CIP-006 Drafting Team Responses to Comments

Commentor	Bob Wallace
Entity	Ontario Power Generation

Comments		*Responses*
General	OPG feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

CIP-006 Drafting Team Responses to Comments

CIP-006 Drafting Team Responses to Comments

Commentor	Carol L. Krysevig
Entity	Allegheny Energy Supply Company

Comments	*Responses*
General	The drafting team acknowledges this concern and invites suggested wording changes for this section. The standard has been modified to allow exceptions in generating stations for safety purposes, but other devices should meet the minimum requirements.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor Dave McCoy
Entity Great Plains Energy Cyber Security Task Force

Comments	***Responses***
General Maintenance of videotapes for logging physical access should be cut from 90 days to something more reasonable, like 30 days.	Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are to be kept for 1 calendar year.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Edwin C. Goff III
Entity	Progress Energy

	Comments	*Responses*
General	The requirements specify physical access controls at every access point to the perimeter which can be accomplished via special locks with non-reproducible keys, which at a substation should be adequate. 24/7 monitoring to detect unauthorized entry, CCTV, alarm systems, computerized logging and procedures for manual logging access to facilities is currently not in place and not recommended based on our ability to recover, reroute, or use redundant assets. These measures may be appropriate for balancing authorities and reliability coordinators, but are excessive for transmission and generation assets. If minimum physical security standards are to be specified, a graded approach should be used based on the criticality of the asset and other factors which may mitigate the impact of access to the asset or asset loss.	CIP002 addresses a formal risk assessment approach. Latitude has been provided within this standard (CIP006) to allow the entity to implement compensating controls for compliance, see Additional Compliance Information.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4	M4 - "implement one or more of the following..." -- this measure could drive network bandwidth requirements that may result in currently unplanned upgrades.	The drafting team believes that sufficient latitude has been provided within this standard that a responsible entity can implement compliant controls without excessive bandwidth requirements. For example, alarming back to a central monitoring system, as contrasted to video, should have minimal bandwidth requirements.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Francis J. Flynn, Jr., PE
Entity	National Grid USA

Comments		***Responses***
General	National Grid believes CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor Gary Campbell
Entity MAIN

Comments	***Responses***
General Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement. The way the measures are written, as an auditor I do not care what the requirements tell me should be in a procedure, policy etc. The measures are telling what to look for by the usage of "shall" and then specify what is to be looked for.	Requirements, Measures and Levels of Non-compliance have been modified.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Gerald Rheault
Entity	Manitoba Hydro

	Comments	***Responses***
General	In CIP-005 & CIP-006 a requirement should clearly state that unauthorized personnel must be escorted by authorized personnel. Compliance sections in CIP-005 & CIP-006 should more closely align. In CIP-006 compliance section 2 "aggregate interruptions" is mentioned with no previous explanation or reference in the requirements or measures sections. What do they mean? How are they measured? Is this really required?	The drafting team will consider this suggestion. Significant changes to compliance have been made in the reformatting of all standards for better alignment that should address this concern. "Aggregate interruptions" means the combined total of multiple interruptions. If this combined total for the period falls into the range specified the entity would report non-compliance at that level.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5	In CIP-006 M5 Logging Physical Access under manual logging "...accompanied by human observation or remote verification." This statement does not belong under logging rather under either/both M3 Physical Access Controls or M4 Monitoring Physical Access Controls.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

CIP-006 Drafting Team Responses to Comments

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Greg Mason
Entity	Dynegy Generation

Comments		***Responses***
General		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3	Measure M3 needs to be clarified for Critical Assets in office buildings. This Measure should state that 4 wall security plus additional security monitoring of the surrounding access areas(i.e hallways,etc.) is sufficient to meet the intent of this section for this type of environment. Development of a FAQ on this issue would also be helpful.	Access controls should be implemented to control access to the perimeter access points regardless where the critical cyber assets reside.
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Guy Zito
Entity	NPCC CP9

Comments		***Responses***
General	CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	James W. Sample
Entity	California ISO

Comments		*Responses*
General	Delete (nearest six-wall boundary) as this is already covered in the definition above or move it to the definition.	Please see responses to comments by Todd Thompson, SPP.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	R6 -- Duplicates R1.	
006-M1	M1 -- 90 days is not found in the requirements section.	
006-M2		
006-M3	M3 -- this is too prescriptive and does not respect changing technologies. The words "or equivalent" would make this section better. The term "Security Officers" is confusing and should be changed to "Security Personnel".	
006-M4	M4. This is redundant. These requirements are referred to in R1 and M1.	
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	1.3 If the documents referred to are video records, then this is excessive, unless the documents relate to a significant security incident.	
006-C1,4		
006-C2,1	2.1.1 Not consistent with M1.	
006-C2,2	2.2.1 Requires more stringent compliance than level 1 compliance.	
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Jerry Freese
Entity	American Electric Power

