CIP-005 Drafting Team Responses to Comments

Commentor	Bob Wallace
Entity	Ontario Power Generation

	Comments	*Responses*
General	OPG feels CIP-005 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.	Please see responses to CIP-002.
005-R1		
005-R2	OPG requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4	Requirement R4.2's third bullet is not clear. We recommend changing from << Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication. >> to << Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entity to utilize their static user id and password.) >>	These items have been moved to the FAQ document.
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Carol L. Krysevig
Entity	Allegheny Energy Supply Company

Comments		*Responses*
General		
005-R1	R1. Allegheny recommends that any devices controlling entry to the Electronic Security Perimeter should be considered Critical Assets. In other words, firewalls that protect an Electronic Security Perimeter should be considered as devices inside that perimeter.	Additional language has been added in R1 to require that cyber assets used for controlling and monitoring access to the Electronic Security Perimeter be protected as critical cyber assets within the perimeter.
005-R2		
005-R3		
005-R4	R4.2 -- Can you more specifically define INTERACTIVE, LOGICAL ACCESS? Almost any access could be deemed interactive since most data communication is bi-directional.	Language has been added to clarify the requirement.
005-R5	R5. - Some devices, such as PLCs, are not capable of being monitored for access. Responsible entities should be allowed to determine the assets inside the Electronic perimeter that need to be monitored directly. The only mandatory monitoring should be via the perimeter access device (firewall). Exact requirements such as this should not be specified. The responsible entity should create its own monitoring guidelines if desired.	The language in this requirement has been changed to clarify that the requirement refers to monitoring the Electronic Security Perimeter. Requirements for the Cyber Assets within the Electronic Security Perimeter are specified in CIP-007, System Security Management.
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3	Compliance, 1.3. Data Retention - The text in this section appears to be a carry over from the previous Standard's Data Retention section (personnel and training) and should be modified accordingly	The text has been removed.
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Earl Cahoe
Entity	Portland General Electric

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3	Requirements, R3 Recommended wording: The Responsible Entity shall secure dial-up modem connections. Protection of the connection may be either remote activation/de-activation of dial-up connectivity via SCADA commands from the security or control center, or by using encryption devices meeting security level 2, or better, of Federal Information Processing Standards Publication (FIPS PUB) 140-1, Security Requirements for Cryptographic Modules, to ensure authenticity of the accessing device and/or application. The use of encryption modems pairs that require a secure handshake negates the need for "physically deactivating" them.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4		
005-R5	Requirements, R5 Question: is this really necessary if encryption modems pairs utilizing a secure handshake are used? See R3 above.	This requirement specifies minimum monitoring requirements for logging of successful accesses as well as intrusion detection processes.
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Edwin C. Goff III
Entity	Progress Energy

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3	R3 - Standard should not be dictating a specific technical approach to disable dial-up modems using SCADA. This approach has the potential to add burden and distractions to transmission dispatcher duties.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4		
005-R5	R5 -- Clarification needed - "detecting unauthorized access (intrusions), and attempts at unauthorized access to the electronic perimeter(s) and Critical Cyber Assets within...24/7." -- use of native security logs at the host level are somewhat limited in their ability to accomplish this task -- the way this reads now looks like we would need HIDS or similar technology to manage this at the asset level. Is that the intent of this requirement? Clarification needed - Monitoring Electronic Access Control -- to perform this on the scale need to meet the intent of this standard as it is written today this would require a team of highly skilled folks, using very sophisticated/costly technology and would require a significant capitol investment in network and host intrusion prevention sensors. Is that the intent of this requirement?	This requirement requires that adequate measures are taken to log and monitor access or attempts at intrusion to the Electronic Security Perimeter. Technical measures such as firewalls and intrusion detection devices are built with features which may meet these requirements, in combination with appropriate processes.
005-R6	R6 - Eliminate the 90 calendar day review for configuration and process reviews. This should be conducted annually or upon changes to the configuration.	Consistent with requirements in other standards in this set, the review requirement has been amended to an annual review and updates for changes to be completed within 90 days.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

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

	Comments	*Responses*
General	National Grid believes CIP-005 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.	
005-R1		
005-R2	National Grid requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	National Grid believes that Requirement R3 - "Where remote activation of dial-up connectivity via SCADA-activated relays from the security or control center is technically feasible,....." is one of many solutions to securing dial-in access. Other solutions are bullet items under Requirement R4.2. National Grid highly recommends that Requirement R3 become another bullet item under Requirement R4.2. Otherwise the System Operator whose main task is to Monitor, Control and Operate the Bulk Power System becomes a clerk and begins performing tasks that are not part of their respective job functions.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4	Requirement R4.2's third bullet is not clear. We recommend changing from <<Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.>> to <<Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entity to utilize their static user id and password.)>>	These items have been moved to the FAQ document.
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 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 and measures will be reviewed and amended as required for consistency.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 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. In CIP-005 the FAQ should provide examples of access points. Are routers and firewalls the only types of access points? Specifically, for devices within the electronic security perimeter, are their keyboards/monitors and corresponding login mechanisms also considered to be access points?	This is stated in CIP-004 (Personnel & Training). Access points, as used in this standard, refer to access points to the electronic security perimeter.
005-R1		
005-R2	CIP-005 R2 is redundant with CIP-007 - R9. Delete CIP-005 R2 lefting this requirement in CIP-007	Additional language has been added to R2 to clarify that the requirement in this standard applies to access points on the perimeter.
005-R3	CIP-005 R3 and M3 uses the term "dial-up modem connections" which should include VPN access using networks. Remove the technology reference to modems and perhaps use "dial-up accessible" as in CIP-002 R2. In CIP-005 R3 we disagree with the requirement for dial-up access physical disconnection via SCADA. There are other ways to ensure secure dial-up access and this one method should not be listed as a must , rather it could listed as an option or alternative in the FAQs. In CIP-005 R3 while SCADA activated relays are a relatively secure mechanism, there are insecure aspects to it. For example, SCADA operators could be susceptible to social engineering attacks. Furthermore, there are arguably more secure methods (e.g. requiring two-factor authentication), so the method involving SCADA activated relays shouldn't be put forth as the most secure method. Also, this method is not feasible when stations allow dialup connectivity to be initiated both manually by people and automatically by computers.	The language in the standard has been modified where appropriate. The specific requirement R3 has been moved to the FAQ document.
005-R4		
005-R5	In CIP-005 R5 it is unclear what the Responsible Entity must respond to on a 7 x 24 basis. CIP-005 FAQ #6 implies that certain events must be responded to immediately. If that is the case then it should be stated in CIP-005 and that not all events require this level of response.	Incident response requirements are specified in CIP-008. This standard requires that access be monitored on a 7x24 basis.
005-R6	CIP-005 R6 "90 calendar days" should be changed to match the "annual" requirement in M6. Compliance sections in CIP-005 & CIP-006 should more closely align.	Consistent with requirements in other standards in this set, the review requirement has been amended to an annual review and updates for changes to be completed within 90 days.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		

CIP-005 Drafting Team Responses to Comments

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor	Gordon Pietsch
Entity	Great River Energy

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3	R3 should be modified by deleting all the language except the first sentence and the last sentence. In particular the reference to technically feasibility is to vague. It is adequate to require that entities implement procedures they have defined as appropriate based on their risk analysis.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Guy Zito
Entity	NPCC CP9

	Comments	*Responses*
General	CIP-005 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.	
005-R1		
005-R2	NPCC Participating Members request clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	Additional language has been added to R2 to clarify the requirement for access points on the perimeter.
005-R3	Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4	Requirement R4.2's third bullet is not clear. We recommend changing from <<Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.>> to <<Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entity to utilize their static user id and password.)>>	These items have been moved to the FAQ document.
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Howard Rulf
Entity We Energies

	Comments	*Responses*
General	Do the same requirements apply if the dial-up connections are used to monitor equipment only and do not permit control or modification of equipment? The Cyber Security Standard refers to Routable OSI-Open Systems Communications vs. Non-Routable communications (Master/Slave communications). Will security at the Modem Dial-up Access point be needed if OSI communications i.e. DNP Networking is used?	The entity must determine, in its risk assessment process, whether the cyber assets qualify as critical cyber assets. If they are, then the requirements apply. DNP is an application protocol. If the underlying protocol used is a routable protocol, and the cyber asset is critical, then the requirements apply. In this case, it is a dial-up accessible device, the requirements apply if it is a critical cyber asset.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor James W. Sample
Entity California ISO

	Comments	*Responses*
General	M2, M3.1 and M3.2 establish new requirements which are not covered in the requirements section.	The standards will be reviewed for consistency.
005-R1	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.	The repeated definition has been removed and the opening paragraph simplified.
005-R2		
005-R3	R3 – attended or unattended is irrelevant to security in this paragraph.	These terms have been removed from this standard.
005-R4	R4 – The phrase “and the Critical Cyber Assets within the Electronic Security Perimeter(s).” is confusing given that this standard refers to Electronic Security Perimeter.	Reference to the actual cyber assets in this item has been removed for clarification, since CIP-007 deals with host systems.
	R4.2 – Did y’all mean “remote access” or really “external interactive logical access”? Please clarify.	The access does not have to be remote. This refers to any access originating from outside the Electronic Security Perimeter.
	R4.2 – Suggest that indicating “Strong procedural or technical controls” is all that is required.	R4 has been restated to remove technology specific requirements.
	R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly.	
	R4.3 – should be removed. This is not a security measure but a legal support measure.	
005-R5	R5 – Monitoring authorized access should be replaced with logging authorized access.	The language has been amended.
005-R6	R6. We could find no requirements for the creation of any documents in the requirements section of this standard.	Requirements and measures have been reviewed and changed where appropriate.
005-M1	M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter which is not reflected in the requirements.	Requirements and measures have been reviewed and changed where appropriate.
005-M2		
005-M3		
005-M4		
005-M5	M5.2 – this appears to be the same as CIP 007, R 7/M6.	This measure refers to documents for monitoring electronic access control at electronic access points.
005-M6	M6 contradicts R6 of this standard.	This has been corrected.
005-C1,1		
005-C1,2	1.2 there is an inconsistency with CIP 007 R 7.1.	There is no inconsistency in these requirements.
005-C1,3		
005-C1,4	1.4.4 – Not consistent with requirements or measures.	1.4.4 has been amended to be consistent with requirements.

