CIP-007 Responses to Comments

Commentor Bob Wallace
Entity Ontario Power Generation

	Comment	*Response*
General	OPG feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1	Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>> to <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>> We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.	The assumption that every entity has a test system is incorrect. The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. This will be clarified in draft three.
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive and should be deleted. The <<monthly review>> in Requirement R4.2 is too prescriptive. We recommend changing R4.2 from << The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.

	>> to << The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch. >> Add <<where technically feasible>> to the end of Requirement R4.3.	
007-R5	Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means. Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3. The combined requirement should allow technically feasible alternative solutions. Change Requirement R5.2 from <<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> to <<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.>> to <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>	1) Yes, the Responsible Entity identifies the appropriate system logs to retain. Each Responsible Entity's systems environment will be at least a little different, so only the Entities themselves can appropriately determine an adequate strategy. 2) Good and valid suggestions all, and in Draft 3 we think we have words more reflective of what you have suggested. The Requirements section has been significantly altered in Draft 3, with some material moved to other sections. We should be pretty close to the intentions outlined in the comment, but if additional word smithy is felt to be necessary, please offer those suggestions during the Draft 3 comment period.
007-R6	1) Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>> 2) Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>> 3) Change Requirement 6.1.4 from <<Security patches and anti-virus version levels>> to <<Assessing security patches and/or anti-virus version levels, as appropriate>> 4) The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an attended facility?	1) Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007. 2) Acknowledged. These matters are now addressed in R9. 3) Acknowledged. These matters are now addressed in R9.

007-R7	The title of Requirement R7 is too broad. We recommend changing this title from <<Retention of System Logs>> to <<Retention of Appropriate System Logs>> The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8		4) Acknowledged. The distinction between attended and unattended facilities has been removed.
007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The standard has been update to clarify when change management is required.
007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	This requirement has been deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.
007-M5	Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>	The drafting team has updated the measures to follow the restructured requirements.

CIP-007 Responses to Comments

007-M6		
007-M7		
007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.	The drafting team agrees with the comment and has updated the standard.
007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2	Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor Carol L. Krysevig
Entity Allegheny Energy Supply Company

Comment		*Response*
General		
007-R1	R1. - Will third party testing be allowed? Power stations have a fairly wide variety of specialized equipment and having non-production systems for each type of equipment is not feasible.	If a third party has an environment that closely simulates an entities production environment and is able to conduct the appropriate security tests for your environment, this is acceptable.
007-R2		
007-R3	R3. -- How are devices that do not support any type of passwords to be handled? The responsible entity should be able to devise its own guidelines and requirements. R3.2 - In power station control rooms, generic accounts are used. In some cases because they are required by the application software, and in other cases because these systems cannot be unavailable for use at any time. If there is no other alternative, this type of account should be allowed, but computers using this type of account should be configured to disallow any kind of administrative access using these accounts, if possible. The responsible entity should be allowed to devise its own guidelines and requirements	The drafting team will update the standard to reflect when technically feasible. The requirement states these accounts should be removed where possible. If their use is required, the entity is required to have a procedure in place for managing access to these accounts.
007-R4		
007-R5		
007-R6		
007-R7	R7. - Some systems will be very difficult if not impossible to configure for this type of logging. The responsible entity should be allowed to implement logging on those systems they deem need it.	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8		
007-R9	R9. - This is a duplicate. It has also been covered in Standard CIP-005-1.	The requirement has been revised to clarify that CIP-005 covers equipment on the electronic perimeter and CIP-007 covers equipment inside the perimeter.
007-R10		

CIP-007 Responses to Comments

CIP-007 Responses to Comments

Commentor Dave McCoy
Entity Great Plains Energy Cyber Security Task Force

Comment		***Response***
General	Please define what is meant by "attended facility" and "unattended facility".	The reference to attended and un-attended will be removed from CIP-007 in Draft 3. The reference was intended for field devices and will be clarified as such in Draft 3.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		

CIP-007 Responses to Comments

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor	Dennis Kalma
Entity	Alberta Electric System Operator (AESO)

Comment		***Response***
General		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5	R5.4 Syntax: repetitive (better word) Grammar: is necessary R5.4. This is a confusing point. Not sure what this is trying to achieve.	The drafting team agrees and has restructured the requirement.
007-R6		
007-R7		
007-R8	R8.2 Why not say that all controlled development and test environments should be located in controlled sites. We disagree with the premise that unattended sites present an additional degree of risk when appropriately secured.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity.
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Earl Cahoe
Entity Portland General Electric

	Comment	*Response*
General	Recommendation: Creating a duplicate test environment can be very expensive. Suggest adding language that allows the vendor's testing results to be used especially if the support is outsourced to the vendor.	Security testing is to verify that changes to systems comply with the entity's cyber policies and does not compromise current cyber security controls. The vendor can not necessarily test for these. If the vendor can document their tests follow your Security Test Procedures and test for your environment then this is acceptable. The standard will be updated to clarify the intent.
007-R1		
007-R2	Requirements, R2 Comment: The wording is confusing. We're not sure what is intended.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3		
007-R4	Requirements, R4.3 Recommendation: We suggest similar language be added to each of the requirements ie, if the requirement can't be followed, allow the use of compensating measures.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.
007-R5		
007-R6		
007-R7		
007-R8	Requirements, R8.2 Recommendation: Toward the end of the first sentence, add the words "permanently stored" after the words "... facilities are not...".	This comment must have been miss-sorted by mistake, because it appears the comment pertains to "R8.2" from another section. The words noted cannot be found in R8.2 within CIP-007. Sorry...
007-R9		
007-R10		
007-R11	Requirements, R11 Question: Does this include "protective relay settings" on some critical cyber assets?	This requirement has been deleted.
007-M1		
007-M2		
007-M3		

CIP-007 Responses to Comments

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Commentor Edwin C. Goff III
Entity Progress Energy

Comment		***Response***
General		
007-R1	R1 - Requiring security test procedures on a non-production environment is not practical for many installed systems. This needs to be revised to state, "when possible". Also, if a 3rd party vendor has a similar non-production environment, can the testing be performed by the vendor and a certificate of conformance be acceptable?	The drafting team believes security testing should be implemented and in such a way that does not affect production operations. If a vendor has an environment that closely simulates an entities production environment and is able to conduct the appropriate security tests for your environment, this is acceptable.
007-R2		
007-R3	R3.3 Generic Account Management --unattended. Unattended access should be controlled by fob or other electronic measures in addition to key/card access control.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		

CIP-007 Responses to Comments

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

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

	Comment	*Response*
General	National Grid believes CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1	Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>> to <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>> We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.	The assumption that every entity has a test system is incorrect. The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. This will be clarified in draft three.
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive and should be deleted. The <<monthly review>> in Requirement R4.2 is too prescriptive. We recommend changing R4.2 from <<The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.>> to <<The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.

	installing the patch.>> Add <<where technically feasible>> to the end of Requirement R4.3.	
007-R5	Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means. Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3. The combined requirement should allow technically feasible alternative solutions. Change Requirement R5.2 from << The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> to << Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from << Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware. >> to << Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	1) Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>> 2) Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>> 3) Change Requirement 6.1.4 from <<Security patches and anti-virus version levels>> to <<Assessing security patches and/or anti-virus version levels, as appropriate>> 4) The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an attended facility?	1) Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007. 2) Acknowledged. These matters arte now addressed in R9. 3) Acknowledged. These matters arte now addressed in R9. 4) Acknowledged. The distinction between attended and unattended facilities has been removed.

007-R7	The title of Requirement R7 is too broad. We recommend changing this title from <<Retention of System Logs>> to <<Retention of Appropriate System Logs>> The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8		
007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	This requirement has been deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.
007-M5	Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.>>	The drafting team has updated the measures to follow the restructured requirements.
007-M6		
007-M7		
007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the	The drafting team agrees with the comment and has updated

	perimeter.	the standard.
007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2	Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor Gary Campbell
Entity MAIN

	Comment	*Response*
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. Level of compliance: Specify review times in the requirements and then measure	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		

CIP-007 Responses to Comments

007-C1,3		
007-C1,4		
007-C2,1	Level 1 - How many documents do I absolutely have to find? Do you want me to determine as the auditor the specific items identified. What if i miss an item. I do not think I can clearly find them.	The Compliance section has been updated to address your comments.
007-C2,2	How big is a gap? How I am to measure a gap?	The Compliance section has been updated to address your comments.
007-C2,3	Level 3 - How many of the 11 items mention constitute level 3 , 1 or all?	The Compliance section has been updated to address your comments.
007-C2,4	Level 4 - This is a waste of a level. The way it is worded, if I have one document I can never be found to be level 4. This does not promote compliance. You would expect entities to have some level of completion to their documentation so may be we should looking for at least half of the documentation completed to be level 4.	The Compliance section has been updated to address your comments.

CIP-007 Responses to Comments

Commentor	Greg Mason
Entity	Dynegy Generation

Comment		***Response***
General		
007-R1		
007-R2		
007-R3	Section R3.2 currently only allows the use of group accounts if individual accounts are not technically supported. This section needs to be modified to unconditionally allow the use of group accounts as long as the associated audit trail and account security steps referenced in this section are maintained. These changes will still meet the intent of this section without the imposition of unnecessary costs. The FAQ on this issue also needs to be revised accordingly.	The drafting team will update the standard to clarify and appropriately reflect the intent.
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		

CIP-007 Responses to Comments

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Guy Zito
Entity NPCC CP9

	Comment	*Response*
General	CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1	Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>> to <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>> We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.	The assumption that every entity has a test system is incorrect. The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. This will be clarified in draft three.
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive and should be deleted. The <<monthly review>> in Requirement R4.2 is too prescriptive. We recommend changing R4.2 from <<The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.>> to <<The Responsible Entity shall perform a routine review of the security patches available for each Critical	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.

	Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.>> Add <<where technically feasible>> to the end of Requirement R4.3.	
007-R5	Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means. Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3. The combined requirement should allow technically feasible alternative solutions. Change Requirement R5.2 from <<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades. >> to <<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> NPCC Participating Members do not agree with <<site-specific installation>> in Requirement 5.4. and recommend changing from <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.>> to <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>	References to Integrity Software have been removed.
007-R6	Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>> Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>>Change Requirement 6.1.4 from<<Security patches and anti-virus version levels >>to<<Assessing security patches and/or anti-virus version levels, as appropriate>> The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an attended facility?	1. Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007 2. Acknowledged. These matters arte now addressed in R9. 3. Acknowledged. The distinction between attended and unattended facilities has been removed
007-R7	The title of Requirement R7 is too broad. We recommend changing this title from <<Retention of System Logs>>to<<Retention of Appropriate System Logs>>	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3.
007-R8		
007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.