Comments		*Responses*
General		
006-R1	In R1 this requirement should include the requirement for the Responsible Entity to actually maintain a security plan. It could be worded as follows: "The responsible entity shall develop and document a physical security plan, which at a minimum, includes the following requirements."	Changes have been made to the required maintenance of the security plan.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Jerry Heeren
Entity	MEAG Power

Comments	***Responses***
General	Requirements and Measures numbering scheme does not match.	The measurements and requirements have been modified.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Jerry Litteer
Entity	INL

	Comments	*Responses*
General	There is no requirement for log review. Suggest alarm at multiple attempts over a short time period, and daily review of logs to establish trends of activities and identify where future vulnerabilities are likely. Monitoring equipment and activities are useless without reviewing results daily. Having a camera system that 'watches' the door traffic would pass as monitoring. If the logs are not examined, how do you know your status? This basic requirement is missing throughout the whole standard, not just in CIP-006-1.	One of the purposes of logging is identifying exceptions to normal operations. Modern logging systems identify these in real time as a standard feature. In the case of legacy systems, entities need to manage this procedurally using a risk based assessment.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5	M5 and Compliance 1.1.2 keep audit records for 90 days -- too short for low and slow cyber activities which might involve a physical aspect, but compliance monitor shall keep audit records for 3 years.	The bulk of comments received do not support this opinion.
006-M6		
006-C1,1	M5 and Compliance 1.1.2 keep audit records for 90 days -- too short for low and slow cyber activities which might involve a physical aspect, but compliance monitor shall keep audit records for 3 years.	The bulk of comments received do not support this opinion.
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Jim Hansen
Entity	Seattle City Light

Comments		*Responses*
General		
006-R1	R1.1, the development of a defense strategy is dependent on what we are trying to physically defend against. For example, do the authors expect us to defend against casual access, unauthorized access via stealthy break-in, armed attack, aerial attack, explosion, terrorist assault teams? The measures do not refer to the defense strategy. Please state more specifically what is intended by this term. 2. In M4, regarding CCTV, what are the retention requirements for the video images?	The term defense strategy has been removed from the document.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4	M4, regarding CCTV, what are the retention requirements for the video images?	Modifications have been made. Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are to be kept for 1 calendar year.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Joe Weiss
Entity	KEMA

Comments	***Responses***
General	CIP 006 FAQ 9. The response provides three generally accepted risk assessment methodologies. It should be noted that ISA TR99.00.02-2004, Technical Report 2 -- Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment provides a risk methodology specific to process control systems and should be referenced. Care should be taken when applying any risk assessment methodology to address control system cyber-specific frequencies and consequences.	Noted.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Joe Weiss
Entity	KEMA

Comments	*Responses*
General	
A risk-based assessment should be performed to determine what facilities should be addressed by this standard. It should be noted that the NERC Control System Security Working Group (CSWWG) debated the issue of excluding the term bulk from the Physical Security - Substations Guideline. The CSSWG removed the term bulk in the next to last version of the Guideline because utilities had identified distribution substations as meeting the Critical Assets definition.	This is provided for in CIP002 Noted.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	John Lim
Entity	Con Edison

	Comments	*Responses*
General	The content of Requirements does not necessarily match the content of the Measurements; for example R2 talks about Physical Access Control while M3 and not M2 talks about that.	The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section.
006-R1		
006-R2	R2/M2 not clear; give examples of "industry or government, generally accepted, risk assessment procedure."	Examples are provided in the FAQ.
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	1.3: it is not clear what documents are referred to in 1.3 (Compliance section) to be kept for three calendar years.	Draft 3 contains changes to this section that the drafting team believes clarifies the documentation to be retained.
006-C1,4		
006-C2,1	2.1.1: neglects to mention (as in M1) that the 90 day review applies in the case of modification to the perimeter or physical security methods. Change to: 2.1.1 Document(s) exist, but have not been reviewed for more than 1 year or have not been updated within 90 days of modifications.	Compliance section has been modified to clarify these items. However, these two points are different levels of non-compliance.
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Karl Tammer
Entity	ISO/RTO Council

