Drafting Team Response to Comments on the Implementation Plan for CIP-002 — CIP-009

Response:
General Responses to Comments on Implementation Plan

The implementation plan associated with the current draft of the Cyber-Security Standards is posted for stakeholder review and comment. The stakeholder comments to Draft 1 of the implementation plan are summarized below, as is a summary of significant changes made to the plan as a result of the drafting team's evaluation of those comments.

The majority of the stakeholder comments can be summarized into three separate groups:

1. The implementation plan is too aggressive and does not allow enough time to achieve compliance considering the breadth and scope of the new standards when compared to the outgoing 1200 standard.
2. The compliance dates are not clear and need additional explanation.
3. What impact will a change in the implementation schedule of the Functional Model have on the cyber security standards?

The drafting team made significant changes to the implementation plan to address these comments. The drafting team's response to comments on the implementation plan is provided below.

Draft 2 of the implementation schedule has been significantly modified to recognize the time necessary to fully implement these standards. This includes the recognition that any undertaking of this scope requires first developing a plan to outline a Responsible Entity's implementation strategy. With this in mind, Draft 2 of the Implementation Plan includes a new phase of implementation referred to as "Begin Work." This phase represents the finalization of a Responsible Entity's plan to address a given Requirement in the standards. The Implementation Plan has been divided into three separate tables to recognize three separate groups of Responsible Entities:

1. Balancing Authorities and Transmission Operators that were required to self-certify compliance to NERC's Urgent Action Cyber Security Standard 1200 (UA 1200), and Reliability Coordinators;
2. Transmission Operators and Balancing Authorities that were not required to self-certify compliance to UA Standard 1200, Transmission Providers, and the offices of NERC and the Regional Reliability Organizations.
3. Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators, and Load-Serving Entities.

Entities in the first two groups have registered per the Functional Model. Entities in the third group, although most likely identifiable, have yet to register to the model and, as such, are not currently included in the NERC Compliance Program. For Responsible Entities in the first two groups, the implementation plan requires Auditable Compliance to all Requirements by second quarter 2009. For Responsible Entities in the third group, the implementation plan requires Auditable Compliance to all Requirements within 36 months of the registration to a Functional Model function.

In regard to the implementation of the Functional Model, the drafting team wishes to point out that standards need to be developed and implemented on a schedule dictated by reliability need and availability of resources to achieve and monitor compliance. The Functional Model should not become an impediment to the devel\opment or implementation of reliability standards.

Comments:

Name	Entity	Comments
Bob Wallace	Ontario Power Generation	OPG feels the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the

		2007 dates change to 2008 dates, etc. We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date? If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?
Carol L. Krysevig	Allegheny Energy Supply Company	The requirements section of the compliance schedule do not match the actual standards. As such, a complete determination cannot be made. However, the electronic and physical security, as well as the systems security, sections CIP-005, CIP-006, CIP-007 should only be required to be auditably complete by 1st Qtr 2008. For Power Stations, there are potentially a significant number of systems that could be affected, requiring significant changes, upgrades, and new equipment to comply with these sections. Without actually performing the risk based analysis and cyber asset review, additional details are not available. CIP-001 does not have sections R2-R4 which are documented in the implementation plan. CIP-002 has section R-5 which is not documented in the implementation plan.
Earl Cahoe	Portland General Electric	Question: When something is to be Auditablilty Compliant in 1st quarter of 2006, does that mean, for the prior year the measures should have been in-place or does it mean starting in the 1st quarter of 2006, the measures should be in-place? In other words in the 1st quarter of 2006, would the auditors be auditing 2005's stated level of compliance or 2006's current level of compliance?
Name	**Entity**	**Comments**
Edwin C. Goff III	Progress Energy	Many stakeholders within Progress Energy feel this implementation plan is too aggressive in general. Rightfully so the new standards have an increased scope so that when properly implemented they will afford increased reliability and security of all of our critical cyber assets. We are fully on board with this direction but fell we all need more time to implement properly. Overall, we are struggling with doing the right thing from a safety, reliabiliy and security prespective to name a few and balancing that with other business drivers like missing the 2005 budget cycle, increased personnel requirements, and proper analysis of the impact of these initiatives to ongoing operations.
Francis J. Flynn, Jr.,	National Grid USA	NPCC feels the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these

		standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date? If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?
Gerald Rheault	Manitoba Hydro	The compliance schedule for Balancing Authorities and Reliability Coordinators is acceptable as stated. The compliance schedule for other facilities is too aggressive considering that most responsible entities will have multiple sites requiring compliance. We suggest that the compliance schedule for other facilities be delayed by one year with SC in 2006, SC in 2007 and AC in 2008.
Greg Mason	Dynegy Generation	The Implementation Plan needs to clarify the provisions that some entities need to be only "Substantially Compliant"(begun process to become compliant) by 1Q 2006,but it appears they will receive Self Certification forms to certify their compliance shortly after 1Q 2006.Is it the intent to only send these Self Certification forms to those entities required to be "Auditably Compliant" by 1Q 2006?

Name	Entity	Comments
Guy Zito	NPCC CP9	The Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. There is concern with compliance for substations. Substations are part of the <<Other Facilities>>. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date? If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?
Hattaway	AECoop	Putting these requirements in place will pose a significant challenge at plants given the number of critical systems. Recommend the following changes: Standard CIP-005-1 --Cyber Security --Electronic Security Standard CIP-006-1 --Cyber Security --Physical Security Standard CIP-007-1 --Cyber Security --Systems Security Management Substantially Compliant 1st Quarter 07, Auditably Compliant 1st Quarter 08
James W. Sample	California ISO	Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in Q1 2006 for the following reasons: •NERC CIP 002 through CIP-009 establish much deeper and wider requirements than NERC 1200 and will require a significant compliance effort even from those already in ful compliance with NERC 1200. •No budgeting can typically be done until the standards are confirmed and solidified. •Most budgets are confirmed four or five months prior to the fiscal target year. Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little to no impact and should be acceptable in view of the development of this new and major standard.

Name	Entity	Comments
		The implementation plan should recognize typical corporate fiscal planning processes.
		The Implementation Plan should be revised as follows: Change the year 2006 to 2007 in the first group of columns, and make corresponding changes to the year in subsequent columns by adding one year. In the first column, for control centers (in the year 2007 after having made the change noted previouly) change AC (auditably compliant) to SC (substantially compliant) in all instances. A good requirement would be to require that a corporate implementation plan for reaching auditable compliance be submitted by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis. Recommendation: Throughout these standards, a requirement is established to be able to provide up to three years of records for examination on request of an auditor. The wording of the standards or of the implementation plan should contemplate that entities may legitimately not have fully 3 years of records to submit until 3 years after they are required to come into Auditable Compliance. It may be suitable to require entities to identify the dates when the document retention processes will be deemed to begin as part of the implementation plan suggested above.
Jim Hansen	Seattle City Light	We like the implementation timeline matrix however it is tied to a specific date rather than the date of adoption of the standard. If the standard isn't adopted until the fourth quarter of 2005, then we are left with very little time to implement. Implementation of the plan in anticipation of a successful ballot without a ratified standard to refer to would be probelmatic if not impossible. We would like the implementation plan to tie its first due date to 6 months after the standard is adopted with all other dates changing, as in a gant chart.
Jim Hiebert	California ISO	We like the implementation timeline matrix however it is tied to a specific date rather than the date of adoption of the standard. If the standard isn't adopted until the fourth quarter of 2005, then we are left with very little time to implement. Implementation of the plan in anticipation of a successful ballot without a ratified standard to refer to would be probelmatic if not impossible. We would like the implementation plan to tie its first due date to 6 months after the standard is adopted with all other dates changing, as in a gant chart
John Lim	Con Edison	The scope and requirements of the standards have been substantially expanded from Urgent Action Standard 1200 and will not be finalized until September 2005. Because of budget planning cycles and in consideration of the substantial financial commitment required to meet these expanded requirements, full Auditable Compliance should be deferred to 2008 for entities owning a large number of field facilities (i.e. other than BA and RC).
Karl Tammer	ISO-RTO Council	The following is the position of the ISO/RTO Council Members: Since the standard will not become official before October 1, 2005, it is not realistic to