007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.
007-M5	The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain. Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>	1) Yes, the Responsible Entity identifies the appropriate system logs to retain. Each Responsible Entity's systems environment will be at least a little different, so only the Entities themselves can appropriately determine an adequate strategy. 2) Good and valid suggestions all, and in Draft 3 we think we have words more reflective of what you have suggested. The Requirements section has been significantly altered in Draft 3, with some material moved to other sections. We should be pretty close to the intentions outlined in the comment, but if additional word smithy is felt to be necessary, please offer those suggestions during the Draft 3 comment period.
007-M6		
007-M7		
007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.	The drafting team agrees with the comment and has updated the standard.
007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		

007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2	Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor	Tim Hattaway
Entity	AECoop

Comment		***Response***
General		
007-R1		
007-R2		
007-R3		
007-R4	R4.1. Need to allow for validation by the software developer. In most cases, this software on many of these systems are proprietary and the impact of a patch is unknown to the purchaser. Need to make provisions for verification from the vendor.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11	R11. Could you change the requirement from "annually" to "periodically". I can see where this may create more problems than it solves. Let the Responsible Entity document and justify his reasoning for choosing the period based on support for the system and criticality. The method of verification should also be documented. For example in an operational environment, there may be not system available to do a system restore without putting a critical system at risk. It may be that the media is shipped to the vendor’s site for restoration on a test environment. Results could be documented and filed.	This requirement has been deleted.
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor	Hein Gerber
Entity	British Columbia Transmission Corporation

Comment		***Response***
General	Remove the use of the term "integrity software" as this is not an IT adopted term. Explicitly say what is intended (e.g., virus detection and intrusion detection software.)	The Drafting Team will update the standard to clarify "Integrity Software" requirements. Integrity monitoring tools are intended to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malicious software (mal-ware) on systems within all Electronic Security Perimeters.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		

CIP-007 Responses to Comments

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Jerry Freese
Entity American Electric Power

	Comment	*Response*
General	There is a page number problem in CIP-007-1. Is "Integrity Software" meant to address detective or protective controls?	The Drafting Team will update the standard to clarify "Integrity Software" requirements. Integrity monitoring tools are intended to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malicious software (mal-ware) on systems within all Electronic Security Perimeters.
007-R1	R1 is actually a few separate requirements mixed together. Can it be split up?	The drafting team agrees and will update the standard accordingly.
007-R2		
007-R3		
007-R4		
007-R5	R5 is inconsistent because it uses a title as the requirement - what is the requirement? Other requirements that have this problem in CIP-007-1 should also be addressed.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		

CIP-007 Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor	Jerry Heeren
Entity	MEAG Power

Comment

General

We suggest that the words "security patches" and "cumulative patches" be removed --as most utilities do not have the capability of and cannot test every software patch that a software manufacturer releases --such as Microsoft, HP, etc. In addition, to fully test whether or not a software patch works, a utility's controlled non-production environment would need to be attacked before and after a patch was applied --to prove that the new patch works. This could be an expensive approach since a utility would have to fully duplicate hardware and software for the systems under test. In addition and in certain cases, if a utility were to try to prove that certain software patches were 100% effective, a utility may have to attack its production environment (versus non-production environment) to verify whether or not a patch worked.   Testing in a production environment is very dangerous and can be compared to putting a gun to your head. As a general statement, NERC needs to trust that the general software industry will update its registered users (i.e., utilities) as appropriate on software patches/fixes. In turn, NERC needs to ensure that its utility members will 1) get the software patches that they need and 2) that they will apply the software patches as appropriate and within acceptable timeframes.

Other Comments --Requirements and Measures numbering scheme does not match.

Response

The intent of the Cyber Security Test Requirement to ensure changes made to Critical Cyber Assets do not compromise the current cyber security controls in place. The requirements also state that testing should be performed in a manner that does not affect production operations. The drafting team will update the standard to clarify the requirement.

The drafting team will review and update the Requirements and Measures for alignment.

007-R1

007-R2

007-R3

007-R4

007-R5

007-R6

007-R7

007-R8

007-R9

007-R10

007-R11

007-M1

007-M2

007-M3

007-M4

007-M5

007-M6

CIP-007 Responses to Comments

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Jerry Litteer
Entity INL

	Comment	*Response*
General	A concise definition of terms is needed here when talking about the different kinds of patches and software. Especially the term integrity software, is it software to validate the size and contents of a other files or is it anti-virus software, just what do you mean.	The Drafting Team will update the standard to clarify "Integrity Software" requirements. Integrity monitoring tools are intended to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malicious software (mal-ware) on systems within all Electronic Security Perimeters.
007-R1	R1 Test procedures ‘ensure that significant changes include but are not limited to security patches, cumulative service packs, new releases, upgrades or versions to operating systems, applications, database or other third party software, and firmware.’ It is way too difficult to discuss all these type of patches together since they affect different functions. There is a need to discuss the testing security patches separate from updates to the application, or vendor software. "These tests are required to mitigate risk from known vulnerabilities, affecting operating systems...." I think this has to be reworded. The patches are to mitigate risk from known vulnerabilities, and the tests are to ensure no adverse impact to production operations. "The responsible entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities..." - way too resource intensive. The patch may be fixing a potential vulnerability that is not in the wild yet. Due to the no time available for patching on these systems, the responsible entity should be able to identify another mitigation instead of testing and applying a patch immediately. This will enable the entity to wait and see if the patch actually worked as advertised in other industries prior to testing in the non-production environment and applying to a 24-7 real-time environment. This discussion is confusing and it might be because too many items are being discussed at once. ‘Tested for known security vulnerabilities...’ might be talking about vulnerability scans --software that will run and look for tens of thousands of known vulnerabilities (e.g. Trojans). It’s difficult to imagine running a COTS vulnerability scan on a production SCADA or control system environment --it will kill communications. This type of scan could be run on a non-production environment.	Security patching is a separate requirement. The testing requirement is to test changes to verify they comply with the entities security policies and procedures and do not introduce vulnerabilities. The standard will be updated to clarify intent.
007-R2		
007-R3	R3 Account and Password Management. This is still an issue with legacy applications that were not designed or implemented for multiple accounts and passwords. Other forms to insure authenticity similar to CIP-005-1 B R4.2 might be required. R3.1 specifies the 6 character alpha, numeric and special character but only mentions changed periodically. Cyber hackers like to see the specifics to focus their cracker programs. The most important password characteristic is frequency of change, which is not specified. R3.4. Invalid accounts, regardless of their origin (vendor-guest, expired, etc.) must be disabled immediately and all account actions (enabled or disabled) reviewed weekly. This will insure that non-authorized accounts are swiftly dealt with.	The drafting team will update the standard to reflect when technically feasible. The entity is required to have a procedure in place for managing access to these accounts. The requirement states the entity should change passwords, but leaves the frequency to the entity to determine based on their environment. The standard will be updated to reference access requirements in CIP-003.

	R3.6 This requirement is redundant. This should be completely spelled out in the security policy required in CIP-003-1.	
007-R4	R4 Security Patch Management --Need definition of security patch management vs. integrity software. R4.1 risk based assessment, so as to avoid un-necessary and excessive patching. This sounds good but the opposite is also valid. Patching a software application that is not applied to the control system but is used inside the security perimeter (e.g. router software) should be tested and done immediately to reduce the exposure if someone penetrated the perimeter. This type of patch should have limited impact on operations. R4.2 Monthly review of patches up to date is not enough if this is truly a security patch with the need to update signatures.	Draft 3 addresses the differences between security patch management in R4 and R5 where integrity software has been changed to "Anti-virus Software". The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.
007-R5	R5 Integrity software: Most integrity software available is based on the ability to update signatures to the integrity software. These signatures are considered security patches and will not be implemented in a timely fashion if they have to go through the known vulnerability testing as specified in R1. R5.2 Monthly review of integrity software is not sufficient. Signature based security patches normally are applied a lot more frequently to keep up to date with published exploits. R5.3 where integrity software is not used, compensating measure --this would be a good place for a discussion on reviewing for unauthorized accounts, reviewing file systems for unrecognized or unexpected files. R5.4 Unattended facilities shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of mal-ware. This also needs to include the scanning of the media used for updating systems at these facilities.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	R6 annually vulnerability assessment that includes scanning for open ports services (CIP005 R2 no time specified) and modems (CIP005-M3.1 annual), factory default accounts, security patch (CIP007 R4.2 monthly) and anti-virus version levels (CIP007 R5.2 monthly). This requirement contradicts with other requirements. Is this in addition to the other requirements?	We cannot tell just which requirement 'this' refers to in the last sentence. However, we do acknowledge inconsistencies in requirement frequencies along the lines noted in the comment, and we believe we have rectified the inconsistencies in draft 3.
007-R7	R7.1 90 day retention of logs will not be long enough for the forensic activity for stealth attacks. Only keep for 3 years if the attack is identified.	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8		
007-R9	R9 change title to Enabling only used host ports and services.	The title has been changed.
007-R10	R10 Issuing of alarms has no specified time. This in conjunction with no frequency for log reviews is worthless. Monitoring the performance and usage is great if you have a trained operator or good system administrator who knows what normally activity based on the outside factors should reflect	This requirement has been deleted.
007-R11	R11 Not only does the media that stores the data have to be tested annually the procedures to restore a	This requirement has been deleted.

	system should be tested or exercised annually. This should be combined with CIP-009-1 R1	
007-M1		
007-M2	M2 24 hour for termination might be too long.	The standard will be updated such that the measures align with the requirements.
007-M3	M3 date of testing might not be needed if security patches for applications that reside on the same machine but do not affect the production operations can be installed without testing.	The standard requires changes to Critical Cyber Assets adhere to Security Test Procedures. Installing a patch is a change to the asset even if it does not directly affect the production application.
007-M4		
007-M5		
007-M6		
007-M7		
007-M8	M8 change disabling unused host ports/services in title and text to enable only those explicitly required.	The drafting team agrees with the comment and has updated the standard.
007-M9		
007-M10	M10.2 Should read ‘include tested recovery procedures...’	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Responses to Comments

Commentor Jim Hansen
Entity Seattle City Light

	Comment	***Response***
General		
007-R1	R1. In the second paragraph, please clarify that a non-production environment can be a production system that has been removed from production mode. This covers the case where non-production testing is not possible, on obsolete equipment for example, while achieving the goal of this section that is to ensure that testing is done safely. 2. R1 requires that we add another layer of tests to our existing test procedures, testing that a vendor's security patches for known security vulnerabilities work correctly. This causes us several problems. First, we have Solaris Unix systems from Sun. Sun tests their patches prior to releasing them (just as Microsoft is starting to do). We install necessary patches and then verify that the patches were installed correctly. We believe that the vendor should be held accountable for ensuring their security patches actually remove the vulnerability. If damages resulted from the patch not correcting the vulnerability, then the vendor would be held liable. Second, the cost of testing, in both human and financial resources is high. The new CIP standards are already creating a significant increase in resource utilization. We believe it would increase security for us to concentrate our resources on more critical security issues. Third, we do not believe that requiring the industry to test the security patches from vendors is effective in increasing security. Pressure is already placed on the vendors when the computer user industry finds that a security patch does not correct the problem. The operating system vendors have significantly increased their quality assurance testing as a result. If this requirement is not removed from the standard, we will be forced to vote 'no' on CIP-007.	The drafting team will take your comment into consideration and update the standard accordingly.
007-R2		
007-R3	R2 should be reworded. We suggest 'The Responsible Entity shall store test documentation, security procedures, and acceptance procedures for Critical Cyber Assets located at unattended facilities at a facility that is staffed 7x24. These documents must not be stored in a facility that is unattended at any time.' The second sentence should be removed since it would be possible to conduct security test procedures at the unattended facility simply by going there and conducing tests on a non-production environment located at that facility. The location of the non-production test environment is not something that should be specified. 4. R3. Entities should be required to 'perform account management to provide for access authentication...' or 'follow an account management program' rather than 'establish an account password management program'. Our program already exists and generic programs that meet these requirements are specified in standard security documents. 5. R3.1 change 'shall use accounts that have a strong password' to 'shall require and utilize strong passwords'.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
007-R4	R4.2 requires a monthly review of available security patches. Our vendor provides us with critical security alerts tat we respond to immediately. Our normal cycle for non-critical security patches is to review and download them every 6 months because it takes at least a month to adequately test our EMS applications. Given the other measures employed on our electronic security perimeter in conjunction with the security alert program, we believe that a monthly review requirement is much too frequent. We request that this sentence be struck.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.