	Comments	***Responses***
General	Purpose: Delete (nearest six-wall boundary) as this is already covered in the definition above or move it to the definition.	Change has been made.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	R6 -- Duplicates R1.	Duplication has been removed.
006-M1	M1 -- 90 days is not found in the requirements section.	This will now be covered only in the requirements section. The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section.
006-M2		
006-M3	M3 -- this is too prescriptive and does not respect changing technologies. The words "or equivalent" would make this section better. The term "Security Officers" is confusing and should be changed to "Security Personnel".	The table was provided to clarify the types of access controls that are acceptable, and latitude has been provided in the compliance section for duly authorized exceptions to a Responsible Entity's cyber security policy when it cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section. Change to Security Personnel has been made.
006-M4	M4. This is redundant. These requirements are referred to in R1 and M1.	Requirements and Measures have been modified.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	1.3 If the documents referred to are video records, then this is excessive, unless the documents relate to a significant security incident.	Modifications have been made. Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are

		to be kept for 1 calendar year.
006-C1,4		
006-C2,1	2.1.1 Not consistent with M1.	Requirements, Measures, and Levels of Non-compliance have been modified for consistency.
006-C2,2	2.2.1 Requires more stringent compliance than level 1 compliance.	Levels of Non-compliance have been modified and the drafting team believes they denote increasing severity of non-compliance.
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Kathleen M. Goodman
Entity	ISO New England Inc.

Comments		***Responses***
General	ISO-NE feels CIP-006 needs more work before it is ready for ballot. The reference to six-wall boundary is only referenced once, but is confusing. Be more specific as to intent.	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.The term <<Security Officers>> is confusing and should be changed to <<Security Personnel>>.	
006-M4	M4. This is redundant. These requirements are referred to in R1 and M1.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

006-C1,4

006-C2,1 2.1 Requires more stringent compliance than level 1 compliance.

2.1.1 Not consistent with M1.2.

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Keith Fowler
Entity	LG&E Energy Corp.

	Comments	***Responses***
General	We are in agreement with the comments submitted by the ECAR CIPP group.	Please see response to comments by ECAR CIPP group.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5	M.5: Does "physical access logs shall be retained for at least 90 days" intend to require retention of digital electronic capture of video images?	Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are to be kept for 1 calendar year.
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Ken Fell
Entity	New York Independent System Operator

Comments		*Responses*
General	This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.	Please refer to responses to comments on CIP-002.
	Measures M3-5 should have the first sentence and table eliminated for each. They are too prescriptive.	Requirements, measures, and levels of non-compliance have been modified.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 should be deleted as it is redundant with R1.	Requirements, measures, and levels of non-compliance have been modified.
006-M1	The 90 day requirement in M1 is not reflected in the requirements section.	Requirements, measures, and levels of non-compliance have been modified.
006-M2		
006-M3		
006-M4	M4 is redundant with M1.	Requirements, measures, and levels of non-compliance have been modified.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	Non-Compliance 2.1.1 is not consistent with M1.	Requirements, measures, and levels of non-compliance have been modified.
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor L.W. Brown
Entity Edison Electric Institute

Comments	*Responses*
General Applying these Requirements to generation facilities raises unique and difficult issues that should be dealt with separately, as they will take a great deal of time and attention to adequately or reasonably address. As noted above (at CIP-002-1 Requirement R1.1.1), we believe most of these Standards should not be applied to most generation facilities. There are simply too many locations within any one generating facility that cannot reasonably be secured more than is the plant as a whole. For instance, network wiring may be located in cable-trays throughout the facility.	The drafting team acknowledges this concern and invites suggested wording changes for this section. The standard allows Responsible Entities to write exceptions to their cyber security policies (see additional compliance section), but otherwise critical cyber assets must meet the minimum requirements as defined in this standard..
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity	Cinergy

	Comments	***Responses***
General	CIP-006-1--Physical Security: Because the requirements are very specific, we still believe that NERC should have some idea of the financial impact of its directives across the industry. This comment was made in response to Draft I, and the drafting team response was that this was up to the individual company to assess financial impacts. It is not up to the individual company to assess the financial impact across the entire industry. The drafting team's response to the comment asking that NERC have some idea of the financial impacts across the industry was un-satisfactory and we again recommend that NERC has responsibility to have some idea of the financial impacts across the industry prior to finalizing these requirements. Additional Question FAQ: Reference Frequently Asked Questions -- Standard CIP-006-01, Cyber Security-Physical Security Section. The question of "What is the Physical Security Perimeter?" has an answer that says, "is a four wall boundary." Shouldn't the answer be a six wall boundary?	The Standards Development Process Manual requires NERC to build consensus among interested parties regarding the scope of its reliability standards. Public comments from interested parties would show if the financial impacts of a suggested standard outweigh the benefits to reliability. This was not the case with the CIP standards. The scope of the CIP standards was developed based on several rounds of public review and comments per NERC's Standard Development process. The Standards Authorization Committee approved the resulting Standards Authorization Request for standards drafting. The SAC and the drafting team recognize that Responsible Entities will incur costs to secure their Critical Cyber Assets and, thus, the grid; the Implementation Plan associated with these standards reasonably accounts for budget cycles. FAQs have been updated.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3	C.M.3--Security Officers: Can a control room operator also fulfill the 'security officer' function of monitoring physical access 24 hours a day, 7 days a week? Can the access point be manned by someone other than a security guard if the access point is in a room that is manned by plant personnel 24x7? Would this be sufficient along with the other access controls?	If a control room operator has been trained in physical security monitoring and procedures for response, this would be sufficient and could be documented as an exception to CIP006.
006-M4		
006-M5	C.M.5.--Manual Logging: Section now states: "A log book or sign-in sheet or other record of physical access accompanied by human observation or remote verifications." We recommend deleting the phrase "...accompanied by human observation or remote verifications." We believe that the logging book and sign in sheet are sufficient documentation for the manual logs.	The drafting team believes that if a manual log book is the ONLY method of logging access that some type of observation or verification is required to ensure that the log is filled out.
006-M6		

