Drafting Team responses to comments received during first posting of the NERC Cyber Security SAR December 1, 2003

Do you believe that this SAR is ready to be developed into a standard? – YES

Alan Boesch, NPPD, Segment 1	1. Some of the information in this SAR is too prescriptive and seems to be based on the language in the Urgent Action Standard. Lets start with a clean slate and get a standard that is supported by the segments of the industry that will implement the standard. Response: The drafting team feels that much was learned during the development of the urgent action standard and believes that it contains information that will be beneficial to the permanent standard. The industry segments will have opportunities to review the SAR and standard and any unacceptable portions will be identified during that process. Some of the ties to the urgent action standard (such as the list of justification items) have been removed in response to this and other comments. 2. In the "Brief Description" section, amend it to read "…implement appropriate and commercially available technical security improvements" Response: The change may be interpreted to imply that in-house solutions that are not compatible with commercial applications do not require compliance to the standard. For this reason, the drafting team cannot include this change. 3. Change the statement on the applicability of this standard to read as follows: "This standard will apply to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Operator, Generator, and Load Serving Entity and functions that are critical to the reliable operation of the Bulk electric system." The Scope of the SAR should not be expanded to include those entities that do not have an effect on the reliability of the bulk electric system. Response: The suggested changes do not appear to limit the applicability of the SAR, but rather expand it beyond the original SAR language. The functions identified in the SAR are those responsible for grid reliability in the functional model. For these reasons, the drafting team does not agree with this change. If the commenter intends to limit the SAR to include only those systems within the identified functions that are critical to reliable grid operation, the drafting team agrees and has modified the definition of critical cyber

	assets to address this. The intent of this SAR is to protect critical cyber assets necessary for bulk system reliability. 4. Definitions- All definitions should be included and reviewed as part of the standard development. The SAR form in the NERC Reliability Standards Process Manual states "Provide enough detail so that an independent entity familiar with the industry could draft a Standard based on this description." Providing definitions from the Urgent Action Standard are beyond the scope of a SAR. Response: In this and other SARs, NERC has included definitions for any terms that are fundamental to understanding the concepts included in the standard or to aid the standard drafting team in writing the standard. The standard drafting team is free to change any definitions included in the SAR or to add new ones during the drafting of the standard, provided this does not substantively change the scope provided in the SAR and is endorsed by industry commenters. 5. Some of the information in this SAR is too prescriptive and seems to be based on the language in the Urgent Action Standard. Lets start with a clean slate and get a standard that is supported by the segments of the industry that will implement the standard. Please resist the temptation to direct the standard drafting team down a path that would lead to the creation of a standard that looks just like the Urgent Action Standard. Response: Please see response to similar comment above. 6. This is a Reliability Standard and should focus on the reliable operation of the bulk electric system and should not include any other entities or systems that will not have an effect on reliability. Response: Please see response to similar comment above.
Alan Johnson Mirant Segment 6	Wondering whether the PSE function should be expected to conform to this standard. The PSE provides transaction data through E-Tag that the BA and RA may reference in making decisions regarding the operation of the bulk power system. As such, if this data is compromised, reliability could be impacted. Response: The PSE function is outside the scope of this NERC reliability standard. The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling.
Carter Edge, SEPA,	