007-R5	In R5, we take ‘Integrity Software’ to mean that set of software commonly called ‘anti-virus software’. Is that the intent or is something else meant? In either case, can you clarify with specific examples or more common terminology?	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	R6.3 Doesn’t this apply to all facilities?	To all critical assets (facilities), yes.
007-R7		
007-R8		
007-R9		
007-R10		
007-R11	R11. As stated in comment 3 above, the location of the non-production test environment is not something that should be specified in any of the CIP standards. Please remove the last sentence so that we can test at an unattended facility if we happen to have a test environment there.	This requirement has been deleted.
007-M1		
007-M2	M2 typo ‘n’.	Noted.
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
	R5.1 We believe the drafting team intended for this integrity software to be run on all Critical Cyber Assets within the Electronic Security Perimeter. However R5.1 does not clearly state this requirement.	
007-M9		
007-M10	M10 in general should consider the use of other backup media. Specifically, ‘backup data and tapes’, and ‘backup data’, should be replaced with ‘backup media’.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		

007-C2,3

007-C2,4

Commentor	John Lim
Entity	Con Edison

Comment		***Response***
General		
007-R1	R1/M1: tests performed by vendors to verify the effectiveness of the patch should be deemed acceptable; for example, a patch tested and released by an EMS vendor would not have to be tested again; a security patch tested and released by Microsoft would not have to be tested again for its effectiveness at remediating the vulnerability. It is unreasonable to expect the Responsible Entity to verify that a vendor supplied patch to fix a specific vulnerability is indeed effective by developing, in cases where exploit code is not available, and running exploit code to verify the effectiveness of the patch. The Responsible Entity should only be required to perform functional quality assurance prior to applying the patch in production. The Responsible Entity should only be expected to verify that the patch has been correctly installed. The requirement for vulnerability assessment addresses the testing of vulnerabilities on a regular basis.	The drafting team will take your comment into consideration and update the standard accordingly.
007-R2		
007-R3		
007-R4		
007-R5	R5.1 This could be made clearer. Why state Wide area network and then include any networked device it may connect to. A statement like "Any Critical Cyber Asset connected to a network or device connected to a network" would mean the same and has less ambiguity.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	R.6.3: doesn't the "limited vulnerability assessment" here imply that the unattended Critical Cyber Assets are less critical than the attended one?	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity.
007-R7		
007-R8	R8 and R9 are covered in CIP-003.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R9	R8 and R9 are covered in CIP-003.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		

007-M6		
007-M7		
007-M8		
007-M9		
007-M10	M10 Back-up and Recovery - The Requirement, Measure and Compliance sections do not match. The Requirement states "information stored on computer media for a prolonged period of time must be tested annually." The Measure and Compliance sections state that you must do an annual restoration exercise. We have several instances in our backup procedures were nothing is stored on computer media longer than 30 days. I do not interpret this as a prolonged period of time. The Measure and Compliance sections mention documentation not mentioned in the requirement section.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Responses to Comments

Commentor Karl Tammer
Entity ISO/RTO Council

	Comment	*Response*
General	This standard is a prime example of the need for a technical writer's review of the standards. It is much more prescriptive than the rest and demonstrates the lack of homogeneity across the standards Please align measurements and to requirements.	The Drafting Team will review CIP-007 and update the standard to better align the requirements and measures. A technical writer will review Draft 3 of the standards.
007-R1	R1 -- Delete. This requirement is well covered in CIP 003, R4 and R5	CIP 003 R4 and R5 address overall change control processes. The testing requirement in 007 is to address security testing specifically.
007-R2	R2 -- Delete. This requirement is well covered in CIP 003, R4 and R5	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3	R3 -- use "account management" instead of "establish an account password management program" R3 -- "by compromised account passwords" should be struck as unnecessary. R3 -- "that include but are not limited to:" should say "that must meet at a minimum:" R3.3 is covered in CIP 006 R3.4 and R3.5 is covered by CIP 003, 005 and 006.	The drafting team will take your comments into consideration for the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	R 4 -- "critical cyber security assets." Security should be deleted. R4.1 -- Should read "all relevant patches" R4.2 & R4.3 -- this requirement is too prescriptive. A better requirement would be for the company to have a patch management policy and procedure based on its own environment.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.
007-R5	R5.1 -- This section is unclear and would be better if written as follows: "The Responsible Entity shall use means to monitor and protect the integrity of data including software associated with critical cyber assets e.g.: technology, processes/procedures, software." to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter. R5.2 - Suggest it be deleted. Covered elsewhere. R5.4 -- Where remote installation of software updates is required, the responsible entity shall ensure the integrity of the software being installed prior to initiating remote installation in order to prevent annual dissemination of malware.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6		

CIP-007 Responses to Comments

007-R7	R7 -- The last sentence gives the entities the responsibility to determine their own logging strategy but R7.1 and R7.2 are contrary and prescriptive and should be deleted	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8	R8 -- Should be deleted as it is well covered in CIP 003.	Agreed. Change control and configuration management requirements have been moved to CIP-003, leaving a specific subset requirement concerning security patch management within CIP-007.
007-R9	R9 -- Should be deleted as it is well covered in CIP 005.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10		
007-R11	R11 -- The last sentence "For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site." should be removed and the rest of this section moved to CIP 009.	This requirement has been deleted.
007-M1		
007-M2	M2. -- Remove "record of semi-annual audit of this policy" as is contrary to R3.1	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3	M3 - The reference to change control is dealt with in CIP 003	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10	M10.1. Replace backup data and tapes with backup media.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		

CIP-007 Responses to Comments

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor	Keith Fowler
Entity	LG&E Energy Corp.

Comment		***Response***
General	We are in agreement with the comments submitted by the ECAR CIPP group.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		

CIP-007 Responses to Comments

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Kenneth A. Goldsmith
Entity Alliant Energy

Comment		***Response***
General	See CIP003 and CIP005 for redundancy	The Drafting Team will review the standard and remove duplications where possible or provide clarification.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		

CIP-007 Responses to Comments

007-C2,1		
007-C2,2		
007-C2,3	Level 3 compliance - much too severe. Suggest: Remove 2.3.1 - same as 2.2 Move 2.3.2, 2.3.6.1, 2.3.7, 2.3.8, 2.3.11 to Level 2	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

Commentor Kurt Muehlbauer
Entity Exelon Corporation

Comment		*Response*
General	Several requirements in this standard reference unattended facilities. These requirements specify special provisions that need to be taken at unattended facilities (e.g. change management and virus checking). Cyber Assets in unattended facilities that are connected to a WAN do not require special provisions. We recommend clarifying through a FAQ the definition of an unattended facility.	The reference to attended and un-attended will be removed from CIP-007 in Draft 3. The reference was intended for field devices and will be clarified as such in Draft 3.
	We recommend that an FAQ be created to define integrity software.	The Drafting Team will update the standard to clarify the "Integrity Software" term.
	D1.2 requires that data shall be kept for three years. R7.1 requires that logs should be kept for 90 days. We request that these data retention periods be clarified.	Data retentions period will be review and updated for consistency and clarity.
	FAQ #13 references question one above. Should the reference really be to FAQ #12?	The Drafting Team agrees with your comment and will update the FAQ in a future draft.
007-R1	In R1 the scope of any security testing should be for compliance to company cyber security standards, such as password standards. Requiring responsible entities to perform specialized testing of all vendor software used in an organization as implied during the Webcast is not feasible. Responsible entities cannot be specialists in vendor software testing since the details of most vulnerabilities are not released to the public. Responsible entities must be able to accept the security certifications provided by the vendor.	The testing requirement is to test changes to verify they comply with the entities security policies and procedures and do not introduce vulnerabilities. A testing certificate from the vendor will suffice if the vendor can simulate the entities and environment for testing. The standard will be updated accordingly.
007-R2		
007-R3	R3.3 describes physical access to unattended facilities. Physical access controls are defined in CIP-006. We recommend that R3.3 be deleted.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
	R3.4 requires semi-annual reviews of access rights. M18 of CIP-003 requires annual reviews of access rights. We recommend that R3.4 from this standard be consolidated with R5.2 of CIP-003.	This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4		
007-R5		
007-R6	R6 requires annual vulnerability assessments. Vulnerability scanning is a mitigating control to ensure that other controls such as change management, security testing, and patch management are effective. We recommend that vulnerability scans be performed once every three years.	Port scanning won’t discover or neutralize malware, but it will tell if ports are unexpectedly available. It is not the intent of the drafting team to require active port scanning of production systems, for the several reasons identified in comments. Accordingly, the term “scanning” has been deleted in draft 3 in favor of the use of the term “assessment.” The preferred approach is to maintain an identical system used for back-up and/or

		testing which is also exposed to the same potential sources of attack as the active system. But this isn’t remotely affordable for many organizations and overkill for others, so this cannot be a requirement. For this reason there needs to be some middle ground, and use of scanning tools conceived specifically for a controls environment is a potential approach. Determining the prudence in use of such a tool to test a critical cyber asset in active operation is the aegis of the Responsible Entity, but any such use must be very carefully considered. Alternatively, an extensive review and documentation “assessment” of hardware and software configurations may indeed be the most prudent approach in instances where a production image back-up or test instance is not available. The drafting team does not feel that an annual assessment is onerous.
007-R7		
007-R8		
007-R9	R9 is almost identical to R2 of CIP-005. We recommend that this requirement only be specified in one standard.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10		
007-R11		
007-M1		
007-M2	M2 requires auditing of passwords against the responsible entities policy. It is not clear if the intent is to ensure that the system is configured to enforce password standards such as length and complexity or if the intent is to check for weak passwords using password-cracking tools. We recommend that this measurement be clarified. We recommend that the last sentence in M2 be changed from: ... have a change n status ... to: ...have a change in status ... M2 requires review of access permissions within 24 hours for any personnel terminated for cause. This is redundant with M4.3 of CIP-004. We recommend that this measurement only be specified in one standard.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8	M8 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.	The drafting team notes your comment.