CIP-006 Drafting Team Responses to Comments

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel

Comments	***Responses***
General	A3. Recommend deleting the word "nearest". Change to: " it is necessary to identify the physical security perimeter(s) (six-wall boundary)"	The words have been removed altogether and entities should reference the definition.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor Laurent Webber
Entity Western Area Power Administration

Comments	*Responses*
General Purpose: Does the reference to a six-wall-boundary mean that this does not apply to outdoor assets, as found in substations and communication sites. Does it apply to the control buildings at substations and the radio building at communication sites? This will be very extensive, expensive, and cascading requirement to apply to all substations and microwave or fiber communication sites that are related to IROL. Again this relates to the definition of Critical Cyber Assets.	Typically, critical cyber assets at control stations that meet the definitions of this standard are housed in the control buildings. Latitude has been provided in the compliance section for approved exceptions to a Responsible Entity's cyber security policy when it cannot implement at least one of these requirements. This standard does not apply to communication sites.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Lawrence R Larson, PE
Entity	Midwest Reliability Organization

Comments	***Responses***
General	It should be clarified that the Requirements herein do not necessarily apply to substations. Separate language should be added that indicates that, in regards to physical security for substations, each entity should establish and follow its own risk assessment policy as they deem appropriate. The prescriptive measures defined here are too much overhead to require for substations. Under Levels of Non-Compliance, 2.1.2, 2.2.2, and 2.3.2 should be eliminated or modified, as there is no reasonable way to track (aggregate interruptions). It is not clear what this term means, and it is introduced in the Compliance Section while it was not discussed in the Requirements or Measures Sections.	CIP002 addresses a formal risk assessment approach. Only those assets that have been defined as critical by the entity using CIP002 as a guide, are subject to these standards. Latitude has been provided in the compliance section of this standard (CIP006) for approved exceptions where an organization cannot implement at least one of these requirements. The standard has been modified to address requirements of outage tracking. "Aggregate interruptions" means the combined total of multiple interruptions. If this combined total for the period falls into the range specified the entity would report non-compliance at that level.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Lee Matuszczak
Entity	U S Bureau of Reclamation

Comments		*Responses*
General	Purpose: - It is very important to limit requirements addressed in this section to defined Critical Cyber Assets. Its impact on non-cyber critical assets would be significant.	The drafting team believes that the Purpose sufficiently limits this standard to critical cyber assets, as opposed to non-cyber assets. If upon further review the commenter still feels that this is not the case the team welcomes suggested wording to reinforce this point.
006-R1		
006-R2		
006-R3	R3. - This requirement may be impractical for a remotely-located outdoor-enclosure-mounted remote terminal unit. It may be practical to detect entry into the enclosure via a door-mounted alarm, but the installation of logging equipment (assumed to be a means of identifying the individual gaining access) may be costly and difficult to support. Consider alternatives or a relaxed requirement.	The table was provided to clarify the types of monitoring controls that are acceptable, and latitude has been provided in the compliance section for approved exceptions where an organization cannot implement at least one of these requirements.
006-R4		
006-R5	R5. - This requirement can only be addressed to a certain assurance level. It should be acknowledged that it is not and cannot be made foolproof.	The drafting team acknowledges that there is no maintenance and testing program that can ensure that components will never fail. However, it is incumbent upon the responsible entities to conduct periodic testing and maintenance to ensure that failures are prevented to the extent possible and detected within a reasonable period of time.
006-R6		
006-M1		
006-M2		
006-M3		
006-M4	M4. - There is no discussion throughout this standard of appropriate or recommended response measures. Monitoring will be ineffective if no response measures are established and exercised.	Please see CIP-008 and CIP-009.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Linda Campbell
Entity	FRCC