CIP-005 Drafting Team Responses to Comments

005-C2,1	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours.	2.1.2 deals with monitoring access control. The item will be amended to reflect monitoring at access points to the perimeter.
005-C2,2		
005-C2,3	2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would "record of [time period] validations or assessments". 2.3.3 – Delete this section because it is not measurable.	This item has been amended. Presuming that the comment refers to missing transactions, these can be revealed if access logs on a host system from an outside party is not matched by access records at the access
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Jerry Freese
Entity	American Electric Power

	Comments	*Responses*
General	This CIP has titles - again, we like the titles. All Requirements in CIP should have titles. Also, this CIP has a good relationship between the requirements and the measures. All off the CIP should use this model - the same number of requirements and measures.	
005-R1	R1 should be broken in to separate subrequirements.	R1 has been restructured to include sub-requirements for better clarity.
005-R2		
005-R3		
005-R4	n R4.2, consider removing "ANI" specifically. Refer to Caller ID generally.	These items have been moved to the FAQ document.
005-R5		
005-R6	R6 - the second half of this requirement is actually a measure. It already exists in M6, so it should probably be removed.	The requirement and measure have been amended for better clarity.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2	Compliance 1.2 - can this be two years instead of three years?	These have been moved to Data Retention.
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Jerry Heeren
Entity MEAG Power

	Comments	*Responses*
General		
005-R1	We suggest that the beginning of section R1 begin with, "To the extent technology allows, the Responsible Entity shall enable only those ports/services required…" Certain technologies (e.g., network hubs) do not allow for port by port configuration and disabling. Typically only Layer 2 and 3 switching/routing devices allow for the disabling of individual ports.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Jerry Litteer
Entity	INL

	Comments	*Responses*
General	Overall Missing items include: a) verifying the integrity (on BOTH production and test hosts) of the operating systems (e.g. no rootkits), reviewing file systems for unexpected files, directory structures or accounts. (CIP007 R5 integrity software?), b) excluded discrete communications and c) no review of logs In the case of Critical Cyber Assets, the security level assigned to these Electronic Security Perimeters is high. Suggest rewording too subjective.	System security is covered in CIP-007. This is part of the introductory text and not a requirement.
005-R1	R1. Discrete communications are excluded. Again this provides an opening for exploit.	The standard excludes communication between discrete Electronic Security Perimeters, but defines requirements for protecting the perimeter at all access points.
005-R2	R2 Disabling unused Network Ports/Services: a) text says shall enable only, and title should change from Disable to Enable Used Only. While I understand the difficulty in identifying all the ports and services used in these architectures (e.g. OPC) that's the point -- you can secure if you don't know.b) Missing a requirement to remove unused applications, this goes beyond ports and services. Eliminated all unused applications also reduces your patching complexity and unknown or unidentified security risks.	This standard deals with the Electronic Security Perimeter. The standard specifies an perimeter access model of deny by default unless explicitly allowed. Host security is covered in CIP-007.
005-R3		
005-R4		
005-R5	R5. Monitoring Electronic Access Control contains no requirement for frequency of review or alarm timing. Typical issue with logging information is that no body uses it again. 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 system that 'watches' the network 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-005-1.	The requirement only requires 24x7 monitoring. The standard is not prescriptive on the frequency of review and action is determined by the entity's risk assessment process. Standard CIP-008 defines requirements for incident reporting and handling.
005-R6		
005-M1		
005-M2	M2 change Disabling unused title and text to enable only used.	Title has been simplified.
005-M3	M3.1 annual audit of all dial-up modem connections is way too infrequent.	These are minimum requirements. Entities can implement more frequent audits based on their risk assessment.
005-M4		
005-M5	M5.3 review access records for authorized access -- no frequency specified.	The review of authorized users and their access rights falls under those required annually under what was formerly M6 (now R5).
005-M6		
005-C1,1	1.1.2 90 calendar days retention for access logs, firewall logs and intrusion detection logs is way too short given the nature of reluctance to share incidences until can't resolve on own or delay in time of recognition of unauthorized activity.	90 days is for retention of routine logs. Other records are required to be kept for one year. Incident Response, CIP-008, has requirements for data retention of incident related data.
005-C1,2		
005-C1,3		

CIP-005 Drafting Team Responses to Comments

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor Jim Hansen
Entity Seattle City Light

	Comments	*Responses*
General	Throughout this section the term ‘authorized access’ is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. Please remove the use of ‘shall’ in measures. ‘Shall’ should appear in the Requirements section only. For example, M1 -- ‘The Responsible Entity shall maintain’ should be changed to ‘The Responsible Entity maintains’.	Requirements for authorization processes are defined in CIP-003 - Security Management Controls. Authorized access implies that the access have been authorized using processes complying with requirements of CIP-003. The use of the term "shall" is standard in NERC measures and is consistent with language used in all NERC standards.
005-R1	R1 - There is a variety of equipment and software typically used in electronic security perimeter access control. We believe that this is what was intended by the word 'logical' in this section. Can you state this more clearly and also ensure that associated measures and compliance levels incorporate the concept that the electronic access point can be this group of hardware and software used to secure the perimeter? In some cases, a single system may be used in more than one logical perimeter. For example, a router may be used to implement level 1 and 2 security and a variety of target machines may implement other levels.	The term "logical" has been removed and the term "electronic" is used in requirements for CIP-005. It is used to denote access through electronic means, as contrasted to physical access. R1 defines requirements for identification of the Electronic Security Perimeter. R4 defines access control requirements.
005-R2		
005-R3	R3 -- ‘unattended’ usually has no bearing on securing and being aware of dial-in access. Should this second sentence read ‘…dial-up equipment shall be…’ instead?	The term unattended has been removed from this requirement. This requirement has also been moved as an option under access controls.
005-R4	R4.2 The measures would be more clear if specific examples were included. R4.2 - Should the word ‘logical’ in the first sentence be removed?	The team has made every effort to clarify the requirement. Examples are not typically included in a standard.
	R4 appears to be written with human access rather than software access to systems. Either can be ‘interactive’. We have numerous interactions with specific computers using specific ports and protocols in various DMZ’s outside of the electronic security perimeter of our EMS. A variety of methods are used to ensure that logins are never presented to anyone who could gain access to these systems outside the security perimeter and attempt unauthorized access. For example, a custom program receiving XML data delivered by another program across a normally unused port will reject any message that does not match the schema. While it is possible that someone could send a bogus XML data set complying with the schema. The damage would be limited to overwriting data that we could easily recover without threatening the reliability of the grid. The bullets in R4.2 do not cover any of these methods however we believe they effectively limit access through our electronic security perimeter.	"Logical" has been removed and "electronic" is used for requirements in CIP-005. This seeks to differentiate this access from physical access. Language has been added in this requirement to clarify the interactive access requirement.
	Would you please split R4 into two requirements? One governing login access or access on defined ports, and the other programmatic access using specialized application software and interfaces on non-standard ports? Also, we believe that login access into a security perimeter should be encrypted when possible in order to ensure integrity and privacy. Networks outside of the perimeter could allow network traffic to be captured and viewed (exposing ip addresses, ports, user id and passwords) or even captured and modified in transit.	
005-R5	R5 Please include ‘where technically feasible’ as this is not always possible with existing systems.	The requirement has been amended to apply, in this standard, to access points to the Electronic Security Perimeter. These monitoring controls are requirements which must be implemented.
	R5 ‘Monitoring’ implies active notification 7x24 when the events specified occur. In the case of Authorized Access, ‘Logging’ for audit purposes is important, however active notification is not. For unauthorized access attempts, (internally or at electronic perimeter(s)) active monitoring should be used. Please modify R5 to remove the requirement for monitoring authorized access.	The language in the standard has been amended to change "monitoring" in authorized access
005-R6		

CIP-005 Drafting Team Responses to Comments

005-M1	.M1 Since this standard focuses on Cyber Security, the document described in M1 should be limited to contain only the Electronic Security Perimeter(s). The remainder of the sentence should be struck as it is outside the scope of this SAR, increases the cost of compliance, and does nothing to increase Cyber Security.	The intent of this measure is to ensure that, not only has an Electronic Security Perimeter been defined, but that it has been defined to include and account for all critical cyber assets and to identify those non-critical cyber assets which are in the Electronic Security Perimeter, for application in other cyber security standards.
005-M2		
005-M3		
005-M4	M4 and 5 also appear to have been written with login access in mind. If you split R4 into two requirements as requested above, can you also create separate measures? It is not necessary to log authorized programmatic access for example when thousands of transactions using different sessions are conducted each hour.	The requirement has been clarified to define interactive access. The corresponding measures will be reviewed to ensure that they match and that they are consistent with requirements.
005-M5	M4 and 5 also appear to have been written with login access in mind. If you split R4 into two requirements as requested above, can you also create separate measures? It is not necessary to log authorized programmatic access for example when thousands of transactions using different sessions are conducted each hour.	See above.
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Jim Hiebert
Entity California ISO