CIP-007 Responses to Comments

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Commentor Larry Conrad
Entity ECAR Critical Infrastructure Protection Panel

	Comment	*Response*
General		
007-R1	B.R1--Recommend changing the reference from test environment to test plan. Also include the requirement that if a test environment is not available, a documented backup plan is required. Change to: The Responsible Entity shall document full detail of the test plan. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities on a controlled non-production system prior to being rolled into production. If a separate test environment is not available, a documented backup plan is required.	The drafting team believes the test environment should be documented to verify it is representative of the production environment.
007-R2	B.R2.-- Recommendation: Procedures need to be available at backup centers. Change to: If test documentation, security procedures, and acceptance procedures are needed and stored at unattended facilities such as backup sites, the materials must be kept in a secure/locked location.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3	B.R3.1--Recommendation: Increase minimum password length from six to eight characters unless it is not supported. Change to: To the extent allowed by the existing technology, a password must consist of a combination of alpha, numeric, and special characters with a minimum of eight characters	The drafting team believes a minimum of 6 is adequate since many legacy systems do not support more. The entity is free to go beyond the minimum requirements.
007-R4		
007-R5	B.R5.1-- Recommend: The requirements in this section should be qualified with the term "as applicable" due to diversity in software and operating systems utilized throughout the industry. Change to: The Responsible Entity shall use integrity software as applicable on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure, and distribution of malicious software (mal-ware) to other Cyber Assets within the Electronic Security Perimeter.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6		
007-R7		
007-R8	B. R8.2--Recommend: Clarification Change to: The Responsible Entity shall insure that controlled environments, which are used to develop or test Cyber Assets that are normally placed at unattended facilities, are not kept at the unattended facility." Recommend: Correct the numbering in this section from page 1 of 1 through page 10 of 10 to correct	Distinction between attended and unattended facilities has been removed.

	numbering.
007-R9	
007-R10	
007-R11	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

Commentor	Larry Conrad
Entity	Cinergy

	Comment	***Response***
General	General Comment about this section. Many of the requirements are not available through existing legacy EMS systems. Cinergy is working with a vendor on a new EMS system, which should be operational in mid 2007 to late 2007. Some clause should be inserted into the documentation to allow time for delivery of a new system, if it is on order, which can supply the required controls. For example, other sections state the requirement applies "if it is technically feasible." We suggest adding this type of language to requirements in this section. General Comment about this section: Need additional clarification regarding the definition of attended vs. un-attended facilities. Is a facility, which is manned 8 hours a day and un-manned 16 hours a day, attended or un-attended?	The Drafting Team will review CIP-007 and provide a technically feasible clause where appropriate. The reference to attended and un-attended will be removed from CIP-007 in Draft 3. The reference was intended for field devices and will be clarified as such in Draft 3.
007-R1	R1. --Documentation requirements in this section are excessive. Draft I documentation requirements were excessive, and, except for formatting, little changed from Draft I to Draft II of this section. For example, "...The Responsible Entity shall document full detail of the test environment..." is not necessary and should be eliminated.	The drafting team believes the test environment should be documented to verify it is representative of the production environment.
007-R2	R. 2--Requirement states: "...shall not store ...security procedures...at an unattended facility..." Recommend that this sentence be deleted. Security procedures and other documentation need to be available at backup sites, which may be generally un-attended.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3	R.3.1--Strong Passwords: The last sentence "Passwords shall be changed periodically per a risk based frequency to reduce the risk of password cracking..." is not practical regarding relays, particularly when networked communication is not used. Recommend that the drafting team modify the language so that relays are excluded from the requirement. R.3.3--The requirement that physical access is authorized by a control or security center operator on an instance by instance basis is harsher than CIP-006-1 and the language here contradicts language in CIP-006-1. In section CIP-006-1 physical access controls, monitoring, and logging are all described in detail and there is no indication in that section that physical access must be authorized by a control or security center operator on an instance by instance basis. Please delete "instance by instance" and "control or security center operator" references in CIP-007-1. R.3.4--Access Reviews: Need standardization on the review periodicity throughout the document. This is one of the only sections that has a semi-annual requirement. Can't reviews be standardized generally on an annual basis?	The drafting team will update the standard to reflect when technically feasible. The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The drafting team will review and update the standards for consistency.
007-R4	R.4.2. & R.5.2.--Review of Patches and Integrity Software: These sections specify a monthly review requirement. A monthly review is over-kill. Recommend that the period for review should be quarterly in these cases. Need standardization and consistency on the review periodicity throughout the document.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.
007-R5	R.4.2. & R.5.2.--Review of Patches and Integrity Software: These sections specify a monthly review	The drafting team has removed references to Integrity

	requirement. A monthly review is over-kill. Recommend that the period for review should be quarterly in these cases. Need standardization and consistency on the review periodicity throughout the document.	Software and has restructured the section.
007-R6		
007-R7		
007-R8		
007-R9		
007-R10	R.10.--Operating Status Monitoring tools: This is another example of documentation that is not necessary. No specific operating status targets are listed. Therefore, this section simply generates documentation without relevance.	This requirement has been deleted.
007-R11	R11--Testing the stored information at least annually will result in a lot of work with very little benefit. Recommend that this requirement be eliminated.	This requirement has been deleted.
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Responses to Comments

Commentor Lawrence R Larson, PE
Entity Midwest Reliability Organization

	Comment	*Response*
General	CIP-003 and CIP-007 should be combined (ie R3.4 3.5 Access reviews also included in 003; R8 Change control also located in 003; R9 Disabling unused host ports also included in 005). Levels of non-compliance - there is a lot under Level 3 - some of these should be moved to Level 2.	The Drafting Team will review the standard and remove duplications where possible or provide clarification. CIP-007 access reviews refer to the technical permission settings on a Critical Cyber Asset. CIP-003 refers to general access controls. CIP-007 will be updated to reference CIP-003 for determining access right for setting permissions. Change control will be removed from CIP-007. Disabling unused ports and services in CIP-005 is for devices on the Electronic Security Perimeter, CIP-007 is for devices inside the perimeter. The standard will be updated to clarify the requirement. The Levels of Compliance will be reviewed and updated.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5	R5 should be deleted. No definition is provided for exactly what is meant by INTEGRITY SOFTWARE, which is a problem. This section should be replaced by a general requirement to address the appropriate use of such software in a security plan. However, requiring the use of such software categorically is not justified; its deployment should be weighed and pursued as appropriate by each entity.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	R6.3 is vague; it should be eliminated.	Agreed
007-R7		
007-R8		
007-R9	R9 is redundant with CIP-005; it should be eliminated from CIP-007	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		

CIP-007 Responses to Comments

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Commentor Linda Campbell
Entity FRCC

	Comment	*Response*
General	R1, R6 During the conference call on 2/2 there seemed to be considerable confusion surrounding the testing of security patches and scanning for vulnerabilities. There was even discussion of trying exploits against production systems after patching. It should be emphasized that great caution should be taken when scanning or testing patches in an EMS or DCS environment. In fact, scanning for open ports and exploits in these environments could result in unintended system outages, and could be considered negligent. Only non-intrusive means to determine open ports, and to verify the installation of patches, should be used in this type of environment, and the drafting team should modify sections R1 and R6 to ensure that they are not suggesting the use of obtrusive tools for testing patches or identifying open ports in a production environment.	The Drafting Team will update the standard to clarify the testing requirements.
007-R1	R1 The use of a separate non-production environment for testing and acceptance of security changes results in the need to re-licensing EMS, DCS and other software to establish such an environment. Test environments may not be feasible for many older EMS or DCS systems running proprietary hardware and software. The drafting team needs to consider a phased in approach for this requirement due to the cost to the industry, and time required to implement such environments. The industry should be asked for feedback on this requirement, as a large percentage of the participants do not have such test environments readily available. Those that do, probably also use those environments for testing upgrades and application changes as well, meaning those environments do not always mirror their production counterparts.	The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. The drafting team will take your comment into consideration for draft 3.
007-R2	R2. The intent of this statement is not clear. Please provide clarification beginning at: The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3	R3.3 This requirement is confusing. What does physical access to an unattended facility have to do with generic account management? For unattended facilities (i.e. substations, backup facilities, unattended control buildings or rooms within a generating station) it is not practical to have approvals of physical access on an instance-by-instance basis. If a trusted employee who has been background screened, has a cardkey, token or other pre-approved access method for physical access to an unattended facility, and the other requirements as dictated by CIP-006 are in place, there is no need to have a separate function approve access each time that employee needs to enter such a facility. Regardless, any requirement of this type belongs in CIP-006. R3.5 This requirement belongs in standard CIP-006.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
007-R4		
007-R5		
007-R6	R6.3 The intent of this requirement escapes us. Why is this requirement specific to unattended facilities?	The distinction between attended and unattended facilities has been removed.

007-R7	R7.2 Again the intent of this requirement for unattended facilities escapes us. A facility that is unattended (substation) should have the same logging requirements as those that are attended (control centers) if the assets housed there are critical.	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8	R8 Does the change control process described in this environment relate to all changes or just those of a security software or patch nature?	Good question... Change control and configuration management requirements have been moved to CIP-003, leaving a specific subset requirement concerning security patch management within CIP-007. Having said that, the change control and configuration management requirements in CIP-003 do indeed apply for any and all cyber assets that are deemed to be critical. So, yes, these requirements also apply for changes to, say, firmware in a relay that's deemed to be critical, whether it's flash upgraded/patched, or the chip itself is replaced.
007-R9		
007-R10		
007-R11	R11 For clarity purposes, this requirement is more appropriate to be contained in CIP-009 Recovery Plans. The level of detail discussed in this section is not currently covered in CIP-009, and having recovery requirements in two separate standards only leads to confusion and creates the possibility of conflicting requirements in future standards versions. Any recovery plan should specify the data, retention period, etc to be backed up for recovery purposes. Including in this section only increases administration on the part of the individual entities for developing procedures, and monitoring compliance.	This requirement has been deleted.
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-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 standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.