Segments 4,5	
Dave Folk, FirstEnergy, Segment 1	The final SAR shall have sufficient detail of expectations to provide guidance to market members for developing a security procedure and policy that will meet the compliance tests. Response: The market function is outside the scope of this NERC reliability standard. The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling.
Dave Norton, Entergy, Segment 1	1. Quantification of Adequate "Quality Metrics" (All Sections) In general, we submit that each requirement in the standard must be examined against the question: "How good is good enough?" Examples: a. Infosec Policy: We do not believe a requirement to simply have cyber security "policy" as adequate to the challenge. One could have a policy "not to worry" about X, Y, Z. What is the metric for adequate policy? b. 24-Hour Physical Access Monitoring: Is someone's Granny and her toothless dog posted at the door adequate? What's the adequacy metric? Is un-manned motion detecting video monitoring /tape recording adequate? If not, what then? The time-honored rule of thumb for determining the answer to the question "How good is good enough" is to conduct a risk analysis, with the result coming in the form of dollars and cents in financial exposure to the organization. The executive leadership of any other commercial enterprise, in the absence of specific metrics imposed from the outside, is free to embrace as much or little risk as felt appropriate – it's a value judgment based in large part on the willingness of executive leadership to embrace risk. But a NERC imposed set of standards removes that latitude, and further, requires signature by a fiduciary officer stating that countermeasures are not just adequate from his or her perspective, but to the letter of the standard. There are many sources to draw upon, such as NIST, SANS, ASIS, etc., to aid us in being very specific in creating adequacy metrics. We believe the practical efficacy of the standard – whether it actually does what it's intended to do – will hinge significantly on the quality of the metrics contained therein. Response: These comments will be submitted to the standard drafting team for consideration when the standard is drafted. 2. Record Retention (All Sections)

	Response to pre-ballot UA SAR comments stated: "…much will be learned [during the effective period of the UA SAR] about record retention for the various types of information. Lessons learned will be used in the development of the final cyber security standard." How will those "lessons" be aggregated and consolidated? How will the permanent cyber security standard requirements and drafting teams proceed at the same time as – in parallel with – learning those lessons? Response: These comments will be submitted to the standard drafting team for consideration when the standard is drafted. 3. Functional Model (All Sections) a. Will we proceed in specifying the standard using the NERC "Functional Model" as the frame of reference, or continue along the lines of the UA SAR with control areas and reliability coordinators as the nexus? b. If the former, should the cyber standard requirements and drafting teams have on board NERC representatives or others who are intimately aware of the constructs of the model and the intent of it's creators? Response: The Functional Model is to be used as the foundation of all NERC reliability standards. 4. Operations and Markets (All Sections) NERC is operations reliability focused by charter, whereas market affairs are the aegis of NAESB. a. Does secure operation of cyber systems that execute/support market transactions fall under the aegis of NERC or NAESB? b. If the latter, will there be a separate cyber standards instrument promulgated by NAESB, and if so… c. How will inconsistencies be resolved, and who is the arbiter for conflict resolution? Response: The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling. The Joint Interface Committee will determine conflict resolution processes if such exist regarding the development of reliability standards and complementary

	business practice standards. 5. Compliance Enforcement (All Sections) a. How will consistency in breath and scope of compliance enforcement be reified across NERC Regions? b. How do we assure consistency in security measures at/across the interconnect points between organizations on both sides of a Regional border? c. Will each NERC Region individually, e.g., SERC, establish non-disclosure provisions incumbent upon assessment/audit teams, or should such an instrument be standardized across NERC? Response: These comments will be submitted to the standard drafting team for consideration when drafting the standard. 6. Critical Assets (1202) This whole matter is very imprecise in both the UA SAR and accordingly the draft permanent standard. And the pre-ballot response to comments on the UA SAR does little to clear it up. The initial thinking to arrange these matters around the NERC Functional Model, and then backing away, also has not made the requirements any simpler to interpret. If the litmus is "anything that materially affects the reliability of the bulk electric power system," double and triple safeguards notwithstanding, it would seem difficult to exclude generation. If PCS in generation are to be excluded, where is the line to be drawn – at the transformers or transmission-side buses in the switchyard? If not, what then? This matter needs to be unambiguously clarified if responsible entities are to be held to cyber security metrics and penalized accordingly for failure to comply. The following questions beg clear answers: a. Are fossil and hydro generation facilities to be included under the aegis of the permanent cyber security standard? Response: Yes, to the extent that the facilities or portions of the facilities meet the revised definition of critical cyber asset in the revised SAR.