	Comments	***Responses***
General		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4	M4 Would human observation (i.e. a security guard checkpoint that is manned 24x7) be an acceptable method for monitoring physical access control, and if so can this be added to the table in M4?	This has been added. The standard has been reformatted and this will now be covered in the requirements section.
006-M5	M5. How does this measure address piggybacking?	Piggybacking cannot be addressed by access controls without significant cost. Entities should address this at a policy level. Requirements have been updated to reflect this.
006-M6		
006-C1,1		
006-C1,2	The words under Compliance section 1.2. really belong under 1.3. Data Retention. Compliance section 1.2. should be as follows: Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.	This section has been modified.
006-C1,3	Compliance section 1.3. should be as follows: 1.3. Data Retention 1.3.1. The compliance monitor shall keep audit records for three (3) calendar years. 1.3.2. The Responsible Entity shall keep data for three (3) calendar years.	This section has been modified.
006-C1,4		
006-C2,1		
006-C2,2		

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Marc Butts
Entity	Southern Company, Transmission, Operations, Planning and EMS Divisions

	Comments	***Responses***
General	Purpose -- Define - six-wall boundary.	The definition of Physical Security Perimeter has been modified to address this.
	Pg 6, Regarding levels of non-compliance: does -aggregate interruptions- refer to a centralized system, therefore assuming there is one?	No, aggregate interruptions" means the combined total of multiple interruptions
006-R1		
006-R2		
	006-R3 Pg 4, R3, Regarding monitoring physical access control, what is meant by -generally accepted industry or government risk assessment procedure-? Monitoring physical access 24/7 will be very difficult for the many locations large companies have. Again, if substations w/ FRAD's are included, this would have far-reaching implications and tremendous costs.	Reference to risk assessment has been removed. Monitoring is not required at every substation with Frame relay connectivity, only those that meet the criteria set forth in CIP002
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3	Pg 4, M3; Regarding special locks: could you please define what a Man-trap might be?	A man-trap is a double door entry system where entry is gained by first opening one door, entering an enclosed area, and then passing through a second door which cannot be opened until the first is closed and locked. This is most commonly used when entering highly secured facilities.
006-M4		
006-M5	Pg 5, M5; Regarding monitoring & logging physical access: per above, it sounds like either CCTV or an alarm system of some kind would be required at every substation w/ frame relay communication. While some may have this already, I would guess that many/most do not.	This would be required at only those substations deemed by the entity to house critical cyber assets, using a risk assessment process as required in CIP002. Card key systems would also be acceptable for monitoring access.
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	Levels of Compliance, Levels 1 and 2 -- Are -aggregate interruptions in monitoring system availability- intended to be for a failure a one location or an aggregate of all Critical locations? If all	The drafting team felt that establishing varying compliance levels based upon the number of facilities an organization must monitor would

	locations, then how can a responsible entity with many Critical locations be held to the same composite (7 days or 1 month) as a responsible entity with only 1 or 2 locations?	be impractical and difficult to administer. Therefore the team established levels that it felt would be reasonable from an industry wide perspective. Please propose language which you believe would improve this section.
006-C2,2	Levels of Compliance, Levels 1 and 2 -- Are -aggregate interruptions in monitoring system availability- intended to be for a failure a one location or an aggregate of all Critical locations? If all locations, then how can a responsible entity with many Critical locations be held to the same composite (7 days or 1 month) as a responsible entity with only 1 or 2 locations?	Please see response, above.
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Patrick Miller
Entity	PacifiCorp

	Comments	***Responses***
General	For section C, M3, there are tabled items which can not be referenced within the letter/number outline format. These items should be represented as M3.1 through M3.5 to correctly adhere to the outline format. There is also an unreferenced paragraph at the end of the measure which should have some identifier attached for reference. For section C, M4, there are tabled items which can not be referenced within the letter/number outline format. These items should be represented as M4.1 and M4.2 to correctly adhere to the outline format. There is also an unreferenced paragraph at the end of the measure which should have some identifier attached for reference. For section C, M5, there are tabled items which can not be referenced within the letter/number outline format. These items should be represented as M5.1 through M5.3 to correctly adhere to the outline format. There is also an unreferenced paragraph at the end of the measure which should have some identifier attached for reference.	Significant changes in the format of this document have been made which should address all of these comments. Tables have been eliminated and all requirements are now numbered. The detail has been moved from measurement section to requirements section
006-R1		
006-R2		
006-R3	For section B, R3, it is unclear if the monitoring requirement is 24/7 or simply by reviewing logs at a later time/date.	This requirement is for an active 24/7 monitoring process. This has been clarified.
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Paul McClay
Entity	Tampa Electric