	The performance-reset period shall be one (1) calendar year.	
007-C1,3	Compliance section 1.3. should be as follows: 1.3. Data Retention 1.3.1. The compliance monitor shall keep audit records for three (3) calendar years. 1.3.2. The Responsible Entity shall keep data for three (3) calendar years.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Responses to Comments

Commentor Lyman Shaffer
Entity Pacific Gas and Electric Company

Comment		***Response***
General	Introduction/Purpose: The sentence that reads, "A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity" should read "A System Security Management Program is necessary to ensure system availability and integrity by minimizing or preventing malicious and non-malicious activity and misuse, whether authorized or unauthorized. This includes measures necessary to detect, document, and counter such threats."	The Drafting Team will update this section for clarity.
007-R1	R1 -- In some cases production systems are taken off-line and removed from production mode and used for testing. We feel that this needs to be permitted and clarified within this requirement.	The Drafting Team agrees and will clarify the standard.
007-R2	R2 -- The second sentence in this requirement is not clear. It needs to either be clearly reworded or removed.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3	R3 -- Instead of requiring the entity to "...establish an account password management program" it should require the entity to "perform account management". - End the first sentence at "unauthorized system access." striking "by compromised account passwords. - Replace "not limited to" with "must meet" or "at a minimum" R3.1 -- Replace "shall use accounts that have a strong password" with "shall use strong passwords".	The drafting team will take your comments into consideration for the next draft.
007-R4	R4.2 -- Remove the first sentence in this requirement.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.
007-R5	R5.1 -- In this requirement it isn't clear where it must be applied. If it is intended for all CCAs, regardless if at the perimeter or internal to the perimeter, it should clearly state that.	The requirement has been update to make this clearer.
007-R6	R6.1.2 This section requires scanning for open ports/services, and modems. Vulnerability scanning on critical production process control systems is not recommended as it can crash systems We recommend that such scanning be done for off line duplicate systems. R6.1.4 -- a company may elect not to install a patch or antivirus system due to concerns about potential impact on operating systems. R6.3 -- "Unattended" doesn't apply, you should comply with this requirement regardless if the facility is	We concur, and changes have been made.

	attended or unattended.	
007-R7		
007-R8		
007-R9		
007-R10	R10 this is not possible on all critical cyber assets. While we can monitor performance and security events on servers and workstations, some devices may not have the ability to install software or otherwise monitor performance or security events.	This requirement has been deleted.
007-R11	R11 -- The last sentence in this requirement doesn't make sense. Why can you not effectively test on-site at unattended facilities? Recommended removing this sentence.	This requirement has been deleted.
007-M1		
007-M2	M2 -- Fix typo. "n" should read "in". A semi annual audit of all this policy against all accounts is password is too proscriptive and onerous (especially if large # of substation devices are included). Suggest striking this measure.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10	M10.1 -- Replace "backup data and tapes" with "backup media".	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Responses to Comments

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

	Comment	*Response*
General	There is much duplication between CIP-007 and CIP-003, CIP-005, and CIP-006. Either move the remaining elements from CIP-007 out and delete it or clearly delineate what belongs in it and remove the duplication. Due to the way that compliance results on these standards are reported to NERC, it is important that any one non-compliance issue not cause non-compliances across multiple standards. Entities, regions, and even the entire industry are deemed 'XX% compliant', so to keep those numbers reflecting reality it is imperative that single issues only be measured once to avoid double penalties. Levels of Compliance, Level 1 and Level 2 - It is stated that -two (and three, respectively) of the specific areas- in documents have not been reviewed or updated. Is this two (or three) things in any one document or in aggregate across all documents in this standard?	The Drafting Team will review the standard and remove duplications where possible or provide clarification. The Levels of Compliance will be updated for clarity.
007-R1	R1 --Combine all Testing requirements from this and R4 of CIP-003 under one standard. Regarding -significant changes- and security testing: most companies have traditionally relied on vendors to perform security testing as appropriate. We believe that to self-test and certify all -significant- changes against all known security vulnerabilities for all our systems would be a monumental task. We are trained and staffed for functional and operational testing. In R1 -- This requirement states that -The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities prior to being rolled into production-. How is this expected to happen for some vulnerability? For example, how would one verify for a known vulnerability to Internet Explorer or to the XP operating system that the fixes provided by Microsoft had indeed been successfully tested by them. As worded the only way the Responsible Entity would be able to verify success would be to try and develop a program to attack the vulnerability. In other words, as worded the responsible entity is required to verify security patches provided by a vendor do indeed fix the vulnerability. This is not practical.	Security testing is to verify that changes to systems comply with the entities cyber policies. The vendor can not necessarily test for these. If the vendor can document their tests follow your Security Test Procedures and test for your environment then this is acceptable. The standard will be updated to clarify the intent.
007-R2		
007-R3	In R3 -- The words -end user account- are used in the last sentence but are qualified by the parenthetical statement that implies accounts other than end user (i.e. administrator accounts are not typically referred to as -end user-). Suggest just removing the words -end user-.	The drafting team will take your comments into consideration for the next draft and update for clarification.
	R3.3-- Covered in CIP-006 under physical security and should not be under generic account mgt R3.5-- The electronic and physical monitoring aspects of CIP-005 and CIP-006 should cover this.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft
007-R4	R4 - Pg 5, Regarding security patch management and performing a monthly review of security patches for each asset: What will companies do if/when a vendor announces that an older version (application, OS, etc.) is no longer supported and should no longer be used? Could companies be forced into multiple expensive upgrades?	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to

	R4 and M3 mention testing as it relates to security patches. During the NERC webcast, this testing was interpreted to mean that entities must test to insure the patch actually fixes the vulnerability. That is impractical and entities should not be in the business of developing exploit code to test vulnerabilities, nor should they be deemed non-compliant if their scanning engines do not have a signature for said vulnerability (some vulnerabilities cannot be detected via a network scan anyway). The term -testing- can also be interpreted as testing to insure that security patches do not compromise the availability of any critical cyber assets and the testing documentation would show that security patches are not blindly applied to critical cyber assets without first knowing their impact to the environment. This interpretation of -testing- seems more in line with the spirit of CIP-007 and is more reasonable.	document the entities appropriate response to the security patch and vulnerability has been added to draft 3. .
007-R5	R5.1-- Delete the confusing phrase -that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer)-. Simplify this to the blanket statement -shall use integrity software on all Critical Cyber Assets to prevent, limit, ...- and let R5.3 handle the exceptions where it can't be used. The term -Integrity Software- needs to be defined in the Definitions of this Standard. R5.2 --Since the #1 integrity software tool is antivirus packages, it is unclear why this is requiring a "monthly review of the available integrity software" R5.4 Unclear what this means	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6		
007-R7		
007-R8	R8 --Change Management requirements and measures should be combined and either placed in CIP-003 or in CIP-007 but not spread across both.	Agreed. Change control and configuration management requirements have been moved to CIP-003, leaving a specific subset requirement concerning security patch management within CIP-007.
007-R9	R9-- Disabling Unused Ports requirements and measures should be combined and either placed in CIP-005 or in CIP-007 but not spread across both.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10	R10 -- The implications of the words -to monitor operating state, utilization and performance, and cyber security events- is going beyond the scope of a Cyber Security Standard particularly the -operating state, utilization and performance- requirements. If the intent is to monitor these parameters for possible intrusion and security compromise through abnormal -fingerprints- in these parameters that makes sense and it should be stated that is the intent. To imply the requirement for general monitoring of these parameters for other reasons such as operational efficiency of the users due to overloaded processors, database capacity, excessive I/O due to defective coding, etc., although good practices for other reason, is beyond the scope of this standard. Perhaps the words at the end could be modified to and issue alarms for specified indications of possible intrusion and or security compromise, as implemented- could be use to be more specific and appropriate.	This requirement has been deleted.
007-R11		
007-M1		

007-M2	M2 --The sentence beginning "Review access permissions within 24 hours for personnel terminated for cause..." should be deleted as this is covered in CIP-004.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4		
007-M5		
007-M6		
007-M7	M7.1 --Change Mgt controls and Testing Procedures should be measured in CIP-003 or here but not both. M7.2 --Change Mgt controls and Testing Procedures should be measured in CIP-003 or here but not both.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M8	M8 Disabling Unused Ports should be measured in CIP-005 or here, but not both.	The measure has been revised to clarify that CIP-005 covers equipment on the electronic perimeter and CIP-007 covers equipment inside the perimeter.
007-M9		
007-M10	M 10.2 -- There is no requirement to document recovery procedures for reconstruction and Critical Cyber Asset from the backup data. R11 only requires storing and testing not the documentation. Although a good practice, if its expected to be documented (i.e., staff may know how to do it without documentation) then should that not be also stated in the R11 requirements. M 10.3 - How would the documentation required verify one is -capable of recovering- from a Critical Cyber Asset failure? Is this implying that tests performed verified this capability then state that the test results should be documented? Be explicit.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3	In Levels of Compliance, Level 3 - Remove 2.3.9 and 2.3.10 because they are -N/A- and serve no purpose. Non-Compliance levels 2.3.8, 2.3.9, and 2.3.10 should follow their appropriate requirements and measures if they move to other standards.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor Patrick Miller
Entity PacifiCorp

	Comment	*Response*
General		
007-R1		
007-R2		
007-R3	For section B, R3.1, there is the requirement for a 6 character password. Most Best Practice recommendations stand at a minimum of 7 characters, and often 8 characters. For section B, R3.1, there is the requirement that passwords be changed frequently, but there is no recommended/required expiration period. The standard best practice for this is 90 days maximum (quarterly).	The drafting team believes a minimum of 6 is adequate since many legacy systems do not support more. The entity is free to go beyond the minimum requirements. The requirement states the entity should change passwords, but leaves the frequency to the entity to determine based on their environment.
007-R4		
007-R5	For section B, R5, the use of the term "Integrity Software" is confusing, with respect to the standard information security lexicon. This term is usually reserved for applications such as Tripwire or Intact which use forms of hashing algorithms or similar mechanisms to validate the integrity of a system. The term "AntiVirus Software" is widely accepted and is more appropriate. It is reasonably clear from the context that AntiVirus software is being referenced, and not Integrity Software. If Integrity Software is also required, please specify where they (Integrity Software and AntiVirus Software) are both applicable. Essentially, the use of Integrity Software in this context is a misnomer.	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	For section B, R6.1.2, "Scanning" is a powerful term, and may imply that just any utility will work for this need. It should be noted that not all critical cyber assets behave the same when scanned by traditional IT vulnerability scanning tools. Programs such as NMAP can cause serious issues for example.	--Excellent observation and point. It was never the intent of the drafting team to require knee-jerk consistency in application of assessment tools, and in draft 3the term "scanning" has been deleted in favor of simply "assessment." We assume organizations will maintain technical expertise guiding the prudent use of such tools.
007-R7		
007-R8		
007-R9	For section B, R9, though this requirement is worded better, it appears to be redundant with CIP-005-01, section C, M2.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.

CIP-007 Responses to Comments

007-R10

007-R11

007-M1

007-M2

007-M3

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Paul McClay
Entity Tampa Electric

Comment		*Response*
General	R1, R6 During the conference call on 2/2 there seemed to be considerable confusion surrounding the testing of security patches and scanning for vulnerabilities. There was even discussion of trying exploits against production systems after patching. It should be emphasized that great caution should be taken when scanning or testing patches in an EMS or DCS environment. In fact, scanning for open ports and exploits in these environments could result in unintended system outages, and could be considered negligent. Only non-intrusive means to determine open ports, and to verify the installation of patches, should be used in this type of environment, and it the drafting team should modify sections R1 and R6 to ensure that they are not suggesting the use of obtrusive tools for testing patches or identifying open ports in a production environment.	The Drafting Team will update the standard to clarify the testing requirements.
007-R1	R1 The use of a separate non-production environment for testing and acceptance of security changes results in the need to re-licensing EMS, DCS and other software to establish such an environment. Test environments may not be feasible for many older EMS or DCS systems running proprietary hardware and software. The drafting team needs to consider a phased in approach for this requirement due to the cost to the industry, and time required to implement such environments. The industry should be asked for feedback on this requirement, as a large percentage of the participants do not have such test environments readily available. Those that do, probably also use those environments for testing upgrades and application changes as well, meaning those environments do not always mirror their production counterparts.	The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. The drafting team will take your comment into consideration for draft 3.
007-R2		
007-R3	R3.3 This requirement is confusing. What does physical access to an unattended facility have to do with generic account management? For unattended facilities (i.e. substations, backup facilities, unattended control buildings or rooms within a generating station) it is not practical to have approvals of physical access on an instance-by-instance basis. If a trusted employee who has been background screened, has a cardkey, token or other pre-approved access method for physical access to an unattended facility, and the other requirements as dictated by CIP-006 are in place, there is no need to have a separate function approve access each time that employee needs to enter such a facility. Regardless, any requirement of this type belongs in CIP-006. R3.5 This requirement belongs in standard CIP-006.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
007-R4		
007-R5		
007-R6	R6.3 The intent of this requirement escapes us. Why is this requirement specific to unattended facilities?	The distinction between attended and unattended facilities has been removed.
007-R7	R7.2 Again the intent of this requirement for unattended facilities escapes us. A facility that is unattended	Agreed, the Drafting Team revised R7 to reflect system logs