		expect an acceptable level of auditable compliance in Q1 2006. --NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort. --No budgeting can typically be done until the standards are confirmed and solidified. --Most budgets are confirmed four or five months prior to the fiscal target year. Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little impact and should be acceptable in view of the development of this new and major standard. The implementation plan should recognize typical corporate fiscal planning processes. Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis. Recommendation: The entity must identify the dates when the document retention processes must begin to be compliant with the standard.
Kathleen M. Goodman	ISO New England Inc.	Since the standard will not become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance in Q1 2006. Specifically: a) NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort; b) No budgeting can typically be done until the standards are confirmed and solidified; c) Most budgets are confirmed four or five months prior to the fiscal target year.Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little impact and should be acceptable in view of the development of this new and major standard.The implementation plan should recognize typical corporate fiscal planning processes.Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis Recommendation: The entity must identify the dates when the document retention processes must begin to be compliant with the standard.
Keith Fowler	Entity Name LG&E Energy Corp.	As noted under each of the previous sections we are in agreement with the comments submitted by the ECAR CIPP group. Additionally, we would like to emphasize that in general the timelines are not only too aggressive, but simply unrealistic. In particular if typical planning and budgeting cycles are taken into account implementation work required to address the increased scope likely will not yet have begun, let alone be complete, by the deadlines proposed in draft I of the implementation plan.

Name	Entity	Comments
Ken Fell	New York Independent System Operator	Given this standard is not expected to become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance by Q1 2006. The CIP's are much deeper and broader in scope than NERC 1200, and will require a significant compliance effort. Standards need to be confirmed and solidified prior to accommodate budgeting process. Budgets typically are confirmed 4-5 month's prior to fiscal target year. Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis.
Kenneth A. Goldsmith	Alliant Energy	The timeframe for full compliance should be extended to 1st quarter 2008. NERC should develop a training program to ensure companies understand the requirements and implement appropriately. This training program should be rolled out in late 2005, early 2006. That will allow companies time to work through any issues and implement by 3/31/08.
L.W. Brown	Edison Electric Institute	Regarding the implementation schedule, NERC must remain sensitive to the normal corporate budgetary cycle. Since many companies will be finished with or already well into finalization of their Fiscal Year 2006 budgets before these Standards could be approved, it would be unreasonable to expect more than "substantial compliance" in 2006.
Larry Conrad	ECAR Critical Infrastructure Protection Panel	CIP-002-1-- R1--Parameters for List of Assets: This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. (IROL's, etc.) R2--Routable protocol/dial up accessibility: This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. Differentiations such as routable protocol and dial up accessibility do not exist in Standard 1200. R4--Approval of list of assets: This requirement is NOT a "direct descendent" of Standard 1200. Approval of the list by senior management is a new requirement. CIP-003-1-- R2--Categorize ALL information: This requirement is NOT a "direct descendent" of Standard 1200 and goes MUCH farther than Standard 1200. Categorizing ALL of the information regardless of media type, senior management involvement etc. are new requirements. R3--Roles & Responsibilities: This requirement is NOT a "direct descendent" of Standard 1200. Defining the roles and responsibilities of all parties involved is a new requirement. R4--Governance Documentation: This requirement is NOT a "direct descendent" of

Standard 1200. Documenting a formalized governance process was not required in Standard 1200.