Comments		*Responses*
General		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4	M4 Human observation (i.e. a security guard checkpoint that is manned 24x7) should be an acceptable method for monitoring physical access control, and added to the table in M4.	Human observation has been added to the table as an acceptable method of monitoring physical access. The standard has been reformatted and this will now be covered in the requirements section.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Pedro Modia
Entity	Florida Power and Light

Comments		***Responses***
General		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5	M5. How does this measure address piggybacking?	Piggybacking cannot be addressed by access controls without significant cost. Entities should address this at a policy level. Requirements have been updated to reflect this.
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Pete Henderson
Entity	IESO Independent Electricity System Operator

	Comments	***Responses***
General	Delete reference to the nearest six-wall boundary from the discussion on "Physical Security Perimeter", as the term "Physical Security Perimeter" is already defined. Alternatively, include the concept in the definition.	The wording is included in the definition and clarified in the FAQ. It has been removed from the purpose.
006-R1	In R1, it is not clear what a physical security plan is. Better phraseology might be, "the Responsible Entity shall develop a physical security plan which shall document the following:".	The drafting team believes that the current version (draft 3) more clearly defines what is required of the security plan.
	In R1.1 Please delete the phrase, "and the development of a defense strategy". It is unclear what is meant by the phrase and how one documents the implementation of the development of a strategy.	The term defense strategy has been removed.
	In R.1.2 Delete the phrase "and the critical assets within them". Controlling access to the Physical Security Perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2 below In R1.3, Delete the phrase "and the critical assets within them. Monitoring access to the Physical Security Perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2 below	The point of this section was to ensure protection of the assets, and the wording has been changed accordingly. The phrase in R1.3 has been removed.
006-R2		
006-R3	In R3, reword as. "for monitoring physical access to the Physical Security Perimeter...."	modifications have been made.
006-R4	In R4, reword as. "for logging physical access to the Physical Security Perimeter....."	modifications have been made.
006-R5		
006-R6	R6 -- Duplicates R1.	Requirements have been updated.
006-M1	M1 -- 90 days is not found in the requirements section. Replace "modification " by "significant modification"	This will now be covered only in the requirements section. The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section.
006-M2		
006-M3	M3 -- this is too prescriptive and does not respect changing technologies. The addition of the words "or equivalent" would make this section better. The term "Security Officers" is confusing and should be changed to "Security Personnel".	The table was provided to clarify the types of access controls that are acceptable, and latitude has been provided in the compliance section for approved exceptions where an organization cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section. The term "Security Officers" has been changed

	The paragraph beginning "In addition" defines requirements that are redundant.	The paragraph beginning "In addition" has been simplified this paragraph in draft 3. We believe these changes address this concern. We do, however, feel the need to emphasize access request and review processes and reference CIP-003 to ensure consistency.
006-M4	M4. This is redundant. These requirements are referred to in R1 and M1. Furthermore, this is too prescriptive and does not respect changing technologies. The addition of the words "or equivalent" would make this section better.	The table was provided to clarify the types of monitoring controls that are acceptable, and latitude has been provided in the compliance section for approved exceptions where an organization cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section.
	The paragraph beginning "In addition" defines requirements that are redundant. The requirement to maintain a physical security plan (R1 and maybe R6) and the requirement to keep it up to date as established in M1 effectively cover all of the ground that the text in this paragraph covers.	The paragraph beginning "In addition" has been eliminated .
	The paragraph beginning "In addition" defines requirements that are redundant	
006-M5		
006-M6		
006-C1,1		
006-C1,2	1.2 establishes requirements that appear to be inconsistent with M5.	This section has been reworded.
006-C1,3	1.3 If the documents referred to are video records, then the requirement for 3 years data storage is excessive, unless the documents relate to a significant security incident.	modifications have been made. Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are to be kept for 1 calendar year.
006-C1,4		
006-C2,1	2.1.1 Not consistent with M1.	Modifications have been made to improve consistency.
006-C2,2	2.2.1 Requires more stringent compliance than level 1 compliance, which would be perverse. to maintain a physical security plan (R1 and maybe R6) and the requirement to keep it up to date as established in M1 effectively cover all of the ground that the text in this paragraph covers. In addition, requirements for maintaining documentation describing the access request, authorization, and review process are specified in CIP-003. There is no need to refer to those requirements in CIP-006.	Modifications have been made to improve consistency.
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor Randy Schimka
Entity San Diego Gas and Electric Co