	Comments	*Responses*
General	Throughout this section the term 'authorized access' is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example, M1 – 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'.	See responses to Jim Hansen of Seattle City Light.
005-R1	R1 - There is a variety of equipment and software typically used in electronic security perimeter access control. We believe that this is what was intended by the word 'logical' in this section. Can you state this more clearly and also ensure that associated measures and compliance levels incorporate the concept that the electronic access point can be this group of hardware and software used to secure the perimeter? In some cases, a single system may be used in more than one logical perimeter. For example, a router may be used to implement level 1 and 2 security and a variety of target machines may implement other levels.	
005-R2		
005-R3	R3 – 'unattended' usually has no bearing on securing and being aware of dial-in access. Should this second sentence read '…dial-up equipment shall be…' instead?	
005-R4	R4 appears to be written with human access rather than software access to systems. Either can be 'interactive'. We have numerous interactions with specific computers using specific ports and protocols in various DMZ's outside of the electronic security perimeter of our EMS. A variety of methods are used to ensure that logins are never presented to anyone who could gain access to these systems outside the security perimeter and attempt unauthorized access. For example, a custom program receiving XML data delivered by another program across a normally unused port will reject any message that does not match the schema. While it is possible that someone could send a bogus XML data set complying with the schema. The damage would be limited to overwriting data that we could easily recover without threatening the reliability of the grid. The bullets in R4.2 do not cover any of these methods however we believe they effectively limit access through our electronic security perimeter. Would you please split R4 into two requirements? One governing login access or access on defined ports, and the other programmatic access using specialized application software and interfaces on non-standard ports? R4.2 - Should the word 'logical' in the first sentence be removed? R4.2 The measures would be more clear if specific examples were included.	
005-R5	R5 Please include 'where technically feasible' as this is not always possible with existing systems. R5 'Monitoring' implies active notification 7x24 when the events specified occur. In the case of Authorized Access, 'Logging' for audit purposes is important, however active notification is not. For unauthorized access attempts, (internally or at electronic perimeter(s)) active monitoring should be used. Please modify R5 to remove the requirement for monitoring authorized access	
005-R6		

CIP-005 Drafting Team Responses to Comments

005-M1	M1 Since this standard focuses on Cyber Security, the document described in M1 should be limited to contain only the Electronic Security Perimeter(s). The remainder of the sentence should be struck as it is outside the scope of this SAR, increases the cost of compliance, and does nothing to increase Cyber Security.
005-M2	
005-M3	
005-M4	M4 and 5 also appear to have been written with login access in mind. If you split R4 into two requirements as requested above, can you also create separate measures? It is not necessary to log authorized programmatic access for example when thousands of transactions using different sessions are conducted each hour.
005-M5	
005-M6	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Commentor Joe Weiss
Entity KEMA

	Comments	*Responses*
General	FAQ 1. The schematic represents the electronic security perimeter for the Urgent Action Standard that does not address substations or power plants. A risk-based assessment should be performed to determine where the security perimeter should be established based on the cyber vulnerability of the RTU and networked substation control and diagnostic devices and the power plant networked control and diagnostics systems. This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment. FAQ 2. A risk-based assessment should be performed to determine the whether and to what level communications to networked control and diagnostic systems should be addressed. FAQ 3. A risk-based assessment should be performed to determine where the security perimeter should be established based on the cyber vulnerability of the RTU and dial-up substation control and diagnostic devices that are input to the RTU. FAQ 9. This should reference ISA TR 99.00.01-2004, Security Technologies for Manufacturing and Control Systems and ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment.	The schematic is intended to provide a general guidance of how an Electronic Security Perimeter can be defined. The standard includes all critical cyber assets as defined in the standard. Entities will define these critical cyber assets using a risk based assessment process. If the assessment determines that the entity must include communications lines, then the entity can define the Electronic Security Perimeter to include these communication facilities. By including these facilities, the entity must apply the requirements of these standards to these facilities as well. In most cases, it is more practical to restrict the Electronic Security Perimeter as close to the networked critical cyber assets themselves as possible and to control and monitor access at the access points to the perimeter. As communication facilities become increasing hosted using shared and untrusted physical infrastructures, the burden of authentication, authorization and integrity assurance will be shifted to protection in transit and at delivery to access points to the Electronic Security Perimeter.
005-R1		
005-R2	R2. To the extent possible, the Responsible Entity shall enable only those ports/services required for normal… It may not be practical or even possible to disable all unused ports and services for Critical Assets.	Additional language has been added to R2 to clarify the requirement for access points on the perimeter.
005-R3	R3. …Where remote activation of dial-up connectivity from Critical Assets is technically feasible, dial-up equipment in substations and power plants shall be physically deactivated, if possible, when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application. This is not just a SCADA issue and it may not be possible to disable the dial-up connection.	These items have been moved to the FAQ document.
005-R4		
005-R5		
005-R6		
005-M1		
005-M2	M2. To the extent possible, the Responsible Entity shall disable all unused ports and services, and where possible maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. It may not be practical or even possible to disable all unused ports and services or identify their status.	Additional language has been added to R2 clarify the requirement for access points on the perimeter. The measure will be correspondingly amended.
005-M3		
005-M4		
005-M5		
005-M6		

CIP-005 Drafting Team Responses to Comments

CIP-005 Drafting Team Responses to Comments

Commentor	John Lim
Entity	Con Edison

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-R6	R6/M6: R6 states 90 days while M6 states "annually". R6 should define an annual review, consistent with other cyber security standards.	The requirement and measure have been amended.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Karl Tammer
Entity ISO/RTO Council

Comments		*Responses*
General		
005-R1	R1 -- delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.	See responses to James W. Sample, California ISO.
005-R2		
005-R3	R3 -- attended or unattended is irrelevant to security in this paragraph.	
005-R4	R4 -- The phrase "and the Critical Cyber Assets within the Electronic Security Perimeter(s)." is confusing given that this standard refers to Electronic Security Perimeter. R4.2 -- Did y'all mean "remote access" or really "external interactive logical access"? Please clarify. R4.2 -- Suggest that indicating "Strong procedural or technical controls" is all that is required. R4.2 -- this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly. R4.3 -- should be removed. This is not a security measure but a legal support measure.	
005-R5	R5 -- Monitoring authorized access should be replaced with logging authorized access.	
005-R6	R6. We could find no requirements for the creation of any documents in the requirements section of this standard.	
005-M1	M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter which is not reflected in the requirements.	
005-M2	M2, M3.1 and M3.2 establish new requirements which are not covered in the requirements section.	
005-M3	M2, M3.1 and M3.2 establish new requirements which are not covered in the requirements section.	
005-M4		
005-M5	M5.2 -- this appears to be the same as CIP 007, R 7/M6.	
005-M6	M6 contradicts R6 of this standard.	
005-C1,1		
005-C1,2	1.2 there is an inconsistency with CIP 007 R 7.1.	
005-C1,3		
005-C1,4	1.4.4 -- Not consistent with requirements or measures.	
005-C2,1	2.1.2 -- This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours.	
005-C2,2		

CIP-005 Drafting Team Responses to Comments

005-C2,3

2.3.2 -- The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would "record of [time period] validations or assessments".

2.3.3 -- Delete this section because it is not measurable.

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor	Kathleen M. Goodman
Entity	ISO New England Inc.

	Comments	*Responses*
General	ISO-NE feels CIP-005 needs more work before it is ready for ballot M2, M3.1 and M3.2 establish new requirements, which are not covered in the requirements section.	
005-R1	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.	The repeated definition has been removed and the introductory paragraph simplified for better clarity.
005-R2	ISO-NE requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	The requirement has been clarified to refer to ports at access points.
005-R3	R3 – attended or unattended is irrelevant to security in this paragraph. We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2	These terms have been removed from this standard.
005-R4	R4 – The phrase <<and the Critical Cyber Assets within the Electronic Security Perimeter(s).>> is confusing given that this standard refers to Electronic Security Perimeter.R4.2 – Did y'all mean <<remote access>> or really <<external interactive logical access>>? Please clarify.R4.2 – Suggest that indicating <<Strong procedural or technical controls>> is all that is required.R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly.R4.3 – should be removed. This is not a security measure but a legal support measure.	Reference to the actual cyber assets in this item has been removed for clarification, since CIP-007 deals with host systems. The access does not have to be remote. This refers to any access originating from outside the Electronic Security Perimeter.
005-R5	R5 – Monitoring authorized access should be replaced with logging authorized access.	The item has been amended.
005-R6	R6. We could find no requirements for the creation of any documents in the requirements section of this standard.M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter, which is not reflected in the requirements	Requirements and measures have been reviewed and changed where appropriate.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5	M5.2 – this appears to be the same as CIP 007, R 7/M6.	The sections have been amended for consistency.
005-M6	M6 contradicts R6 of this standard.	The sections have been amended for consistency.
005-C1,1		
005-C1,2	1.2 there is an inconsistency with CIP 007 R 7.	The section has been amended for consistency.
005-C1,3		
005-C1,4		

CIP-005 Drafting Team Responses to Comments

005-C2,1	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours. 2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours.	2.1.2 deals with monitoring access control. The item will be amended to reflect monitoring at access points to the perimeter.
005-C2,2		
005-C2,3	2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would <<record of [time period] validations or assessments>> 2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would <<record of [time period] validations or assessments>>.	The section has been clarified.
005-C2,4		

CIP-005 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 responses to comments by the ECAR CIPP group.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 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. Measures M1-M3.2 need to have complementary requirements defined.	
005-R1	Migrate the definition of “Electronic Security Perimeter” from R1 to the definition section/faq section	The repeated definition has been removed and the introductory paragraph simplified for better clarity.
005-R2	The use of the word “port” needs to be better defined within Requirement 2.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	There’s no need to limit securing modems to unattended facilities, delete “unattended” in R3.	These terms have been removed from this standard.
005-R4	Migrate R4.2 “examples” to faq, Citing “strong procedural or technical measures” should suffice.	These items have been moved to the FAQ document.
005-R5	Change the word “monitoring” with “logging” in R5.	The word monitoring has been changed to logging for authorized access.
005-R6	R6 has no corroborating requirements for documentation.	Requirements and measures have been reviewed and changed where appropriate.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5	M5.2 appears in CIP 007, R7/M6.	This requirement refers to documentation for access points, as required by R5.
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Kenneth A. Goldsmith
Entity	Alliant Energy

