.</p>	
<b>Clarification needed:</b>	
<p>If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?</p> <p>Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?</p>	
<b>Identify the material impact associated with this interpretation:</b>	

## Request for an Interpretation of a Reliability Standard

The material impact is potential non-compliance with the standard as written.

**Other industry entities interested in the clarification requested above are:**

- PacifiCorp
- Idaho Power
- Puget Sound Energy
- Platte River Power Authority
- Eugene Water & Electric Board
- Seattle City Light
- Arizona Public Service
- Bonneville Power Administration
- TransAlta
- Xcelenergy

**Project 2009-13: Response to Request for an Interpretation of CIP-006-1 Requirement R1.1 for PacifiCorp**

The following interpretation of CIP-006-1 — Cyber Security — Physical Security of Critical Cyber Assets was developed by the Cyber Security Order 706 SAR drafting team.

**Requirement Number and Text of Requirement**

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

**Question**

If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?

Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

**Response**

For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.