	(substation) should have the same logging requirements as those that are attended (control centers) if the assets housed there are critical.	to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8	R8 Does the change control process described in this environment relate to all changes or just those of a security software or patch nature? Please clarify the wording.	Change control and configuration management requirements have been moved to CIP-003, leaving a specific subset requirement concerning security patch management within CIP-007. Having said that, the change control and configuration management requirements in CIP-003 do indeed apply for any and all cyber assets that are deemed to be critical. So, yes, these requirements also apply for changes to, say, firmware in a relay that's deemed to be critical, whether it's flash upgraded/patched, or the chip itself is replaced.
007-R9		
007-R10		
007-R11	R11 For clarity purposes, this requirement is more appropriate to be contained in CIP-009 Recovery Plans. The level of detail discussed in this section is not currently covered in CIP-009, and having recovery requirements in two separate standards only leads to confusion and creates the possibility of conflicting requirements in future standards versions. Any recovery plan should specify the data, retention period, etc to be backed up for recovery purposes. Including in this section only increases administration on the part of the individual entities for developing procedures, and monitoring compliance.	This requirement has been deleted.
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		

CIP-007 Responses to Comments

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Pedro Modia
Entity Florida Power and Light

	Comment	*Response*
General		
007-R1		
007-R2	R2. The intent of this statement is not clear. Please provide clarification beginning at: The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		

CIP-007 Responses to Comments

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

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

	Comment	*Response*
General	CHGE feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1	Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>> to <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>> We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.	The assumption that every entity has a test system is incorrect. The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. This will be clarified in draft three.
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive and should be deleted. The <<monthly review>> in Requirement R4.2 is too prescriptive. We recommend changing R4.2 from << The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.

	>> to << The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch. >> Add <<where technically feasible>> to the end of Requirement R4.3.	
007-R5	Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means. Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3. The combined requirement should allow technically feasible alternative solutions. Change Requirement R5.2 from <<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> to <<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.>> to <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>> Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>> Change Requirement 6.1.4 from <<Security patches and anti-virus version levels>> to <<Assessing security patches and/or anti-virus version levels, as appropriate>> The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an	1) Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007. 2) Acknowledged. These matters arte now addressed in R9. 3) Acknowledged. These matters arte now addressed in R9. 4) Acknowledged. The distinction between attended and unattended facilities has been removed.

	attended facility?	
007-R7	The title of Requirement R7 is too broad. We recommend changing this title from <<Retention of System Logs>> to <<Retention of Appropriate System Logs>> The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3 and addresses your comments.
007-R8		
007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The test requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	This requirement has been deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.
007-M5	Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>	1) Yes, the Responsible Entity identifies the appropriate system logs to retain. Each Responsible Entity's systems environment will be at least a little different, so only the Entities themselves can appropriately determine an adequate strategy. 2) Good and valid suggestions all, and in Draft 3 we think we have words more reflective of what you have suggested. The Requirements section has been significantly altered in Draft 3, with some material moved to other sections. We should be pretty close to the intentions outlined in the comment, but if additional word smithy is felt to be necessary, please offer those suggestions during the Draft 3 comment period.
007-M6		

007-M7		
007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.	The measure has been revised to clarify that CIP-005 covers equipment on the electronic perimeter and CIP-007 covers equipment inside the perimeter.
007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2	Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

Commentor Richard Engelbrecht
Entity Rochester Gas and Electric

	Comment	*Response*
General	NPCC feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1	Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>> to <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>> We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.	The assumption that every entity has a test system is incorrect. The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. This will be clarified in draft three.
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive and should be deleted. The <<monthly review>> in Requirement R4.2 is too prescriptive. We recommend changing R4.2 from <<The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.>>	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the

	to <<The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.>>	technically feasible or non-feasible aspect of the patch.
	Add <<where technically feasible>> to the end of Requirement R4.3.	
007-R5	Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.	The drafting team has removed references to Integrity Software and has restructured the section.
	Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.	
	The combined requirement should allow technically feasible alternative solutions.	
	Change Requirement R5.2 from <<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades. >> to <<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>>	
	NPCC Participating Members do not agree with <<site-specific installation>> in Requirement 5.4. and recommend changing from <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.>> to <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>	
007-R6	Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>>	1) Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007. 2) Acknowledged. These matters arte now addressed in R9.
	Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>>Change Requirement 6.1.4 from<<Security patches and anti-virus version levels >>to<<Assessing security patches and/or anti-virus version levels, as appropriate>>	3) Acknowledged. These matters arte now addressed in R9.
	The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an attended facility	4) Acknowledged. The distinction between attended and unattended facilities has been removed This requirement has been deleted.
007-R7	The title of Requirement R7 is too broad. We recommend changing this title from <<Retention of System Logs>>to<<Retention of Appropriate System Logs>>	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3.
007-R8		

CIP-007 Responses to Comments

007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	This requirement has been deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.
007-M5	The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain. Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>	1) Yes, the Responsible Entity identifies the appropriate system logs to retain. Each Responsible Entity's systems environment will be at least a little different, so only the Entities themselves can appropriately determine an adequate strategy. 2) Good and valid suggestions all, and in Draft 3 we think we have words more reflective of what you have suggested. The Requirements section has been significantly altered in Draft 3, with some material moved to other sections. We should be pretty close to the intentions outlined in the comment, but if additional word smithy is felt to be necessary, please offer those suggestions
007-M6		
007-M7		
007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.	The drafting team agrees with the comment and has updated the standard.

007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2	Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor	Richard Kafka
Entity	Pepco Holdings, Inc. - Affiliates

Comment		***Response***
General	CIP-007-1 Includes much material that also appears elsewhere. Such duplication should be eliminated. The approach taken in these comments is to suggest that material in other sections be removed if it is duplicative of CIP-007. n general, much of this standard appears to have been duplicated in other standards. We suggest that the other material be removed.	The Drafting Team will review the standard and remove duplications where possible or provide clarification.
007-R1		
007-R2		
007-R3	R3.3, 3.5. It would be more appropriate to move these two Requirements into CIP-006, as they appear to relate more to physical access. R.3.4. In this case, it may be more appropriate to address the issue in CIP-003-1 Requirement R5.5 where there is similar material.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
007-R4		
007-R5		
007-R6	R6.1.3, 6.1.4. There appear to be no Measures that correspond to these two Requirements. As noted above, Measures and Requirements should correlate one-for-one.	You are correct, thank you.
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2	M2. The second half of this measure, reviewing access permissions, appears already to be covered, and more appropriately located in, the personnel standard CIP-004. It should be removed from this Measure.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		

CIP-007 Responses to Comments

007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2	Compliance 2.2.1.1. In CIP-003-1 Compliance 2.2.2, the applicable review period is one calendar year. Although the review issue should be addressed here rather than there, that longer period is the more appropriate term for review.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Compliance 2.3. The intent of the list of items is unclear. The list may be appropriate, although overly complex, if Level 3 noncompliance results from noncompliance with all of the items on the list. On the other hand, it would be completely inappropriate for Level 3 noncompliance to result from noncompliance with any one or two items on the list. If the original intent was to do just that, then this entire structure should be moved to Level 2, as otherwise it is far too easy to fall into the most severe Level 3 noncompliance. Why is there so many items listed under a Level 3 non-compliance? Should some of the items in Level 3 be in Level 2?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor	Robert L. Sypult
Entity	Southern California Edison

Comment		*Response*
General		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	CIP-007-1.R6.1.2 - Scanning for open ports/services and modems. It should be clearly stated that ANY penetration testing/scanning for vulnerabilities is NOT to be performed on the production system, it will ONLY be performed on either the backup control center or the test system configured and running like the production system. In the case where it is not possible to perform penetration testing on an off-line system (due to lack of back of control center or test system), an extensive review of hardware and software configurations shall be performed and documented.	--Agreed, We hope the wording in Draft 3 better clarifies and emphasizes the requirement
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		

CIP-007 Responses to Comments

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Robert Strauss
Entity New York State Electric & Gas Corporation

	Comment	*Response*
General	NYSEG concurs with NPCC that CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1	Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>> to <<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>> We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.	The assumption that every entity has a test system is incorrect. The requirement is to perform the test and do so without affecting production in the process. If a production system can be configured in such a way as not to affect production during testing it can be used. This will be clarified in draft three.
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive and should be deleted. The <<monthly review>> in Requirement R4.2 is too prescriptive. We recommend changing R4.2 from <<The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.>> to <<The Responsible Entity shall perform a routine review of the security patches available for each Critical	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.

	Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.>> Add <<where technically feasible>> to the end of Requirement R4.3.	
007-R5	Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means. Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3. The combined requirement should allow technically feasible alternative solutions. Change Requirement R5.2 from <<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades. >> to <<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>> NPCC Participating Members do not agree with <<site-specific installation>> in Requirement 5.4. and recommend changing from <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.>> to <<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6	Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>> Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>>Change Requirement 6.1.4 from<<Security patches and anti-virus version levels >>to<<Assessing security patches and/or anti-virus version levels, as appropriate> > The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an attended facility?	1) Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007. 2) Acknowledged. These matters arte now addressed in R9. 3) Acknowledged. These matters arte now addressed in R9. 4) Acknowledged. The distinction between attended and unattended facilities has been removed.
007-R7	The title of Requirement R7 is too broad. We recommend changing this title from <<Retention of System Logs>>to<<Retention of Appropriate System Logs>>	Agreed, the Drafting Team revised R7 to reflect system logs to specifically "Security Status Monitoring" in Draft 3.
007-R8		

007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	This requirement has been deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.
007-M5	The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain. Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>	1) Yes, the Responsible Entity identifies the appropriate system logs to retain. Each Responsible Entity's systems environment will be at least a little different, so only the Entities themselves can appropriately determine an adequate strategy. 2) Good and valid suggestions all, and in Draft 3 we think we have words more reflective of what you have suggested. The Requirements section has been significantly altered in Draft 3, with some material moved to other sections. We should be pretty close to the intentions outlined in the comment, but if additional word smithy is felt to be necessary, please offer those suggestions
007-M6		
007-M7		

CIP-007 Responses to Comments

007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.	The drafting team agrees with the comment and has updated the standard.
007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2	Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,3	Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

CIP-007 Responses to Comments

Commentor Roger Champagne
Entity Hydro-Québec TransÉnergie

	Comment	*Response*
General	HQTÉ feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	The Drafting Team will review CIP-007 and make the appropriate updates based on comments received on Draft 2.
007-R1		
007-R2		
007-R3	Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006. Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft. This requirement addresses the technical aspects of user accounts and permissions and verification that they align with access permissions. The standard will be updated for clarification and reference to the appropriate access requirement standards.
007-R4	Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>. Requirement R4.1 is too prescriptive Add <<where technically feasible>> to the end of Requirement R4.3. Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3. R5 has been changed in draft 3 to reflect the change to "Anti-virus Software" from "Integrity Software.
007-R5	Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3. The combined requirement should allow technically feasible alternative solutions. Change Requirement R5.2 from <<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>>to<<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity	The drafting team has removed references to Integrity Software and has restructured the section.

	software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>>	
007-R6	Change Requirement R6.1 from <<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>> to <<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>> Change Requirement 6.1.3 from <<Factory default accounts>> to <<Scanning for factory default accounts>> Change Requirement 6.1.4 from <<Security patches and anti-virus version levels>> to <<Assessing security patches and/or anti-virus version levels, as appropriate>> The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assessment schedule than an attended facility?	1) Acknowledged. While not stated in just these terms, this requirement is now expressed in section R2 of CIP-007. 2) Acknowledged. These matters arte now addressed in R9. 3) Acknowledged. These matters arte now addressed in R9. 4) Acknowledged. The distinction between attended and unattended facilities has been removed.
007-R7		
007-R8		
007-R9	Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10	The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.	This requirement has been deleted.
007-R11	Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.	This requirement has been deleted.
007-M1		
007-M2	Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4	<<where applicable>> should added to the end of Measure 4.3.	The drafting team agrees with the comment and has updated the standard.