Comments		*Responses*
General		
005-R1		
005-R2	Requirement R2 is same as CIP007 R9	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3		
005-R4		
005-R5	R5 - should state …for monitoring unauthorized access (rather than authorized)	The language has been changed to logging for authorized access, and monitoring for unauthorized access.
005-R6		
005-M1		
005-M2	Measurement M2 same as CIP007 M8	The measure has been modified to refer to access points.
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Kurt Muehlbauer
Entity	Exelon Corporation

	Comments	*Responses*
General	Levels of non-compliance under D2 do not allow for any gaps in monitoring. One minute of lost logging is a Level 1 violation. Since 100% uptime is almost impossible, no one could be compliant. The physical monitoring in CIP-006 has a better approach - it looks at aggregate gaps within a time period when measuring levels of non-compliance. We recommend replacing D2.1.2, 2.2.2, and 2.3.4 of this standard with the D2.1.2, 2.2.2, 2.3.2 from CIP-006. If the CIP-006 approach is not used, we recommend changing 2.1.2 to: Access to any Critical Cyber Asset was unmonitored for 24 hours or more. Recommend that the review period be yearly and only be specified in the measures section.	The sections have been amended for better clarity and sets a lower boundary.
005-R1	We believe that the risk-based assessment and applying greater protections to Critical Cyber Assets is a sound security practice introduced in this standard. However, applying all requirements of CIP-005 to non-Critical Cyber Assets within the defined Electronic Security Perimeter (referred to as other Cyber Assets in R3 of CIP-002) negates the benefits of the risk-based assessment. For other Cyber Assets, only R3 and R4 should be required. We recommend that the last sentence in R1 be changed to: Other Cyber Assets as identified in R3 of CIP-002 must comply with R3 and R4 of this standard.	R3 and R4 constitute the major access and monitoring requirements. The security of the perimeter is only as strong as its weakest component. For this reason, the access control and monitoring mechanisms at access points must include access to non-critical components as well if they share the same electronic security perimeter.
005-R2	R2 is almost identical to R9 of CIP-007. We recommend that this requirement only be specified in one standard.	R2 has been amended to clarify that it is applicable in this standard to controls at access points.
005-R3		
005-R4	The organizational and procedure references of R4 and M4 are redundant with R5 of CIP003. We recommend that R4 only address technical controls.	Controls can only be effective if all of technical, procedural and organizational components are implemented. Implementation of just technical controls without the corresponding procedural and organizational controls cannot be effective. CIP-003 approaches the requirements from a policy and governance point of view. CIP-005 requires that the technical , procedural and organizational controls specific to the electronic security perimeter be implemented.
005-R5		
005-R6	R6 calls for quarterly reviews of documentation and processes. M6 calls for annual reviews of documents. Process documentation is not likely to change very often, so quarterly reviews are of low value. We recommend that the review period be yearly and only be specified in the measures section.	The sections have been amended for consistency.
005-M1		
005-M2	M2 requires responsible entities to maintain documentation of all ports and services available on Critical Cyber Assets. This requirement will be very difficult to implement and of little value. We recommend removing this requirement.	M2 has been amended to apply to ports at access points. With a default stance of deny unless explicitly permitted, this documentation is a by product of the implementation of the permitted port configuration.
005-M3		
005-M4		

CIP-005 Drafting Team Responses to Comments

005-M5

005-M6

005-C1,1

005-C1,2

005-C1,3

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor L.W. Brown
Entity Edison Electric Institute

	Comments	*Responses*
General		
005-R1	R1. In the last line of this Requirement, reference is made to “this standard.” Since the original Standard 13430 has been divided into eight separate standards, it is no longer clear which standard is intended. For instance, does this refer to CIP-005-1, to the entire set from CIP-002-1 through CIP-009-1, or to some subset of the entire set?	References to this or other standards in the set will be clarified where required.
005-R2	R2. This Requirement is redundant here, as substantially identical material also appears in CIP-007.	The requirement has been clarified to apply to access points.
005-R3	R3. Is this intended to be the only permitted solution for dial-up modems? Alternative methods should be allowed.	These items have been moved to the FAQ document.
005-R4	R4.2. Is this intended to apply to dial-up modems as well? Is this intended to be the only permitted solution? Alternative methods should be allowed, such as by means of hardware devices. Moreover, it has been pointed out that the final bulleted method (“call back”) can be defeated.	These items have been moved to the FAQ document.
005-R5		
005-R6		
005-M1		
005-M2	M2. This Measure is redundant here, as substantially identical material also appears in CIP-007.	This has been clarified to apply to access points.
005-M3		
005-M4		
005-M5	M5. Is this intended to apply to dial-up modems as well? If so, there are serious technical difficulties with attempting to do so. M5.3. The original language is unclear and confusing. We suggest that it be clarified by changing it to read as follows: “…implemented to review all access and attempts in order to permit reports and alerts regarding unauthorized access and attempts…”	M5 applies to controls at all access points, including dial-up access, to the electronic security perimeter. The language will be reviewed and clarified if necessary.
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance 2.1.1, 2.2.2. The time periods in these items are more stringent than for physical	Requirements and measures for electronic security perimeters differ inherently from

	security of cyber assets. There does not appear to be a justifiable reason for such additional stringency, and these should be modified to conform to those. More, there needs to be a reasonable lower bound, as otherwise an Entity could be held noncompliant for even a one-second lapse. Twelve hours has been suggested as a reasonable lower	physical access. Where it is reasonable to make them consistent, they have been matched. In many cases, because of the very high frequency and automation which electronic attempts can utilize, the requirements and measures must necessarily match the additional
005-C2,2		
005-C2,3	Compliance 2.3.2. This item is redundant here, as substantially identical material also appears in CIP-007. Compliance 2.3.3.2. The word “some” is too vague. Either a firm lower limit needs to be established, or it should be clarified that interpretations will be acceptable for compliance purposes, even if they may differ from those of other entities or of auditors, as long as they are reasonable	These items have been reviewed and amended for clarity where warranted.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Larry Conrad
Entity Cinergy

	Comments	*Responses*
General	If a firewall is established between the operator consoles and the Secure LAN, will the operator consoles be considered outside of the Electronic Perimeter and the Physical Perimeter? If the operator consoles of a critical cyber asset communicate by non routable serial communications between the keyboard and mouse and the processor and remaining peripherals are secured within the physical and electronic perimeter, is it permissible for the keyboards, mouse and display device to be outside of the electronic perimeter? What if the keyboard and mouse are USB connected? To maintain the electronic perimeter, are the consoles required to meet the access requirements of CIP-005-1 Electronic Security, Section B.R4? Please clarify how the requirements would apply to "read-only" consoles that cannot impact the bulk electric system.	The risk assessment process should define which components are considered critical cyber assets, and an electronic perimeter defined around them and access points to the perimeter must be identified. Access through these access points to anything inside the perimeter must be protected. Consoles where you can issue commands to effect critical functions to critical assets would normally be considered a critical cyber asset. Read-only consoles, if outside the electronic perimeter, normally do not affect the reliable operation of the critical assets and therefore do not qualify as critical cyber assets, unless the loss of that console would affect the reliable operation of a critical asset.
005-R1		
005-R2		
005-R3		
005-R4	R.4.3.-- This requirement states ‘where technically feasible’. Some of the requirements in this section and in the Security Management Controls and Systems Security Management sections may NOT be technically feasible with legacy EMS systems. We recommend that organizations, which are in the process of replacing their EMS legacy systems, should be given the time to comply with requirements as they become ‘technically feasible’ after they implement the new EMS systems. We have made specific recommendations in the implementation section. R.4.3.-- Please explain how companies are to deal with the 24 X 7 monitoring of devices such as RTU’s. This 24 X 7 monitoring appears to be mandatory in requirements 4 and 5.	The implementation plan addresses these issues. The standard only addresses requirements.
005-R5	R. 5-- Change this language: "The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring ..." to the following: "The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, to log the following and review in a timely manner: monitoring authorized access, detecting unauthorized access..." R. 5-- This requirement should only be applicable to networks utilizing a routable protocol. The requirement may not be technically feasible otherwise.	The language has been clarified.
005-R6	R6. & C.M.6.-- R6 requirement calls for a review of the documents at least every 90 calendar days with updates made within 30 calendar days. However M6 states that the documents referenced in the standard should be reviewed annually. Is the review requirement every 90 days or annually? See general comments about standardizing the times for review and providing participants with a consistent schedule for updates and reviews. Recommend making the review an annual review rather than every 90 days. Annual should be sufficient time for this requirement.	The requirements and measures have been reviewed and changed where appropriate.