CIP-004-1--
R1--Awareness Program: This requirement is NOT a "direct descendent" of Standard 1200. A separate "Awareness Program" was not required in Standard 1200.
--

CIP-005-1--
R1--Electronic Perimeter: This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of CIO-005 has been expanded to include access from sub stations and generation facilities, the electronic access requirements to the perimeter have been expanded.
R4--Electronic Access Controls: This requirement is NOT a "direct descendent" of Standard 1200. Electronic Access controls to the EMS system will have to be created for substations and for generation facilities.
R5--Monitoring Electronic Access.: This requirement is NOT a "direct descendent" of Standard 1200. Means to monitor access controls to the EMS system will have to be created for substations and for generation facilities.
R6--Documentation: This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the new permanent standard has been significantly increased, much new documentation is now required over and above Standard 1200 requirements.

CIP-006-1--
R2--Access Controls following risk assessment: This requirement is NOT a "direct descendent" of Standard 1200. The generally accepted industry or government risk assessment procedure was not required in Standard 1200.
R5--Maintenance & Testing Program: This requirement is NOT a "direct descendent" of Standard 1200. Maintenance and Testing program was not required in Standard 1200.

R6--Documents: This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the permanent standard has been significantly increased over Standard 1200, additional documentation is required.

CIP-007-1--
R1--Testing & Environment: This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as documenting full detail of the test environment were not part of Standard 1200. Separating requirements for attended vs. un-attended facilities were not part of Standard 1200.
R3--Account & Password Mgt.: This requirement is NOT a "direct descendent" of Standard 1200. The requirements for password management such as strong passwords and the distinction between controls for unattended vs. attended facilities are new to the current version and did not appear in Standard 1200.
R4--Security Patches: This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the risk based assessment are new requirements in this standard and were not part of Standard 1200.
R5--Integrity Software: This requirement is NOT a "direct descendent" of Standard

		1200. Requirements such as the monthly review and the formal change control process for integrity software were not part of Standard 1200. R7--System Logs: This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the distinctions for managing logs at unattended facilities were not part of Standard 1200. R8--Change Control: This requirement is NOT a "direct descendent" of Standard 1200. The scope of the requirements for change control has been expanded over the requirements of Standard 1200. Specifics regarding the assets at unattended facilities were not part of Standard 1200. R10--Op. Status Monitoring: This requirement is NOT a "direct descendent" of Standard 1200. Operating Status monitoring and performance monitoring tools requirements have been significantly expanded over Standard 11200 requirements. R11--Backups & Recovery: This requirement is NOT a "direct descendent" of Standard 1200. Items such as the requirement that the backup must be stored in a remote locations and the requirement for annual tests to ensure recoverability are new to this standard. CIP-009-1-- R4--Notification of changes: This is not a "direct descendent" of Standard 1200. There was no requirement to notify personnel of changes within 7 calendar days of the modification. R5--Recovery Plan Training: This is not a "direct descendent" of Standard 1200. Standard 1200 did not contain a requirement that all the testing mirror testing defined in current CIP-004 Personnel and Training.
Larry Conrad	Cinergy	Self Certification, Page #1: Delete the references to self-certification in the Implementation Plan language. It is no longer relevant. Implementation Plan for "Other Facilities" (not Control Centers): Some weeks ago, participants had been asked to provide an estimate of how long it would take them to implement the proposed permanent standards. Cinergy indicated that approximately four (4) years would be required. However, the NERC implementation plan states that all entities must be audibly compliant with all sections by 1st quarter of 2007. We once again state that it will take four (4) years to implement all requirements of the proposed permanent standards. One year will be spent planning and the remaining time will be spent in implementation. If the implementation plan is not adjusted for all CIP sections, then at least the following need to be moved back for "other facilities," which are not Control Centers: --CIP006-1 Physical Security: It is not possible to implement the standards across the number of generation and substation sites involved by the 1st quarter of 2007. Deadline needs to be moved back as indicated by the participants. --CIP-003-1 Security Management Controls: It is not possible to implement the requirements, such as change management, password management, operating system monitoring tools, and testing, using the existing legacy EMS system. A new EMS system is on order and should provide the needed controls by early 2008. --CIP-007 Systems Security Management: It is not possible to implement the requirements such as change management, password management, operating system monitoring tools, and testing, using the existing legacy EMS system. A new EMS