Comments	***Responses***
General Compliance Section - Please add language in the compliance section to address the requirements for archiving the closed circuit or video images discussed in M4 and M5. Any time duration beyond that of just a few days is going to require specific plans to rotate, store, and archive a large amount of video tapes.	Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are to be kept for 1 calendar year.
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Raymond A'Brial
Entity	Central Hudson Gas & Electric Corporation (CHGE)

Comments		***Responses***
General	CHGE feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Richard Engelbrecht
Entity	Rochester Gas and Electric

Comments		***Responses***
General	NPCC feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Robert Strauss
Entity	New York State Electric & Gas Corporation

Comments		***Responses***
General	NYSEG concurs with NPCC that CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.	Please refer to responses to comments on CIP-002. The "nearest six-wall boundary" was used to ensure that floors and ceilings were considered in the boundary. The term has been added to the definition of Physical Security Perimeter. Further clarification has been added to the FAQ
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	The point was to ensure protection of the assets, and the wording has been changed accordingly. R1.3 wording has been changed.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.	Changes have been made
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	Requirements and Measures have been modified and aligned. The measurements section now contain assessment criteria only, and detailed criteria in the requirements section
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	The table was provided to clarify the types of access controls that are acceptable, and latitude has been provided in the compliance section for duly authorized exceptions to a Responsible Entity's cyber security policy when it cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section.
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	The table was provided to clarify the types of access controls that are acceptable, and latitude has been provided in the compliance section for duly authorized exceptions to a Responsible Entity's cyber security policy when it cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section.

CIP-006 Drafting Team Responses to Comments

006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	The table was provided to clarify the types of access controls that are acceptable, and latitude has been provided in the compliance section for duly authorized exceptions to a Responsible Entity's cyber security policy when it cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section.
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	Modifications have been made. Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are to be kept for 1 calendar year.
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Roger Champagne
Entity	Hydro-Québec TransÉnergie

Comments		***Responses***
General	HQTÉ feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. The term "six-wall boundary" should be in the definitions. We recommend moving this information from question 16 under CIP-006 in the FAQ	Please see responses to comments by Robert Strauss, NYSEG.
006-R1	Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2. Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.	
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.	
006-M1	Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.	
006-M2		
006-M3	Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M4	Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M5	Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.	

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Roman Carter
Entity	Southern Company Generation

Comments		*Responses*
General	Purpose -- Define - six-wall boundary. Pg 6, Regarding levels of non-compliance: does -aggregate interruptions- refer to a centralized system, therefore assuming there is one?	Please see responses to comments by Marc Butts.
006-R1		
006-R2		
006-R3	Pg 4, R3, Regarding monitoring physical access control, what is meant by -generally accepted industry or government risk assessment procedure-? Monitoring physical access 24/7 will be very difficult for the many locations large companies have. Again, if substations w/ FRAD's are included, this would have far-reaching implications and tremendous costs.	
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3	Pg 4, M3; Regarding special locks: could you please define what a Man-trap might be?	
006-M4		
006-M5	Pg 5, M5; Regarding monitoring & logging physical access: per above, it sounds like either CCTV or an alarm system of some kind would be required at every substation w/ frame relay communication. While some may have this already, I would guess that many/most do not.	
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	Levels of Compliance, Levels 1 and 2 -- Are -aggregate interruptions in monitoring system availability- intended to be for a failure a one location or an aggregate of all Critical locations? If all locations, then how can a responsible entity with many Critical locations be held to the same composite (7 days or 1 month) as a responsible entity with only 1 or 2 locations?	

CIP-006 Drafting Team Responses to Comments

006-C2,2 Levels of Compliance, Levels 1 and 2 -- Are -aggregate interruptions in monitoring system availability- intended to be for a failure a one location or an aggregate of all Critical locations? If all locations, then how can a responsible entity with many Critical locations be held to the same composite (7 days or 1 month) as a responsible entity with only 1 or 2 locations?

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Scott R Mix
Entity	KEMA

	Comments	***Responses***
General	Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Physical Security of Critical Cyber Assets". There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual). Measures (general) There appears to be a lot of "implementation detail" included in the measures section. According to the NERC Reliability Standards Process Manual, measures are used to "assess performance and outcomes for determining compliance with the requirements. Specifying that a Responsible entity "shall implement one of the following ..." sounds like a requirement, not a measure. FAQ CIP-006-1.Q1 still refers to a "four-wall" boundary. FAQ CIP-006-1.Q11 is a duplicate of FAQ CIP-006-1.Q10. FAQ CIP-006-1.Q13 should be augmented to indicate that a fence provides only a "four-wall" boundary, not a "six-wall" boundary as required by the standard	Title has been modified. The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section. FAQs have been updated.
006-R1		
006-R2		
006-R3	Requirement R3 and R4: Please comment on the functional distinction between these requirements, and why they are specified separately.	The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section.
006-R4	Requirement R3 and R4: Please comment on the functional distinction between these requirements, and why they are specified separately.	The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section.
006-R5		
006-R6		
006-M1		
006-M2		