CIP-005 Drafting Team Responses to Comments

005-M1		
005-M2		
005-M3		
005-M4	M4.2.2-- Language states "...periodic review process...defined in CIP-003-1..." The review timing should be spelled out in the relevant CIPP document rather than referencing another section. Timing review requirements are poorly presented throughout the documents and need	The language has been reviewed and amended where appropriate.
005-M5		
005-M6	R6. & C.M.6.-- R6 requirement calls for a review of the documents at least every 90 calendar days with updates made within 30 calendar days. However M6 states that the documents referenced in the standard should be reviewed annually. Is the review requirement every 90 days or annually? See general comments about standardizing the times for review and providing participants with a consistent schedule for updates and reviews. Recommend making the review an annual review rather than every 90 days. Annual should be sufficient time for this requirement.	Consistent with requirements in other standards in this set, the review requirement has been amended to an annual review and updates for changes to be completed within 90 days.
005-C1,1		
005-C1,2		
005-C1,3	1.3-- Strike reference to personnel risk assessment documents as they do not pertain to this section at all.	The requirements and measures have been reviewed and changed where appropriate.
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3		
005-R4		
005-R5	Change to: The responsible Entity shall implement the organizational, technical, and procedural controls, including tools and procedures, to log the following and review in a timely manner: monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized access to the electronic perimeter(s) and Critical Cyber Assets within the perimeter(s), 24 hours a day, 7 days a week commensurate with the value of the asset.	The language of this has been clarified.
005-R6	Change to: The entity shall conduct a review of these documents at least annually to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes.	Consistent with requirements in other standards in this set, the review requirement has been amended to an annual review and updates for changes to be completed within 90 days.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3	Recommendations: Change data retention from three years to two years. This is a general comment which pertains to all of these standards. Also delete the language after the 2 year data retention requirement because it is not appropriate for Electronic Security and pertains to a different section, i.e., personnel risk assessments. Change to: Data Retention: The Responsible Entity shall keep documents specified in this standard for two calendar years.	Data retention has been rewritten for consistency.
005-C1,4		
005-C2,1	2.1.1.--Change to: Document(s) exist, but have not been updated with known changes within the 30 calendar day period and/or, D.2.1.2--Change to: Access to any Critical Cyber Asset was not logged for a period that does not exceed 24 hours.	The language has been clarified.
005-C2,2		
005-C2,3		

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor	Laurent Webber
Entity	WAPA Western Area Power Administration Western Area Power Administration

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3	R3 unattended facilities should be more clearly defined. An attended facility implies personnel on duty 24X7. A facility only (attended) 8 hours a day should still be defined as unattended.	References to unattended facilities have been removed.
005-R4	R4.2 The term (external interactive logical access) should be better defined or explained. R4.2: Since measures have special meaning in the CIPs, the last word before the bulleted list, (measures:), should be changed to (methods:).	These have been moved to the FAQ.
005-R5	R5 and M5: Requiring monitoring of authorized access for all Critical Cyber Assets within the perimeter creates a cascading and unreasonable requirement. If Critical Cyber Assets includes individual intelligent electronic devices, as it seems in CIP-002, the addition of thousands of expensive monitoring systems and log review and retention will crush most utilities. A reasonable requirement would be to apply this only to the electronic perimeter. In addition, clarify the 24x7 requirement. Does 24x7 apply to the log collection or does a person have to monitor 24x7?	The requirement has been amended to specify logging for authorized accesses.
005-R6	R6: 90 day document reviews are overkill; annual review is adequate.	Consistent with requirements in other standards in this set, the review requirement has been amended to an annual review and updates for changes to be completed within 90 days.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4	Compliance 1.4.1 seems too vague. It should more clearly list the documents to be made available for inspection.	The requirements and measures have been amended to clarify these requirements.
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Lawrence R Larson, PE
Entity	Midwest Reliability Organization

	Comments	*Responses*
General	The reference to "Document(s)" in the Levels of non-compliance is too vague - which documents specifically?	The requirements and measures have been amended to clarify these requirements.
005-R1		
005-R2		
005-R3	R3 should be modified by deleting all the language except the first sentence and the last sentence. In particular, the reference to technically feasibility is too vague. It is adequate to require that entities implement procedures they have defined as appropriate based on their risk analysis.	The specific R3 requirement has been moved to the FAQ document. Access control requirements for dial-up accessible devices have been moved as a sub-requirement of Access Control.
005-R4		
005-R5		
005-R6		
005-M1		
005-M2	M2 and 2.3.2 - disabling unused ports - this is redundant with language in 007, put in one or the other but not in both	Additional language has been added to clarify the requirement to apply to access points on the perimeter.
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3	M2 and 2.3.2 - disabling unused ports - this is redundant with language in 007, put in one or the other but not in both	Additional language has been added to clarify the requirement to apply to access points on the perimeter.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Lee Matuszczak
Entity	U S Bureau of Reclamation

	Comments	*Responses*
General		
005-R1	R1. - Consider including the first sentence of this requirement in the definition for "electronic security perimeter." R1. - The sentence beginning, "Access points to the …" is unclear. Consider revising to clarify or cite a representative example to illustrate.	The repeated definition has been removed and the introductory paragraph simplified for better clarity. The FAQ contains examples and clarifications.
005-R2		
005-R3	R3. - Please reconsider the practicality of this requirement with respect to remotely-located facilities, particularly under adverse weather conditions. Other cyber security control alternatives may be preferred.	This has been moved to the FAQ. The language of the requirement has been included in access controls of dial-up accessible cyber assets.
005-R4	R4.3 - Provide a sample banner. More importantly, indicate information that should NOT be included on a log-in banner (e.g., name of system, name of entity, anything indicating importance of system).	The FAQ contains examples.
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Linda Campbell
Entity	FRCC

	Comments	*Responses*
General		
005-R1	R1. Restates the definition of an Electronic Security Perimeter and the first sentence can be deleted. Upon the approval of this standard this term will be added to the NERC Glossary. The last sentence of the paragraph needs to be re-worded so as to mirror CIP-002-1 R3. Proposed language would be: The Electronic Security Perimeter would include any other Cyber Asset as defined in CIP-002-1 Requirement R3.	The repeated definition has been removed and the introductory paragraph simplified for better clarity.
005-R2	R2. Disabling unused Network Ports/Service is covered under CIP-007-1 and should be deleted from CIP-005-1. Both CIP-005-1 and CIP-007-1 have this requirement and its associated measurement and level of non-compliance.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	R3. Just because it may be technically feasible to remotely activate a dialup connection via SCADA, does not mean that is the most prudent control to implement. If Dialup is necessary because of a SCADA communications problem, then the responsible entity would have no way to access the device except physically, which could lead to a more serious incident. This is something that should not be dictated in the standard, but left to the individual organization to decide, so long as procedural and technical controls are in place over the dialin. We recommend removing this requirement, or providing it as an alternative to other procedural or technical controls that may be more effective.	These items have been moved to the FAQ document.
005-R4	R4.2. Where a firewall has been implemented to allow access only to and from certain specific IP addresses within the electronic perimeter, does the firewall have to implement one of the strong technical controls listed, or can the critical cyber asset be relied upon to provide the authentication requirement? For example, a server on the corporate network, or within another secure perimeter, has to communicate with a server within the perimeter. Can the authentication take place between the servers, or does the firewall have to provide authentication over and above IP address filtering?	The requirement refers to strong controls at the access points to the Electronic Security Perimeter(s).
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-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.	The compliance section has been rewritten.

CIP-005 Drafting Team Responses to Comments

005-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: 1.3.2.1. Keep documents specified in this standard for three (3) calendar years. 1.3.2.2. Keep personnel risk assessment documents for the duration of employee employment. 1.3.2.3. Keep contractor and service vendor records for the duration of their engagement. 1.3.2.4. Keep document revisions and security incident related data (such as unauthorized access reports) for three (3) calendar years. 1.3.2.5. Keep other audit records such as access records (e.g. access logs, firewall logs and intrusion detection logs) for a minimum of 90 calendar days.	The compliance section has been rewritten.
005-C1,4		
005-C2,1		
005-C2,2	Compliance, Levels of Non-compliance 2.2.2 How does an organization demonstrate compliance (i.e. prove it) with a level that states non-compliance if gap exists in system logs of between 1 and 7 days? How does an organization measure this across the multiple logs that are retained? Or does an organization report it only if it knows about it?	If an organization reports compliance (and therefore does not know of the gap) and a gap is revealed during an audit, it becomes non-compliant. If the organization knows about the gap, then it is required to report the non-compliance.
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Lyman Shaffer
Entity Pacific Gas and Electric Company

	Comments	*Responses*
General		
005-R1		
005-R2	R2- The requirement is very prescriptive. We're required to disable unused network ports. However, we should be allowed to use a different type of access control to ensure that unauthorized devices don't gain access to the network. We suggest the following working: Restricting access to the network: The Responsible entity shall restrict access to network ports to only those devices and individuals that are authorized to connect. This shall be accomplished through either a network authentication system such as 802.1xor by disabling unused ports on the network switches.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	R3 -- "Unattended" doesn't apply, you should comply with this requirement regardless if the facility is attended or unattended. (We find this control to be overly prescriptive by suggesting that the only method to secure modems is by enabling/disabling them via SCADA. There are other methods available and appears to be in conflict with R4.2 which suggests that dial-back is an acceptable method to secure modems.	The term "unattended" has been removed.
005-R4	R4.2 -- The word "logical" is not needed. R4, R4.2, & R5 -- The reference to "organizational, technical, and procedural controls" are not consistently used in R4 and R5 sections. R4.2 -- Digital certificates is a form of Two-factor authentication. Should be removed as it's own bullet and be used as an example for Two-factor authentication. R4.2 -- In the sentence "These strong procedural or technical measures shall include at least one of the following measures", "measures" should be replaced with "methods". R4.2.2 -- we are not comfortable with the proposed use of ANI as an authentication source for modems. Dial-up accessible critical cyber assets that do not support a network connection, such as substation IED's that expose only binary or ASCII serial interfaces, shall be secured using at least one of the measures listed in R4.2, or, alternatively, using at least one of the following (or similar) measures: - Physical activation and deactivation of the modem through SCADA, controlled by a control center or security center operator, logged, and subjected to appropriate authentication of the requesting party. - Installation of link encryptors that, together with an IED password, provide effective two-factor authentication. - Assignment (and periodic reassignment) of strong, unique passwords to all dial-up accessible IED's, and installation of a centralized, secure dial-out server that effectively preserves the secrecy of these passwords.	Te word "logical" has been removed and "electronic" is used in the requirements. These terms have been applied more consistently and the examples in 4.2 have been moved to the FAQ document.
005-R5	R5 -- Best practices is not to necessarily perform real-time monitoring of authorized access, but rather create logs to track authorized access in a manner that creates an audit trail. We agree that you should "monitor" unauthorized access attempts. So, this requirement should be worked in a way that allows for best practices without creating unnecessary administration overhead that doesn't reduce any risk.	The requirement has been amended to specify logging for authorized accesses.
005-R6		

CIP-005 Drafting Team Responses to Comments

005-M1	M1 -- Remove the reference to "all interconnected Critical Cyber Assets within the security perimeter." We agree with maintaining documents depicting the Electronic Security Perimeter(s) and all electronic access points, however, documents depicting interconnectivity within the security perimeter changes often and is captured in design and maintenance documents.	M1 has been revised for better clarity.
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