system is on order and should provide the needed controls by early 2008.
--CIP-005-1 Electronic Security: Being able to sufficiently monitor the sites is tied to new capability to be delivered with the new EMS system. Due to the new requirements and number of sites which are involved, this requirement will be difficult to implement by 1st quarter of 2007.

Implementation Plan for Control Center Requirements to be Audibly Compliant by 1st Quarter of 2006, Page #2: We were told by an ECAR representative that Control Centers would be required to be 'audibly compliant' by 1st quarter of 2006 with those requirements, which were "direct descendent" of Standard 1200. In many cases the Control Centers are expected to be audibly compliant by 1st quarter, but the increase in scope has significantly altered the requirements in CIP-002-1 through CIP-009-1 vs. Standard 1200. Because the scope of the permanent standard has expanded so much over the requirements of Standard 1200, there are very few 'direct descendents' from Standard 1200 to the proposed permanent CIP-002-1 through CIP-009-1. For all of the items listed below, because the scope has increased, we do not agree that these are 'direct descendents' and we recommend that Control Areas should be given until 1st quarter of 2007 to be "audibly compliant."

For all of the following requirements, the Control Centers must now be Auditably Compliant by 1st Quarter of 2006.
For Control Centers, deadline to be Auditably Compliant should be changed to 1st Quarter of 2007, not 2006.

Comment
CIP-002-1----

R1--Parameters for List of Assets--This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. (IROL's, etc.)
R2--Routable protocol/dial up accessibility--This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. Differentiations such as routable protocol and dial up accessibility do not exist in Standard 1200.
R4--Approval of list of assets--This requirement is NOT a "direct descendent" of Standard 1200. Approval of the list by senior management is a new requirement.

CIP-003-1----
R2--Categorize ALL information--This requirement is NOT a "direct descendent" of Standard 1200 and goes MUCH farther than Standard 1200. Categorizing ALL of the information regardless of media type, senior management involvement etc. is a new requirement.
R3--Roles & Responsibilities--This requirement is NOT a "direct descendent" of Standard 1200. Defining the roles and responsibilities of all parties involved is a new requirement.
R4--Governance Documentation--This requirement is NOT a "direct descendent" of Standard 1200. Documenting a formalized governance process was not required in Standard 1200.

CIP-004-1----
R1--Awareness Program--This requirement is NOT a "direct descendent" of Standard 1200. A separate "Awareness Program" was not required in Standard 1200.

CIP-005-1----
R1--Electronic Perimeter--This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of CIP-005 has been expanded to include access from sub stations and generation facilities, the electronic access requirements to the perimeter have been expanded.
R4--Electronic Access Controls--This requirement is NOT a "direct descendent" of Standard 1200. Electronic Access controls to the EMS system will have to be created for substations and for generation facilities.
R5--Monitoring Electronic Access.--This requirement is NOT a "direct descendent" of Standard 1200. Means to monitor access controls to the EMS system will have to be created for substations and for generation facilities.
R6--Documentation--This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the new permanent standard has been significantly increased, much new documentation is now required over and above Standard 1200 requirements.

CIP-006-1----
R2--Access Controls following risk assessment--This requirement is NOT a "direct descendent" of Standard 1200. The generally accepted industry or government risk assessment procedure was not required in Standard 1200.
R5--Maintenance & Testing Program--This requirement is NOT a "direct descendent" of Standard 1200. Maintenance and Testing program was not required in Standard 1200.
R6--Documents--This requirement is NOT a "direct descendent" of Standard 1200.

Because the scope of the permanent standard has been significantly increased over Standard 1200, additional documentation is required.