007-M5	Change the Measures M5.1 - M5.3 from <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >> to <<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.>>	1) Yes, the Responsible Entity identifies the appropriate system logs to retain. Each Responsible Entity's systems environment will be at least a little different, so only the Entities themselves can appropriately determine an adequate strategy. 2) Good and valid suggestions all, and in Draft 3 we think we have words more reflective of what you have suggested. The Requirements section has been significantly altered in Draft 3, with some material moved to other sections. We should be pretty close to the intentions outlined in the comment, but if additional word smithy is felt to be necessary, please offer those suggestions
007-M6		
007-M7		
007-M8	Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.	The drafting team agrees with the comment and has updated the standard.
007-M9		
007-M10	Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Which Requirement and Measurement is Compliance 2.1 associated with?	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,2		
007-C2,3		
007-C2,4		

Commentor Roman Carter
Entity Southern Company Generation

Comment		***Response***
General	There is much duplication between CIP-007 and CIP-003, CIP-005, and CIP-006. Either move the remaining elements from CIP-007 out and delete it or clearly delineate what belongs in it and remove the duplication. Due to the way that compliance results on these standards are reported to NERC, it is important that any one non-compliance issue not cause non-compliances across multiple standards. Entities, regions, and even the entire industry are deemed 'XX% compliant', so to keep those numbers reflecting reality it is imperative that single issues only be measured once to avoid double penalties. Levels of Compliance, Level 1 and Level 2 - It is stated that -two (and three, respectively) of the specific areas- in documents have not been reviewed or updated. Is this two (or three) things in any one document or in aggregate across all documents in this standard?	The Drafting Team will review the standard and remove duplications where possible or provide clarification. The Levels of Compliance will be updated for clarity.
007-R1	R1 --Combine all Testing requirements from this and R4 of CIP-003 under one standard. Regarding -significant changes- and security testing: most companies have traditionally relied on vendors to perform security testing as appropriate. We believe that to self-test and certify all -significant- changes against all known security vulnerabilities for all our systems would be a monumental task. We are trained and staffed for functional and operational testing. In R1 -- This requirement states that -The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities prior to being rolled into production-. How is this expected to happen for some vulnerability? For example, how would one verify for a known vulnerability to Internet Explorer or to the XP operating system that the fixes provided by Microsoft had indeed been successfully tested by them. As worded the only way the Responsible Entity would be able to verify success would be to try and develop a program to attack the vulnerability. In other words, as worded the responsible entity is required to verify security patches provided by a vendor do indeed fix the vulnerability. This is not practical.	Security testing is to verify that changes to systems comply with the entities cyber policies. The vendor can not necessarily test for these. If the vendor can document their tests follow your Security Test Procedures and test for your environment then this is acceptable. The standard will be updated to clarify the intent.
007-R2		
007-R3	In R3 -- The words -end user account- are used in the last sentence but are qualified by the parenthetical statement that implies accounts other than end user (i.e. administrator accounts are not typically referred to as -end user-). Suggest just removing the words -end user-.	The drafting team will take your comments into consideration for the next draft and update for clarification.
	R3.3-- Covered in CIP-006 under physical security and should not be under generic account mgt R3.5-- The electronic and physical monitoring aspects of CIP-005 and CIP-006 should cover this.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be
007-R4	R4 - Pg 5, Regarding security patch management and performing a monthly review of security patches for each asset: What will companies do if/when a vendor announces that an older version (application, OS, etc.) is no longer supported and should no longer be used? Could companies be forced into multiple expensive upgrades? R4 and M3 mention testing as it relates to security patches. During the NERC webcast, this testing was interpreted to mean that entities must test to insure the patch actually fixes the vulnerability. That is	Agreed, the Drafting Team believes that security patch management should be a continual process and the documentation and implementation of security patches should be contingent on the releases of patches and the discovery of security vulnerabilities. A 30-day window to document the entities appropriate response to the security patch and vulnerability has been added to draft 3.

	impractical and entities should not be in the business of developing exploit code to test vulnerabilities, nor should they be deemed non-compliant if their scanning engines do not have a signature for said vulnerability (some vulnerabilities cannot be detected via a network scan anyway). The term -testing- can also be interpreted as testing to insure that security patches do not compromise the availability of any critical cyber assets and the testing documentation would show that security patches are not blindly applied to critical cyber assets without first knowing their impact to the environment. This interpretation of -testing- seems more in line with the spirit of CIP-007 and is more reasonable.	clarified in the next draft.
007-R5	R5.1-- Delete the confusing phrase -that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer)-. Simplify this to the blanket statement -shall use integrity software on all Critical Cyber Assets to prevent, limit, ...- and let R5.3 handle the exceptions where it can't be used. The term -Integrity Software- needs to be defined in the Definitions of this Standard. R5.2 --Since the #1 integrity software tool is antivirus packages, it is unclear why this is requiring a "monthly review of the available integrity software" R5.4 Unclear what this means	The drafting team has removed references to Integrity Software and has restructured the section.
007-R6		
007-R7		
007-R8	R8 --Change Management requirements and measures should be combined and either placed in CIP-003 or in CIP-007 but not spread across both.	Agreed. Change control and configuration management requirements have been moved to CIP-003, leaving a specific subset requirement concerning security patch management within CIP-007.
007-R9	R9-- Disabling Unused Ports requirements and measures should be combined and either placed in CIP-005 or in CIP-007 but not spread across both.	The measure has been revised to clarify that CIP-005 covers equipment on the electronic perimeter and CIP-007 covers equipment inside the perimeter.
007-R10	R10 -- The implications of the words -to monitor operating state, utilization and performance, and cyber security events- is going beyond the scope of a Cyber Security Standard particularly the -operating state, utilization and performance- requirements. If the intent is to monitor these parameters for possible intrusion and security compromise through abnormal -fingerprints- in these parameters that makes sense and it should be stated that is the intent. To imply the requirement for general monitoring of these parameters for other reasons such as operational efficiency of the users due to overloaded processors, database capacity, excessive I/O due to defective coding, etc., although good practices for other reason, is beyond the scope of this standard. Perhaps the words at the end could be modified to and issue alarms for specified indications of possible intrusion and or security compromise, as implemented- could be use to be more specific and appropriate.	This requirement has been deleted.
007-R11		
007-M1		

007-M2	M2 --The sentence beginning "Review access permissions within 24 hours for personnel terminated for cause..." should be deleted as this is covered in CIP-004.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M3		
007-M4		
007-M5		
007-M6		
007-M7	M7.1 --Change Mgt controls and Testing Procedures should be measured in CIP-003 or here but not both. M7.2 --Change Mgt controls and Testing Procedures should be measured in CIP-003 or here but not both.	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M8	M8 Disabling Unused Ports should be measured in CIP-005 or here, but not both.	
007-M9		
007-M10	M 10.2 -- There is no requirement to document recovery procedures for reconstruction and Critical Cyber Asset from the backup data. R11 only requires storing and testing not the documentation. Although a good practice, if its expected to be documented (i.e., staff may know how to do it without documentation) then should that not be also stated in the R11 requirements. M 10.3 - How would the documentation required verify one is -capable of recovering- from a Critical Cyber Asset failure? Is this implying that tests performed verified this capability then state that the test results should be documented? Be explicit.	This requirement has been deleted.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3	In Levels of Compliance, Level 3 - Remove 2.3.9 and 2.3.10 because they are -N/A- and serve no purpose. Non-Compliance levels 2.3.8, 2.3.9, and 2.3.10 should follow their appropriate requirements and measures if they move to other standards.	The standard will be updated such that the compliances align with the requirements and reviews are consistent throughout the standards.
007-C2,4		

Commentor Scott R Mix
Entity KEMA

	Comment	*Response*
General	There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual). In FAQ CIP-007-1.Q8, please comment on how a "security patch" is considered a "significant change" requiring testing, while a "Version revision" is not a "significant change" and therefore may not require testing. FAQ CIP-007-1.Qnew Why does requirements R6.1.2 require scanning of "functionally identical test systems", not the actual productions systems? Answer: Scanning of production systems by vulnerability testing tools and port scanners have caused operational problems, including the complete loss of function on the systems being scanned. Scanning for vulnerabilities is important, but it cannot be done at the expense of a functioning system. The scanning of "functionally identical test systems" provides for the testing and identification of the vulnerabilities, while not impacting the production environment. FAQ CIP-007-1.Qnew: What is meant by "Integrity Software"?	The Drafting Team agrees with your comment regarding Requirements and Measures alignment and will update the standard accordingly. The standard states that a "security patch" and "Version Upgrades" are considered significant changes. Significant changes include major product releases, characterized as "x to y", e.g., Oracle 7 to Oracle 8. New versions are significant software changes that constitute a major change to a release level, characteristically identified as "x.1 to x.2" or greater increments; these are sometimes referred to as "point releases." Version revisions are typically denoted as "x.1.1 to x.1.2.", but these typically do not constitute a significant change. This is not always the case however, so "read me" notes should be consulted for specific naming conventions, content, and impact applicability. In general, it is better to err on the side of conservatism when change impact is not well quantified. Security patches require testing as they implicitly affect cyber security. The testing requirement is in place to ensure significant changes do not compromise the entity's current cyber security controls. The Drafting Team will update the standard to clarify "Integrity Software" requirements. Integrity monitoring tools are intended to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malicious software (mal-ware) on systems within all Electronic Security Perimeters. The Drafting Team will update the standard to clarify the scanning requirement and the "Integrity Software" term, thus these FAQ's will not be required.
007-R1	Requirement R1: Insert the following sentence between the existing first and second sentences: "These test procedures shall take into consideration the special needs and requirements of the Critical Cyber Assets covered by this standard." Requirement R1: The requirement to test installation of security patches "for known security vulnerabilities" as discussed in the 2/2/05 web cast is excessive. On the other hand, it may be reasonable to require testing for security vulnerabilities when installing new application code to ensure that the new application does not introduce vulnerability into the system. Is a testing certificate fro the application developer sufficient? Please clarify	The testing requirement is to test changes to verify they comply with the entities security policies and procedures and do not introduce vulnerabilities. A testing certificate from the vendor will suffice if the vendor can simulate the entities and environment for testing. The standard will be updated accordingly.
007-R2		