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

	Comments	*Responses*
General		
005-R1	Requirements R1-- In the last sentence, where it is explaining about non-critical cyber assets within the electronic perimeter and it states -these non-Critical Cyber Assets must comply with the requirements of this standard-, please clarify the word -this-. It is unclear as to whether it is implying that they must comply with CIP-005 only or if this is a holdover from when all the standards were under the one 1300 banner.	The intent is access to these devices through the perimeter access points be subject to the same access control and monitoring requirements at these access points.
005-R2	Pg 4, R2, Regarding disabling unused network ports/services: We are very dependent on our vendors for this info and they have thus far refused to provide this kind of detail free of charge. They want to do a -security assessment- and then give recommendations. We will have to pay for this and it will probably not be cheap. Some estimates were in the low tens of thousands of dollars.	This refers to ports at the access points and the requirement has been clarified to specify this. If a policy of deny by default at the network access point is implemented (as do most commercial firewalls), this is satisfied by default.
005-R3		
005-R4		
005-R5	Pg 5, R5, Regarding monitoring electronic access control: See CIP-002-1 above; if FRAD's in substations are subject to this, how would companies comply with this?	It depends on the type of FRAD and the logging facilities available on the FRAD.
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5	In Measure 5.2 -- The essence of this measure would seem to be to maintain documents to demonstrate the concept of -operational effectiveness- of the tools and procedures. Unless this concept is defined and utilized, these standards may be ineffective. Unless corroborating evidence such as detective controls is used to identify circumvention of -normal- access, logs can provide insufficient evidence of operational effectiveness because it may log only those instances when something did happen like it was suppose to and not those instances where it did not. Measure M5.3 --Consider changing -review access records for authorized access against access control rights- to -review access records for Unauthorized access against access control rights-. It is not a productive use of time to have personnel reviewing records for each and every cyber asset for authorized access. That time is better spent reviewing unauthorized access (failed logon attempts, etc) looking for suspicious -knocking on the door- type activity. Reviewing voluminous reports of legitimate access should not be a requirement.	Measures have been rewritten for better clarity. The intent is to ensure that persons who have access records are indeed duly authorized through normal procedures. Most of these checks can be automated.
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		

CIP-005 Drafting Team Responses to Comments

005-C2,1	2.1.2 (Level 1 Non-Compliance)-- All measures must have a reasonable lower bound and not be left open-ended. This one effectively generates non-compliance for ANY gap less than 24 hrs. It is suggested that this measure be made parallel with its physical security counterpart in CIP-006 which states -aggregate interruptions in system availability over a calendar year exist for more than 7 days but less than 1 month-. This at least allows you time to institute your backup monitoring plans should your primary fail without generating a non-compliance.	Levels of non-compliance have been reviewed and amended where appropriate.
005-C2,2		
005-C2,3	2.3 (Level 3 Non-Compliance)-- In 2.3.2, a non-compliance can be generated from -a record of regular audits does not exist-, but the standard only requires that all ports not used for -normal or emergency operations- be disabled. Measure M2 requires documentation of the required ports and services, but nowhere is there a requirement or measure for a regular audit. 2.3 (Level 3 Non-compliance) 2.3.3.2 needs to be deleted or clarified greatly. -Required documents exist, but records for some transactions are missing- is too vague. For example, exactly what transactions are required? How will the entity or an outside audit team know any are missing?	Levels of non-compliance have been reviewed and amended where appropriate.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Patrick Miller
Entity	PacifiCorp

Comments		*Responses*
General	For section B, R4.2, there are bulleted items which can not be referenced within the letter/number outline format. These items should be represented as R4.2.1 through R4.2.6 to correctly adhere to the outline format. For section C, M4.2, the submeasures are incorrectly referenced as M1.4.2 through M3.4.2. This should be corrected to refer to these submeasures as M4.2.1 through M4.2.3 to adhere to the outline format. If there is no 'real-time' requirement, it would be assumed that log review would satisfy this.	Formatting has been corrected.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Paul McClay
Entity Tampa Electric

	Comments	*Responses*
General		
005-R1	R1 states that non-critical assets within the electronic security perimeter must comply with the requirements of the standard. This is already stated in CIP-002 R1.16 and appears to be redundant here. Would recommend that either this be restated in every standard or deferred to CIP-002.	This has been removed from CIP-002 and is referenced in the individual standards where appropriate.
005-R2	R2 disable unused network services and port is redundant to CIP-007 R9. It should be stated in one standard to ensure that future modifications do not necessitate changes in two places. We would recommend CIP-007 as that appears to be the all inclusive section on server/device configuration. If a requirement is still needed in CIP-005 it should refer to CIP-007.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	R3 Just because it may be technically feasible to remotely activate a dialup connection via SCADA, does not mean that is the most prudent control to implement. If Dialup is necessary because of a SCADA communications problem, then the responsible entity would have no way to access the device except physically, which could lead to a more serious incident. This is something that should not be dictated in the standard, but left to the individual organization to decide, so long as procedural and technical controls are in place over the dialin. We recommend removing this requirement, or providing it as an alternative to other procedural or technical controls which may be more effective.	These items have been moved to the FAQ document.
005-R4	R4.2 Where a firewall has been implemented to allow access only to and from certain specific IP addresses within the electronic perimeter, does the firewall have to implement one of the strong technical controls listed, or can the critical cyber asset be relied upon to provide the authentication requirement? For example, a server on the corporate network, or within another secure perimeter, has to communicate with a server within the perimeter. Can the authentication take place between the servers, or does the firewall have to provide authentication over and above IP address filtering?	The requirement refers to strong controls at the access points to the Electronic Security Perimeter(s).
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		

CIP-005 Drafting Team Responses to Comments

005-C2,2	Compliance, Levels of Non-compliance 2.2.2 How does an organization demonstrate compliance (i.e. prove it) with a level that states non-compliance if gap exists in system logs of between 1 and 7 days? How does an organization measure this across the multiple logs that are retained? Or does an organization report it only if it knows about it? In addition, D1.4 indicates we would "supply for inspection" access logs. There will only be 90 days of access logs available, therefore logs cannot be audited for a year.	If an organization reports compliance (and therefore does not know of the gap) and a gap is revealed during an audit, it becomes non-compliant. If the organization knows about the gap, then it is required to report the non-compliance.
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Pete Henderson
Entity	Independent Electricity System Operator

	Comments	*Responses*
General	Purpose: The reference to “critical assets” should be changed to “Critical Cyber Assets M2, M3.1 and M3.2 establish new requirements which are not covered in the Requirements	See response to James Sample, California ISO.
005-R1	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant as it is defined in the definitions section above. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.	
005-R2	The wording of R2 fails to contemplate that having ports/services open for testing purposes may be required for an entity to “operate normally”	
005-R3	R3 – attended or unattended is irrelevant to security in this paragraph.	
005-R4	R4 – The phrase “and the Critical Cyber Assets within the Electronic Security Perimeter(s).” is confusing given that this standard refers to Electronic Security Perimeter. R4.2 – Did y’all mean “remote access” or really “external interactive logical access”? Please clarify. R4.2 – Suggest that indicating “Strong procedural or technical controls” is all that is required. R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly. R4.3 – should be removed. This is not a security measure but a legal support measure.	
005-R5	R5 – Monitoring authorized access should be replaced with logging authorized access.	
005-R6	R6. We could find no requirements for the creation of any documents in the “Requirements” section of this standard.	
005-M1	M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter which is not reflected in the Requirements.	
005-M2		
005-M3		
005-M4		
005-M5	M5.2 – this appears to be the same as CIP 007, R7/M6.	
005-M6	M6 contradicts R6 of this standard.	
005-C1,1		
005-C1,2	1.2 there is an inconsistency with CIP 007 R 7.1.	
005-C1,3	1.3 establishes a requirement (new to this standard) to retain personnel risk assessment documents. This requirement neither belongs in this section, nor does it belong in this standard. See also comments on CIP-004-1.	

CIP-005 Drafting Team Responses to Comments

005-C1,4	1.4.4 – Not consistent with requirements or measures.
005-C2,1	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability and availability of monitoring systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours.
005-C2,2	
005-C2,3	2.3.2 – The word audit establishes a new requirement and has specific connotations. The word regular is un-measurable. A better expression would be “record of [time period] validations or assessments”.
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Commentor	Randy Schimka
Entity	San Diego Gas and Electric Co

	Comments	*Responses*
General	We'd like to see a definition or differentiation made between different types of attended or unattended sites. Some sites have no permanent personnel assigned as their primary work location, but are staffed 3-4 days per week for 4-6 hours per day for maintenance or development work, as well as associated security personnel or other Facility tradespeople doing work in and around the facility. We would call that type of facility 'attended' unless directed otherwise.	Unattended has been removed from the standard.
005-R1		
005-R2		
005-R3	R3 - The requirements for securing modem connections are different for attended vs. unattended sites. Should this be the case? In our view, unsecure modem connections can make a system vulnerable, no matter whether a site is attended or unattended. 2. R3 - We strongly recommend that an electronic access system be used to control dial up access instead of relying on operations personnel to issue a control to the device and then shutting off access later. The electronic system should use access rosters, two-factored authentication, and logging through the use of a secure server. The benefits of this system are immediate updating, more accurate control, and electronic logging.	Unattended has been removed from the standard.
005-R4	R4.2 - We don't think the modem dial-back requirement is particularly effective against hackers. We suggest that the dial back requirement be dropped and replaced with a requirement to utilize electronic handshakes, certificates, or keys to establish a secure connection.	These items have been moved to the FAQ document.
005-R5	R5 - The discussion of monitoring electronic access and detecting unauthorized access 24x7 should be more fully defined. What response is required in the event of an unauthorized access, especially after normal business hours? R5 - We suggest adding "where technically feasible" in this section since many existing systems don't have these capabilities.	Incident Response Planning, CIP-008 addresses Incident Response.
005-R6	R6 and M6 - There is a discrepancy between these sections for the timeframes required. Annual documentation review is preferred.	Consistent with requirements in other standards in this set, the review requirement has been amended to an annual review and updates for changes to be completed within 90 days.
005-M1	M1 - We suggest removing 'and to the interconnected environment(s)'	This is no longer in the measure.
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		