CIP-007-1----
R1--Testing & Environment--This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as documenting full detail of the test environment were not part of Standard 1200. Separating requirements for attended vs. un-attended facilities were not part of Standard 1200.
R3--Account & Password Mgt.--This requirement is NOT a "direct descendent" of Standard 1200. The requirements for password management such as strong passwords and the distinction between controls for unattended vs. attended facilities are new to the current version and did not appear in Standard 1200.
R4--Security Patches--This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the risk based assessment are new requirements in this standard and were not part of Standard 1200.
R5--Integrity Software--This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the formal change control process for integrity software were not part of Standard 1200.
R7--System Logs--This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the distinctions for managing logs at unattended facilities were not part of Standard 1200.

		R8--Change Control--This requirement is NOT a "direct descendent" of Standard 1200. The scope of the requirements for change control has been expanded over the requirements of Standard 1200. Specifics regarding the assets at unattended facilities were not part of Standard 1200. R10--Op. Status Monitoring--This requirement is NOT a "direct descendent" of Standard 1200. Operating Status monitoring and performance monitoring tools requirements have been significantly expanded over Standard 11200 requirements. R11--Backups & Recovery--This requirement is NOT a "direct descendent" of Standard 1200. Items such as the requirement that the backup must be stored in a remote locations and the requirement for annual tests to ensure recoverability are new to this standard. ---- CIP-009-1---- R4--Notification of changes--This is not a "direct descendent" of Standard 1200. There was no requirement to notify personnel of changes within 7 calendar days of the modification. R5--Recovery Plan Training--This is not a "direct descendent" of Standard 1200. Standard 1200 did not contain a requirement that all the testing mirror testing defined in current CIP-004 Personnel and Training.
Laurent Webber	Western Area Power Administration	The Auditably Compliant criteria for BA & RC Control Centers should be delayed another year. Substantial Compliance must be considered adequate for the first year. There is uncertainty as to the volume of documentation and the resources required to comply with the Cyber Security Standard. Given that the Standard is adopted by September 2005 the Implementation Plan calls for Control Centers to be Audit Compliant by 1st Quarter 2006. That is only 3 months and those months include some major holidays. It is absolutely unreasonable to allow only 3 months to evaluate the new Cyber Security Standard, assess compliance, define cyber and physical boundaries, install physical access controls, install physical monitoring devices, generate an undetermined amount of documentation, perform numerous background checks, choose and implement numerous cyber monitoring and auditing tools, and a multitude of other tasks.
Lawrence R Larson,	Midwest Reliability Organization	All compliance requirements should be delayed an additonal year. Starting the first quarter of 2006, NERC should work with the industry to gather examples of documents that would fulfill the requirments of this Standard - that is, to gather best practices examples. In mid-2006, NERC should host industry training sessions to review this material. This would give companies the last half of 2006 to review their current documentation as compared to these examples, and make adjustments as required. Field testing should also be provided for. The phased-in (AC vs SC and Control Center vs Other Facilities) approach, as defined in the Implementation plan, should then commence in 2007. This assumes the schedule proceeds as defined in the assumptions bulleted at the beginning of the Implementation Plan.
Lee Matuszczak	U S Bureau of Reclamation	No specific comments, but implementation, if accelerated too quickly, may result in poor implementation practices and improperly vetted procedures. In some instances, this could lead to counter-productive actions in times of crisis. All plans and procedures should be afforded adequate time for development, vetting and testing before penalty-based audits are started.