006-M3

006-M4

006-M5

006-M6

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Terry Doern
Entity	Bonneville Power Administration, Department of Energy

Comments		*Responses*
General		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5	Change 'Unauthorized Activity' to 'Unauthorized Access'.	Change made.
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Tim Hattaway
Entity	AECoop

Comments		*Responses*
General	This standard addresses physical security as it applies to cyber assets. For generation facilities, this is a small piece of the puzzle. Our security plans address physical security as it applies to all critical assets. We would apply the same philosophy for physical security to a DCS room as a water intake structure. Unless I'm misinterpreting this section of the regulations, it does not preclude this approach.	This standard does not preclude that approach, as long as the security plans meet the requirements of the standard.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Todd Thompson
Entity	Southwest Power Pool

Comments		***Responses***
General	Delete (nearest six-wall boundary) as this is already covered in the definition above or move it to the definition.	Change has been made.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	R6 -- Duplicates R1.	Duplication has been removed.
006-M1	M1 -- 90 days is not found in the requirements section.	This will now be covered only in the requirements section. The measurements and requirements in CIP006 have been reformatted to comply with the NERC reliability standards process manual. The measurements section will now contain assessment criteria only, and detailed criteria will be covered only in the requirements section.
006-M2		
006-M3	M3 -- this is too prescriptive and does not respect changing technologies. The words "or equivalent" would make this section better. The term "Security Officers" is confusing and should be changed to "Security Personnel".	The table was provided to clarify the types of access controls that are acceptable, and latitude has been provided in the compliance section for duly authorized exceptions to a Responsible Entity's cyber security policy when it cannot implement at least one of these requirements. The standard has been reformatted and this will now be covered in the requirements section. Change to Security Personnel has been made.
006-M4	M4. This is redundant. These requirements are referred to in R1 and M1.	Requirements and Measures have been modified.
006-M5		
006-M6		
006-C1,1		
006-C1,2		
006-C1,3	1.3 If the documents referred to are video records, then this is excessive, unless the documents relate to a significant security incident.	Modifications have been made. Logs (video, access, etc) are to be kept 90 days. If video is used as the primary method to log entry to the facility, then it must be kept for 90 days. Otherwise, the organization can select whatever retention period it deems reasonable for video images. All other documentation (i.e. security plan, procedures, access authorizations, etc) are

		to be kept for 1 calendar year.
006-C1,4		
006-C2,1	2.1.1 Not consistent with M1.	Requirements, Measures, and Levels of Non-compliance have been modified for consistency.
006-C2,2	2.2.1 Requires more stringent compliance than level 1 compliance.	Levels of Non-compliance have been modified and the drafting team believes they denote increasing severity of non-compliance.
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Tom Pruitt
Entity	Duke Power Company

	Comments	***Responses***
General	Overall -- Effective date of 10/1/05 for this standard is unrealistic due to the volume of systems and locations that must be modified or enhanced to become compliant with the required physical access restrictions. The entire issue of logging may need to be addressed. Does Duke have any "critical assets" in remote locations? How expensive is it going to be to meet the logging requirements? To implement manual logging as described in M5, the utility would have to automatically send two technicians on every job. And if one wanted to be devious, he'd just go back after hours when no-one is around. Plus, such manual logging is reactive at best. It won't prevent anything. Is this intended to require physical security (including logging, monitoring, maintenance and testing, etc.) at remote, unstaffed, substations? A - 4 -- typo? Any reference in this Standard to Critical.... Why is this listed here and in A - 3 in the other standards?	Please see the Implementation plan. Manual logging is just one of the acceptable logging controls, and would be accompanied in some facilities with human observation (i.e. security personnel). Yes, physical security is required at remote, unstaffed substations that contain critical cyber assets. The standards have been modified for consistency.
006-R1	R1.1. Need the definition of "defense strategy". This appears to be more than passive physical security provided by locks, etc.	This term has been removed.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3	M3 -- Security Enclosure is a nice addition to this requirement. It will still be a significant feat to get all the cabinets at these locations where they can be locked.	Noted.
006-M4		
006-M5		
006-M6		
006-C1,1		
006-C1,2		

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Tony Eddleman
Entity	Nebraska Public Power District

Comments		*Responses*
General		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5	Under section M5 - Manual logging - what constitutes human observation or remote verification?	Human observation is covered in further detail in the requirements. Typically this is a security officer or other personnel stationed at the access point to verify that the manual log is filled out.
006-M6		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		