007-R3	Requirement R3.1: add the following phrase to the end of the first sentence: ", subject to the technical limitations of the secured Critical Cyber Asset"	The drafting team will update the standard to clarify and appropriately reflect the intent.
007-R4		
007-R5		
007-R6	Requirement R6.1.2. Split into two requirements: R6.1.2 Scanning of functionally identical test systems for open ports/services R6.1.3 Scanning for modems	Done.
007-R7		
007-R8		
007-R9	Requirement R9. Add the following sentence: "In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall use and document (a) compensating measure(s)."	The drafting team agrees and has updated the requirement.
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8	Measure M8. Add the following sentence: "If unused ports and services cannot be disabled due to technical limitations of the device, documentation of other compensating measures must be provided."	
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		

CIP-007 Responses to Comments

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Terry Doern
Entity Bonneville Power Administration, Department of Energy

	Comment	*Response*
General		
007-R1	R1 Issue: Many of the requirements in R1 should apply to Critical Cyber Assets in unattended facilities. Recommendation: Change R1 so that it addresses all requirements that apply to both attended and non-attended.	The drafting team agrees and will update the standard accordingly.
007-R2	R2 Change R2 to address the requirement of storing procedures at an attended site.	The drafting team will remove references to attended and unattended facilities in the next draft, procedures requirements will be the same for both. This will be clarified in the next draft.
007-R3	R3: Define Attended and Unattended R3.2 Issue: Many of the requirements in R3.2 should apply to Critical Cyber Assets in unattended facilities also. Recommendation: Delete 'Attended' or change the wording on R3.2 so that it is understood which requirements apply to cyber assets at both attended and unattended facilities. R3.3 Issue: Change item to address only that users must request physical access to an unattended facility for each individual event OR delete 3.3 OR move to the physical standard.	The drafting team will remove references to attended and unattended facilities in the next draft and update the standard for clarity. The intent was for field devices and the standard will be updated where applicable to reflect this intent.
007-R4		
007-R5		
007-R6		
007-R7		
007-R8	R8.1 and M7 Issue: Requirement R8.1 and M7 appear to be duplicates of CIP-003-1 R4.2 and M13.2. CIP-003 should be focused on management level policies, roles, responsibilities and procedures that apply to all systems while CIP-007 should be a system level requirement to ensure the Change Control Process has been and is being followed. Recommendation: Modify CIP-003 R4 such that it is clear the measures and compliance is management level documentation. Modify CIP-007 so it is clear the measures and compliance are system level documentation (i.e., a system unique identifier, system user and maintenance documentation that represents the system, test reports for the production version of the system, etc.)	The comment is well taken, and the drafting team agrees in essence. We hope and believe that we have rectified most of these inconsistencies in Draft 3. Thank you.
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		

CIP-007 Responses to Comments

007-M3		
007-M4		
007-M5		
007-M6		
007-M7	R8.1 and M7 Issue: Requirement R8.1 and M7 appear to be duplicates of CIP-003-1 R4.2 and M13.2. CIP-003 should be focused on management level policies, roles, responsibilities and procedures that apply to all systems while CIP-007 should be a system level requirement to ensure the Change Control Process has been and is being followed. Recommendation: Modify CIP-003 R4 such that it is clear the measures and compliance is management level documentation. Modify CIP-007 so it is clear the measures and compliance are system level documentation (i.e., a system unique identifier, system user and maintenance documentation that represents the system, test reports for the production version of the system, etc.)	The standard will be updated such that the measures align with the requirements and reviews are consistent throughout the standards.
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Responses to Comments

Commentor Tony Eddleman
Entity Nebraska Public Power District

Comment		***Response***
General		
007-R1	Requirement R1 states to test for known security vulnerabilities. This means we must have the malicious software to run the test and the expertise. This is not practical nor logical. If Microsoft puts out a patch for a known vulnerability, we should not have to test using the malicious software. What if the problem is for a vulnerability and the malicious software hasn't been developed yet - are we suppose to develop the malicious software to use for testing? We should test our critical cyber asset to make sure their patch doesn't fail to corrupt the system, but we shouldn't have to test the malicious software.	The drafting team agrees with your comment and will update the standard accordingly.
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		

CIP-007 Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor	Tony Kroskey
Entity	Brazos Electric Power Cooperative

	Comment	*Response*
General		
007-R1	The R1 requirement for testing of security patches is unreasonable. As discussed in the phone meeting on Feb 2, the requirement to check for known vulnerabilities was interpreted to mean that each company would have a test environment that they would use to attempt to exploit the system with the known vulnerability after patches are applied in order to prove that the vulnerability was successfully dealt with. This is unreasonable for several reasons. Several known vulnerabilities have no known exploits making the requirement all but impossible. Several vulnerabilities that have exploits still require a high level of programming skill to exploit. Known exploit code that can be taken from the internet comes from suspect sites and should not be used even in a test lab unless you are prepared to do a complete rebuild of the lab. If you do find that the exploit was not fixed you can not write a patch to fix it, so you the only thing you have accomplished is the ability to notify the vendor that the patch does not work. A more appropriate requirement would be for each company to have the ability to test each system for patch requirements, have a test environment to test patches on before they are deployed on their production system, have a way to verify that the patch was actually applied, have a way to roll the patches back if they cause a problem. We should be held accountable for keeping all systems to the vendors specifications for a "secure" system, not the security testing entity for a vendor. If NERC is going to require the use of some type of vulnerability scanning to take place, then they need to supply a list of approved products as the capabilities of the products in this field vary widely.	The drafting team agrees and will update the standard accordingly.
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		

CIP-007 Responses to Comments

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor Trevor Tidwell
Entity Texas-New Mexico Power Company

	Comment	*Response*
General		
007-R1		
007-R2		
007-R3	With regards to R3.1 Strong Passwords, the use of strong password for user login to PC attached to the secured network only encourages written passwords, thus defeating any gain in using strong passwords. Once someone discovers where a user writes down his or her password then it is compromised. It is stated "Passwords shall be changed periodically per a risk-based frequency to reduce the risk of password cracking". Isn't that why strong passwords are required? It was knowing where the password was written down that allowed a character in the movie War Games to get into the school computer system, even after a periodic change in passwords. It may only be a movie, but it a long known hacker tactic. Strong Passwords should be required of electronic access points. All the other security measures are for not if a password is discovered written down. A good article regarding this is located at the following link http://www.smat.us/sanity/pwdilemma.html Also when we began to implement requirements for 1200, our auditors said that we should also have all accounts lock out via screensaver or some other mechanism after 10 minutes of inactivity. Our operator complained about have to recall the password if the system were to alarm and the screensaver had lock them out. Imagine what it would be like if a system event was occurring and the operator could not act in time because he could not remember the strong password required. Cyber security should be to protect the grid, not prevent the operator from controlling it. Inactivity of logged in user accounts is not addressed in CIP-002 through CIP-009.	The drafting team appreciates your comment and respectfully disagrees; changing passwords on a regular basis is good practice. This limits access time should a password be compromised. The drafting team encourages the used of multi-factor authentication such as tokens to prevent requirements for passwords, but if an entity does not use these, they must at a minimum have strong passwords and change them based on their environment. There is not currently a requirement in the standard to lock out accounts after periods of inactivity.
007-R4	R4 Security Patch Management refers to the testing of security patches. This is unrealistic. Many security patches deal with buffer overflows, and malformed TCP/IP packets. It would take sometime to train up staff to do this and not to mention hiring extra staff to cover this. We are hard pressed to keep staffing at a level to maintain SCADA, much less take on this responsibility. If testing is to make sure that the system suffers no ill effect in terms of up time or does not interfere with normal or emergency operation, then it is acceptable.	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.
007-R5	With regards to R5 Integrity Software, R5.1 states "use integrity software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer)". The statement could be better worded. A suggested statement is "use integrity software on all Critical Cyber Assets that are connected to unsecured network, or can connect to unsecured networks back through an electronic access point, or connected to a device that is connected to an unsecured network and the	The drafting team has removed references to Integrity Software and has restructured the section.

	device could transmit malicious software to the Critical Cyber Asset". The phrase "another device that is connected to a network" could include a master system talking via a serial link to an RTU that is connected to a substation network. This type of connection poses no threat since the serial communication is master poll driven, and no virus or intrusion to the master system is possible.	
007-R6	R6.1.2 Scanning for open ports/services and modems should be scanning for open ports/services and modems on access points to the Electronic Security Perimeter and for modems on Critical Cyber Assets. It is our position that open ports/services on access points is a valid concern, but not for all Critical Cyber Assets.	Draft 3 better clarifies and distinguishes port-level assessment relative to the electronic security perimeter and assets within, respectively. At the same time, we must respectfully disagree that there is less urgency concerning port-level protections on applicable critical cyber assets inside the perimeter. This contention is based upon the widely acknowledged importance of 'defense in depth' security tactics. Why? 1) Firewalls are hack-able; 2, protections must be maintained against threats from the inside; 3, if a 'host' is a critical cyber asset and it has been compromised, then it's possible for said asset to infect neighbor machines. Responsible Entities are responsibility for protecting critical cyber assets, and how that shall be done is ultimately up to same. Conventional wisdom argues against the perspective proffered in this comment.
007-R7		
007-R8		
007-R9	R9 refers to disabling unused host ports/services. However CIP-005 also addresses this issue. The wording should be changed to allow for better distinction of what each is to cover. If no wording change is to be made then it should only be in this CIP. See my comments under CIP-005 regarding suggested rewording for CIP-005. While the wording could be changed to clarify that R9 refers only to Critical Cyber Assets and not any electronic access point, it is our position that this is unnecessary. The secure network has not only strong controls to the electronic access points, but also to the physical security. It is hard to disable all ports and services on all Critical Cyber Assets because it may not be known what is and is not being used. Our system does not run email, touch the Internet, and has firewall separating it from the corporate network. Considering this and the other security implementations, the disabling of all unused ports seems beyond excessive. Either make a caveat for systems that have a very low or no profile to the outside world, or remove this requirement.	The requirement has been restructured and now indicates that CIP-005 applies to devices on the Electronic Perimeter.
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		

CIP-007 Responses to Comments

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Responses to Comments

Commentor	William J. Smith
Entity	Allegheny Power

Comment		***Response***
General		
007-R1		
007-R2		
007-R3		
007-R4	R4 --The requirement of testing installed patches to ensure that they address a particular vulnerability is unreasonable. Vulnerabilities are most often identified by system vendors and may not be readily reproduced by system administrators. The reference to testing should be removed.	The Drafting Team feels strongly that the continual review of security patches is a recognized best security practice in maintaining a secure critical infrastructure. Not all patches can be installed due to operations maintenance windows or in-compatibility with other applications and components. In those cases, the Drafting Team feels 30 days of notification and documentation of the time the security patch is released is sufficient time to test and document the technically feasible or non-feasible aspect of the patch.
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-R11		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4