Linda Campbell	FRCC	The new standards are a significant increase in scope and requirements over the existing 1200 standard. Implementation and ongoing maintenance of the technical controls required by this standard across the industry will entail time and cost many millions of dollars. Implementation to a point of auditable compliance will likely take several years for many larger organizations, with significant generation or transmission systems. The timetable for passage of this standard has missed 2005 budget cycles, and the standard may not be finalized and passed before most entities can identify costs and budget for 2006. As such we believe that NERC has an obligation to perform a thorough impact analysis, with full participation from the industry, as a part of implementation plan development, and allow for a phased in implementation across multiple years. We support the need for these critical standards. But we don't support standards that neglect costs, complexity and reasonable timeframes for implementation.
Lyman Shaffer	Pacific Gas and Electric Company	All items are required to be substantially compliant by 1st quarter 2006 for TO. Given the fact that the emergency action cyber standard did not apply to a significant portion of the industry and the permanent standard will not be in effect until well into 2005, this is unreasonable particularly as it will apply to a large number of facilities, employees and procedures. The time frame for substations and other facilities other than control centers will clearly be insufficient
Marc Butts	Southern Company, Transmission, Operations, Planning and EMS Divisions	The implementation plan only addresses when entities should be "auditably compliant' but does not address the introduction of audits, sanctions, or penalties as previous implementation plans have addressed.
Mr. Dennis Kalma	Alberta Electric System Operator (AESO)	As a general comment, we feel that the implementation timetable is too rigorous. It does not align with corporate budgets nor take into consideration the magnitude of the effort to go from NERC 1200 to CIP 002-009. We believe that entities should be requested to certify they will remain compliant with NERC 1200 indefinitely and that 2006 be a planning and budget year for CIP 002-006 implementation with 2007 requiring compliance.
Patrick Miller	PacifiCorp	PacifiCorp has double (or more) the Transmission line mileage than any other WECC member. Additionally, PacifiCorp has many more substations that most other utilities, by far. Please consider allowing an exception or extension to the compliance for "other facilities" where this is the case. The terms "Auditably Compliant" and "Substantially Compliant" would be more effective (and accepted) if there were more language around exactly what they mean. Consider providing a minimum and maximum specification or framework for each. As they stand, there is a considerable amount of ambiguity which could lead to misinterpretation.
Paul McClay	Tampa Electric	The new standards are a significant increase in scope and requirements over the existing 1200 standard. Implementation and ongoing maintenance of the technical controls required by this standard across the industry will entail time and cost many millions of dollars. Implementation to a point of auditable compliance will likely take several years for many larger organizations, with significant generation or transmission systems. The timetable for passage of this standard has missed 2005 budget cycles,

		and the standard may not be finalized and passed before most entities can identify costs and budget for 2006. As such we believe that NERC has an obligation to perform a thorough impact analysis, with full participation from the industry, as a part of implementation plan development, and allow for a phased in implementation across multiple years. We support the need for these critical standards. But we don't support standards that neglect costs, complexity and reasonable timeframes for implementation.
Pedro Modia	Florida Power and Light	For GOP, the schedule is too aggressive. We recommend at least 12 months from the time the standard is approved to become "Significantly Compliant" and 24 months from the time the standard is approved to become "Auditably Compliant". This will allow time for a budget cycle and planning and implementation time.
Pete Henderson	Independent Electricity System Operator	Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in Q1 2006 for the following reasons: •NERC CIP 002 through CIP-009 establish much deeper and wider requirements than NERC 1200 and will require a significant compliance effort even from those already in ful compliance with NERC 1200. •No budgeting can typically be done until the standards are confirmed and solidified. •Most budgets are confirmed four or five months prior to the fiscal target year. Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little to no impact and should be acceptable in view of the development of this new and major standard. The implementation plan should recognize typical corporate fiscal planning processes. The Implementation Plan should be revised as follows: Change the year 2006 to 2007 in the first group of columns, and make corresponding changes to the year in subsequent columns by adding one year. In the first column, for control centers (in the year 2007 after having made the change noted previouly) change AC (auditably compliant) to SC (substantially compliant) in all instances. A good requirement would be to require that a corporate implementation plan for reaching auditable compliance be submitted by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis. Recommendation: Throughout these standards, a requirement is established to be able to provide up to three years of records for examination on request of an auditor. The wording of the standards or of the implementation plan should contemplate that entities may legitimately not have fully 3 years of records to submit until 3 years after they are required to come into Auditable Compliance. It may be suitable to require entities to identify the dates when the document retention processes will be deemed to begin as part of the implementation plan suggested above.