CIP-005 Drafting Team Responses to Comments

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

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

	Comments	*Responses*
General	CHGE feels CIP-005 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.	See Response to Guy Zito, NPCC CP9
005-R1		
005-R2	CHGE requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	
005-R3	We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.	
005-R4	Requirement R4.2's third bullet is not clear. We recommend changing from << Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication. >> to <<Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entity to utilize their static user id and password.) >>	
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Richard Engelbrecht
Entity	Rochester Gas and Electric

Comments		*Responses*
General	NPCC feels CIP-005 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.	See response to Guy Zito, NPCC CP9
005-R1		
005-R2	NPCC Participating Members request clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	
005-R3	Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.	
005-R4	Requirement R4.2's third bullet is not clear. We recommend changing from <<Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.>> to <<Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entity to utilize their static user id and password.)>>	
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Richard Kafka
Entity	Pepco Holdings, Inc. - Affiliates

	Comments	*Responses*
General		
005-R1	R1. In the last line of this Requirement, reference is made to "this standard." Since the original Standard 1300 has been divided into eight separate standards, it is no longer clear which standard is intended. For instance, does this refer to CIP-005-1, to the entire set from CIP-002-1 through CIP-009-1, or to some subset of the entire set?	The intent is access to these devices through the perimeter access points be subject to the same access control and monitoring requirements at these access points.
005-R2	R2. This Requirement is redundant here, as substantially identical material also appears in CIP-007.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	R3 and R4.2. Is SCADA-activated relays required for all dialed up modems accessing Critical Assets? Is R3 and R4.2 intended to be the only permitted solution for dial-up modems? Alternative methods should be allowed such as hardware keys. Note the call back can be defeated. Dial-back modems have proven to be an insecure means of user authentication. From Schweitzer Engineering Laboratories paper, Attack and defend tools for remotely accessible control and protection equipment in electric power systems, available at http://www.selinc.com/techpprs/6132.pdf, pg. 16. Dial-back security was once common in the electric power industry, but is no longer adequate because of dial-back spoofing. Hackers have learned to fake the hang-up tone and remain on the line while the called modem attempts to dial its predefined dial-back number. Hackers just ignore the incoming dial tones and issue an answer tone that reestablishes connection to the dial-back modem. Thus, the dial-back has been spoofed or fooled into an unauthorized connection.	These items have been moved to the FAQ.
005-R4	R3 and R4.2. Is SCADA-activated relays required for all dialed up modems accessing Critical Assets? Is R3 and R4.2 intended to be the only permitted solution for dial-up modems? Alternative methods should be allowed such as hardware keys. Note the call back can be defeated. Dial-back modems have proven to be an insecure means of user authentication. From Schweitzer Engineering Laboratories paper, Attack and defend tools for remotely accessible control and protection equipment in electric power systems, available at http://www.selinc.com/techpprs/6132.pdf, pg. 16. Dial-back security was once common in the electric power industry, but is no longer adequate because of dial-back spoofing. Hackers have learned to fake the hang-up tone and remain on the line while the called modem attempts to dial its predefined dial-back number. Hackers just ignore the incoming dial tones and issue an answer tone that reestablishes connection to the dial-back modem. Thus, the dial-back has been spoofed or fooled into an unauthorized connection.	These items have been moved to the FAQ.
005-R5		
005-R6		
005-M1		
005-M2	M2. This Measure is redundant here, as substantially identical material also appears in CIP-007.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-M3		
005-M4		
005-M5	M5. Is this intended to apply to dial-up modems as well? If so, there are serious technical difficulties with attempting to do so. M5.3. The original language is unclear and confusing. We suggest that it be clarified by changing it	The requirement and measure has been amended.

	to read as follows: "…implemented to review all access and attempts in order to permit reports and alerts regarding unauthorized access and attempts…"	
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance 2.1.1, 2.2.2. The time periods in these items are more stringent than for physical security of cyber assets. Suggest that the time periods here be made the same as those listed for Physical security of cyber assets. More, there needs to be a reasonable lower bound, as otherwise an Entity could be held noncompliant for even a one-second lapse. Twelve hours has been	The levels of non-compliance have been rewritten.
005-C2,2	Compliance 2.1.1, 2.2.2. The time periods in these items are more stringent than for physical security of cyber assets. Suggest that the time periods here be made the same as those listed for Physical security of cyber assets. More, there needs to be a reasonable lower bound, as otherwise an Entity could be held noncompliant for even a one-second lapse. Twelve hours has been	The levels of non-compliance have been rewritten.
005-C2,3	Compliance 2.3.2. This item is redundant here, as substantially identical material also appears in CIP-007.	The levels of non-compliance have been rewritten.
	CIP-005-1 The word "some" is too vague in Compliance 2.3.3.2. How will an auditor judge "some"	
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Robert L. Sypult
Entity	Southern California Edison

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3	Section CIP 005-R3 instructs HOW to implement this standard, as opposed to defining the specifics needs. It is too prescriptive. This section only needs general guidelines and the responsible entity can determine HOW to meet the compliance requirements. This section should simply state "Responsible entity shall secure dial-up modem connections", and let the responsible entity determine HOW to accomplish that	The section has been moved to the FAQ.
005-R4	Section CIP 005-R4.2 This section is also too prescriptive, and it is questionable if some of the bullet items included would be feasible (e.g., "In dial-up access, call back to augment static user id and password authentication"). We do not feel we should be instructed on how to specifically address the problem in terms like "…..include at least one of the following measures:", but this section should be modified to reflect "….these strong procedural or technical measures shall include measures like…" and let the responsible entity determine the appropriate measures to address the concern.	These items have been moved to the FAQ.
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Robert Strauss
Entity	New York State Electric & Gas Corporation

	Comments	*Responses*
General	NYSEG concurs with NPCC that CIP-005 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.	See response to Guy Zito, NPCC.
005-R1		
005-R2	We request clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	
005-R3	Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.	
005-R4	Requirement R4.2's third bullet is not clear. We recommend changing from <<Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.>> to <<Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entity to utilize their static user id and password.)>>	
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Roger Champagne
Entity	Hydro-Québec TransÉnergie

Comments		*Responses*
General	HQTÉ feels CIP-005 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.	See response to Guy Zito, NPCC.
005-R1		
005-R2	HQTÉ requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.	
005-R3		
005-R4	Requirement 4.2's third bullet is not clear. We recommend changing from <<Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.>> to <<Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call an administrator will enable access allowing the entity to utilize their static user id and password.)>>	
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Roman Carter
Entity	Southern Company Generation

Comments		*Responses*
General		See response to Marc Butts, Southern Company
005-R1	Requirements R1-- In the last sentence, where it is explaining about non-critical cyber assets within the electronic perimeter and it states -these non-Critical Cyber Assets must comply with the requirements of this standard-, please clarify the word -this-. It is unclear as to whether it is implying that they must comply with CIP-005 only or if this is a holdover from when all the standards were under the one 1300 banner.	
005-R2	Pg 4, R2, Regarding disabling unused network ports/services: We are very dependent on our vendors for this info and they have thus far refused to provide this kind of detail free of charge. They want to do a -security assessment- and then give recommendations. We will have to pay for this and it will probably not be cheap. Some estimates were in the low tens of thousands of dollars.	
005-R3		
005-R4		
005-R5	Pg 5, R5, Regarding monitoring electronic access control: See CIP-002-1 above; if FRAD's in substations are subject to this, how would companies comply with this?	
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5	In Measure 5.2 -- The essence of this measure would seem to be to maintain documents to demonstrate the concept of -operational effectiveness- of the tools and procedures. Unless this concept is defined and utilized, these standards may be ineffective. Unless corroborating evidence such as detective controls is used to identify circumvention of -normal- access, logs can provide insufficient evidence of operational effectiveness because it may log only those instances when something did happen like it was suppose to and not those instances where it did not. Measure M5.3 --Consider changing -review access records for authorized access against access control rights- to -review access records for Unauthorized access against access control rights-. It is not a productive use of time to have personnel reviewing records for each and every cyber asset for authorized access. That time is better spent reviewing unauthorized access (failed logon attempts, etc) looking for suspicious -knocking on the door- type activity. Reviewing voluminous reports of legitimate access should not be a requirement.	
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		

CIP-005 Drafting Team Responses to Comments

005-C2,1	2.1.2 (Level 1 Non-Compliance)-- All measures must have a reasonable lower bound and not be left open-ended. This one effectively generates non-compliance for ANY gap less than 24 hrs. It is suggested that this measure be made parallel with its physical security counterpart in CIP-006 which states -aggregate interruptions in system availability over a calendar year exist for more than 7 days but less than 1 month-. This at least allows you time to institute your backup monitoring plans should your primary fail without generating a non-compliance.
005-C2,2	
005-C2,3	2.3 (Level 3 Non-Compliance)-- In 2.3.2, a non-compliance can be generated from -a record of regular audits does not exist-, but the standard only requires that all ports not used for -normal or emergency operations- be disabled. Measure M2 requires documentation of the required ports and services, but nowhere is there a requirement or measure for a regular audit. 2.3 (Level 3 Non-compliance) 2.3.3.2 needs to be deleted or clarified greatly. -Required documents exist, but records for some transactions are missing- is too vague. For example, exactly what transactions are required? How will the entity or an outside audit team know any are missing?
005-C2,4	