Name	Entity	Comments
Raymond A'Brial	Central Hudson Gas & Electric Corporation (CHGE)	CHGE feels the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date? If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?
Richard Engelbrecht	Rochester Gas and Electric	RGE concurs with NPCC that the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. There is concern with compliance for substations. Substations are part of the <<Other Facilities>>. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date? If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

Name	Entity	Comments
Richard Kafka	Pepco Holdings, Inc. - Affiliates	Thank you for providing an implementation plan. Our comments on the draft plan are dependent on the responses to our comments to the standards. It is therefore difficult at this time to offer comments on the timing.
Robert L. Sypult	Southern California Edison	st Quarter of 2006 is too tight of a timeline for "Auditably Compliant" requirements for Control Centers, as the Standards are not likely to be approved and issued until after 2006 budgets and training plans are developed in 2005. Control Centers should be classified as "Substantially Compliant" in 2006 and "Auditably Compliant" in 2007 and beyond.
Robert Strauss	New York State Electric & Gas Corporation	NYSEG concurs with NPCC that the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. There is concern with compliance for substations. Substations are part of the <<Other Facilities>>. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date? If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?
Roger Champagne	Hydro-Québec TransÉnergi	The Implementation Plan does not allow enough time for compliance. These standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. There is concern with compliance for substations. Substations are part of the <<Other Facilities>>. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Name	Entity	Comments
Roman Carter	Southern Company Generation	The implementation plan only addresses when entities should be "auditably compliant' but does not address the introduction of audits, sanctions, or penalties as previous implementation plans have addressed.
Steven L Townsend	Consumers Energy	The need to secure Control Centers has been recognized for some time and implementation has also been underway while the need for securing substations and plants is new. It will be extremely difficult and expensive to meet the 1st quarter 2007 due date for these standards for substations and plants. We would recommend that the "Auditably Compliment" target for substations and plants be set to a later time period (i.e. – 1st quarter 2008).
Terry Doern	Bonneville Power Administration, Department of Energy	Recommend extending general implementation date at least until 1st quarter 2007 for Control Centers' Balancing Authority. We can't comment on the implementation plan until we understand the scope of the requirements. For example due to size and scope of our system, an assessment could take upwards of a year. Completing the technical feasibility study and addressing budget issues related to implementation could take multiple years. In some cases like CIP006 Physical Security M4 Alarm System or CCTV, full compliance could take 20 years assuming 4-5 sites a year are improved to the standard at a cost of $100,000 or more per site.
Todd Thompson	SPP	The following is the position of the ISO/RTO Council Members: Since the standard will not become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance in Q1 2006. --NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort. --No budgeting can typically be done until the standards are confirmed and solidified. --Most budgets are confirmed four or five months prior to the fiscal target year. Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little impact and should be acceptable in view of the development of this new and major standard. The implementation plan should recognize typical corporate fiscal planning processes. Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis.

		Recommendation: The entity must identify the dates when the document retention processes must begin to be compliant with the standard.
Tom Pruitt	Duke Power Company	Clarification is needed whether the implementation plan is included in proposed ballot process. If not, how can we be assured plan will not be changed requiring more immediate compliance? --This has much broader impact that 1200. Other than delaying implementation of 2 years, we need to review scope and refine to take a smaller incremental step from 1200. --The implementation plan dates is too aggressive and not realistic.
Tony Eddleman	Nebraska Public Power District	The implementation schedule is too aggressive. Delay implementation at least one year or please consider an intial implementation of a much smaller scope to include control centers (CIP-002-1, R1.1.1 and R1.1.2), with full implementation over several years of other critical assets (CIP-002-1, R1.1.3 through R1.1.9).
William J. Smith	Allegheny Power	