CIP-005 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 "Electronic Security of Critical Cyber Assets". The compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual). FAQ CIP-005-1.Q1 should be augmented to include one RTU with an electronic security perimeter surrounding it, with an explanatory note indicating that it communicates with the central site using a routable protocol. In FAQ CIP-005-1.Q5, the sentence beginning "A strong authentication scheme is usually defined as one" appears to be missing some words.	Requirements and measures have been reviewed and changed where appropriate. The requirement for remote critical cyber assets which are dial-up accessible has been clarified.
005-R1		
005-R2	Requirement R2 is duplicated in CIP-007-1 as requirement R9. Since standard CIP-005-1 deals with the electronic perimeter, the requirement should be deleted from standard CIP-005-1 (and remain in standard CIP-007-1). (If the requirement stays in CIP-005-1, please refer to my comment concerning CIP-007-1 R9.)	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3	Requirement R3: Replace requirement with: R3: The Responsible Entity shall Secure dial-up modem connections. R3.1: In unattended facilities, where remote activation of dial-up connectivity via SCADA-activated relays from the security or control center is technically feasible, the dial-up equipment shall be physically deactivated when not in approved use and remotely activated upon approval of activation. R3.2: In all other cases, the Responsible Entity shall normally disable unneeded dial-up connectivity, and implement procedural or technical measures to enable the dial-up connectivity after ensuring the authenticity and authorization of the accessing user, device and/or application.	This item has been moved to the FAQ.
005-R4		
005-R5		
005-R6		
005-M1	Measure M1. Change the first sentence to read "…all interconnected Cyber Assets (Critical and otherwise) within the security perimeter, …"	This clause has been removed.
005-M2	Measure M2. See comment concerning Requirement R2.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-M3		
005-M4	Measures M4.2.1, M4.2.3, move to standard CIP-003-1. These are procedural and belong in the Management Control section, not the technical Electronic Security section.	Electronic Security is not a technical standard. It has a strong technical content, but inludes procedural controls as well.
005-M5		

CIP-005 Drafting Team Responses to Comments

005-M6

005-C1,1

005-C1,2

005-C1,3

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor	Steven L Townsend
Entity	Consumers Energy

Comments		*Responses*
General	There is still redundancy in the standards, i.e. – unused ports/services appears in CIP-005-1 and CIP-007-1 standards. While it is understood that each of the standards needs to stand alone on its own merits, what assurances are there that a future revision to one standard will not cause a conflict with the same item in another standard.	The standard has been reviewed and amended where appropriate.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor	Terry Doern
Entity	Bonneville Power Administration, Department of Energy

Comments		*Responses*
General		
005-R1		
005-R2	R2. : Replace where it states 'The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets' with 'The Responsible Entity shall enable only those ports/services required for normal and emergency operations and monitoring of Critical Cyber Assets'. R2.3 and R3 Issue: Requirement discusses Electronic and Physical Security Perimeters. The physical and electronic perimeter should not alone be a factor for producing a list of Critical Cyber Assets. While it is best practice to hold all cyber systems within an electronic security perimeter to the highest network security requirements, it does not, by default, make them all Critical Cyber Assets. One system in the network could be turned off without impact to the mission while the other cannot. e.g. Incident response, while required, will be different for non-critical assets. Recommendation: Delete R2.3 and R3. R3 is taken care of by the last sentence of CIP-003-1 R1. CIP-002 should be limited to the requirements for identifying critical cyber assets.	The requirement has been amended to include ports necessary for monitoring critical cyber assets within the perimeter.
005-R3	R2.3 and R3 Issue: Requirement discusses Electronic and Physical Security Perimeters. The physical and electronic perimeter should not alone be a factor for producing a list of Critical Cyber Assets. While it is best practice to hold all cyber systems within an electronic security perimeter to the highest network security requirements, it does not, by default, make them all Critical Cyber Assets. One system in the network could be turned off without impact to the mission while the other cannot. e.g. Incident response, while required, will be different for non-critical assets. Recommendation: Delete R2.3 and R3. R3 is taken care of by the last sentence of CIP-003-1 R1. CIP-002 should be limited to the requirements for identifying critical cyber assets.	The requirement has been clarified to specify that CIP-005 requirements for access control and monitoring apply to these devices.
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		

CIP-005 Drafting Team Responses to Comments

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor	Todd Thompson
Entity	Southwest Power Pool

	Comments	*Responses*
General	M2, M3.1 and M3.2 establish new requirements which are not covered in the requirements section	See response to James Sample, California ISO.
005-R1	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.	
005-R2		
005-R3	R3 – attended or unattended is irrelevant to security in this paragraph.	
005-R4	R4 – The phrase “and the Critical Cyber Assets within the Electronic Security Perimeter(s).” is confusing given that this standard refers to Electronic Security Perimeter. R4.2 – Did y’all mean “remote access” or really “external interactive logical access”? Please clarify. R4.2 – Suggest that indicating “Strong procedural or technical controls” is all that is required. R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly. R4.3 – should be removed. This is not a security measure but a legal support measure.	
005-R5	R5 – Monitoring authorized access should be replaced with logging authorized access.	
005-R6	R6. We could find no requirements for the creation of any documents in the requirements section of this standard.	
005-M1	M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter which is not reflected in the requirements.	
005-M2		
005-M3		
005-M4		
005-M5	M5.2 – this appears to be the same as CIP 007, R 7/M6.	
005-M6	M6 contradicts R6 of this standard.	
005-C1,1		
005-C1,2	1.2 there is an inconsistency with CIP 007 R 7.1.	
005-C1,3		
005-C1,4	1.4.4 – Not consistent with requirements or measures	
005-C2,1	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours.	
005-C2,2		

CIP-005 Drafting Team Responses to Comments

005-C2,3

2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would “record of [time period] validations or assessments”.

2.3.3 – Delete this section because it is not measurable.

005-C2,4

CIP-005 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 that must be documented and setup for monitoring. We are still getting our hands around this one.	A new draft of the implementation plan has been published.
	A - 4 – typo? Any reference in this Standard to Critical…. Why is this listed here and in A - 3 in the other standards?	The standards have been reviewed for consistency.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		The implementation plan takes implementation time frames into account.
	R5: this is a HUGE effort. It will take a LONG time to implement.	
005-R6	R6: this is an even LARGER effort than #R5 above. It will take an even LONGER time to implement.	The implementation plan takes implementation time frames into account.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Tony Eddleman
Entity Nebraska Public Power District

	Comments	*Responses*
General		
005-R1	Under section R1. - What constitutes a secure gateway across the electronic security perimeter? If a firewall can be used and an entity uses a firewall in conjunction with a routable protocol, does this conflict with requirements in CIP-002-1, R2.1	The routable protocol criteria applies to how you would qualify a critical cyber asset under these standards.
005-R2		
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Commentor Trevor Tidwell

Entity Texas-New Mexico Power Company

	Comments	*Responses*
General	Logical access is mentioned several times in the document, but remains vague as to what it is. There are several types of electronic or logical access, but have varying degrees of risk. A VPN or a dial-up access to a network where the computer getting access is a high risk because the setup allows for greater access and visibility to the secure network. However a user getting access through a firewall only to view a web page from a web server on the secure network is less of a risk, because the user can only access port 80 of that machine provided a properly setup firewall. Right now we use a web server to allow personnel access to SCADA information. No one logging into the web site regardless of privileges can control any devices. Is this considered have authorized access to a Critical Cyber Asset, since the server is in the control center and uses a routable protocol? Do all the web users than have to go through the training required for personnel with electronic access to a Critical Cyber Asset. Also logical access does not seem to cover what to do for ICCP links. Not all ICCP links go to other companies that the NERC CIPs would apply to. Some ICCP links are used to connect to other computer systems on non-secure networks that use the data.	This is exactly why non-critical assets within the secure network must be protected for access and monitoring. The standard requires that access through the Firewall be subject to the access control and monitoring requirements of CIP-005. In this scenario, since access to the Web server is interactive and originates from outside the perimeter, you must implement strong controls. These types of requirements typically have the Web server outside the Firewall with the Web application access the back-end data across the Firewall using an application port. If the ICCP link accesses an electronic security perimeter which contains critical and non-critical cyber assets, the requirements of this standard (CIP-005) applies at the access points, irrespective of whether the ICCP link services a critical or non-critical asset within that perimeter.
005-R1		
005-R2	Requirement R2 is regarding Disabling unused Network Ports/Services, however it is also stated in CIP-007 R9. This should be either in only one CIP or each should be more specific to what the CIP is covering. R2 could just cover disabling unused Network Ports/Services on all electronics access points. The similar wording could be used in CIP-007, where the Network Ports/Services applied only to Critical Cyber Assets. See my CIP-007 comments for the more detailed suggestion. If no distinction is to be made in the Network Ports/Services wording between the two CIPs then it should only be in CIP-007. Also R2 should have a caveat for Critical Cyber Assets that do not access a wide-area network, the Internet, or to another device that is connected to non-secure network (e.g., printer). This caveat is already in CIP-007 R5.1 regarding Integrity Software. Disabling unused Network Ports/Services can be difficult since it is not always clear what Ports or Services are being used. Unused ports or services are only a threat it the machine is accessible by a malicious threat. Such threat would have to be on the electronic network, which already has physical security, electronic access control, and integrity software on the machines that access unsecured networks protecting it. Requiring disabling unused Network Ports/Services is overkill for devices that cannot reach unsecured networks.	Additional language has been added to R2 to clarify the requirement to apply to access points on the perimeter.
005-R3		
005-R4		
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		

CIP-005 Drafting Team Responses to Comments

005-C1,1

005-C1,2

005-C1,3

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Commentor	William J. Smith
Entity	Allegheny Power

Comments		*Responses*
General		
005-R1		
005-R2		
005-R3		
005-R4	R4.2 -- The specific procedural and technical measures are too prescriptive and don't allow for future technology advances. They should be removed from the standard and placed in the FAQ document as examples of strong procedural and technical measures.	These items have been moved to the FAQ.
005-R5		
005-R6		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-M6		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		