	b. Will permanent cyber security standards compliance be incumbent on "downstream" organizations outside/beyond control area operator and reliability coordinator organizations? [We perceive the answer to be "yes."] c. Response: NERC's purview is reliability of the bulk electric grid. Downstream organizations and their systems are outside NERC's scope. However, a requirement that organizations who must comply with this standard identify and protect themselves from threats from interconnected cyber systems has been added to the SAR in response to this and other comments made during the development of the urgent action standard. d. How will assets owned and/or managed by organizations downstream of control area operators and reliability coordinators be determined to be "critical?" Who shall decide? What shall be the process for resolving conflict of opinion? [What are the legal ramifications?] Response: NERC's purview is reliability of the bulk electric grid. The identification of critical cyber assets not related to bulk electric system reliability, while important, is outside the scope of this standard. e. Are wholesale and retail markets trading systems operated by entities that own no infrastructure considered critical assets? Response: The drafting team will encourage NAESB to adopt comparable standards for market systems such as those listed in this comment. f. The DHS Information Analysis and Infrastructure Protection Directorate has briefed CIPAG that it is in process of – and will – "define critical assets." How shall we accommodate potential differences between the NERC CIPAG and DHS definitions? Response: This SAR deals with critical cyber assets, as opposed to critical *electric system* assets. The drafting team does not believe that any conflicts exist with DHS definitions. However, this issue will be forwarded to CIPAG for coordination with DHS. 7. <u>Inclusion of SCADA within the Standard</u> (1202) It is the contention of our national intelligence organizations that transmission infrastructure is a more attractive terrorist target than either distribution resources (not high enough impact), or those of generation (too "hard" a target, especially nuclear). All things being equal, we see this as probably being the case. We also support the conclusion that physical attacks are both simpler/easier to conduct than

	cyber assaults, and are therefore more likely. We further support the idea that physical security and cyber security must be mutually supportive, and that both types of security should be incorporated in complimentary fashion within the standard. At the same time, we recognize the literal impossibility of the industry being able to ubiquitously upgrade the cyber security of electronic controls now in use at any time in the near future. Universal upgrade or retrofit is impractical financially and logistically, even if appropriate SCADA/PCS cyber security technologies were now available for existing infrastructure – which they are not. If these contentions were true, it would also seem true that in the short run our capital resources should rightly be focused to sure up physical security at substations and switchyards. But we do not concur with the inclination on the part of some who seem to want to simply ignore cyber hardening of SCADA controls in the cyber standard development process, because it is too difficult logistically, too expensive, or because off the shelf solutions are not readily available right now. Some advocate that the entire issue should be relegated to consideration at some indeterminate date in the future through yet another cyber SAR process. We do not agree. While we do not argue for a moment that we should mandate the impossible for the near term in drafting the permanent standard, we do submit that the matter should be addressed with specificity in the standard – now – spelling out both technical requirements and a date for uniform compliance at some distant date in the future, say five-to-seven years out. The longer we wait to set these requirements, the longer we will protract the matter, and we're already two years away from a permanent standard at best as it is. If we include longer-range requirements now, we will put EMS/SCADA/IED product manufacturers on notice, and obviate the "chicken and the egg" phenomenon concerning product feature development (i.e., "When enough customers ask for it, we'll develop it."). Additionally, if we do so now, we will give management reasonable advanced notice and something tangible with which they can work, providing a better basis for constructing appropriate rate cases to support future operations. We contend that it is not difficult to define appropriate and specific techniques using existing technologies *available today* which will fulfill our needs for cyber hardening of SCADA gear (and PCS for that matter, too). We simply need the will to embrace it. The *National Strategy to Secure Cyberspace* calls out in black and white the urgent need for both authentication and encryption of SCADA/PCS infrastructure, so it would appear just a matter of time before this requirement is imposed upon us from on high. If we start now, we will most likely give ourselves more lead time to implement these measures than if we wait until it is legislated, which would probably come with a shorter implementation compliance timeline. If we do a good enough job we may even avoid such legislation altogether, or at least be able to substantially influence it's content and timetable. Response: To the extent that SCADA meets the new definition of critical cyber assets found in the revised SAR, it is included. The drafting team does not believe that current technology will support SCADA encryption and that encrypting the multitude of devices involved will take significant time. There may be alternatives to encryption, such as proper perimeter design and protection. The industry will be asked if

	SCADA/PCS encryption should be included in the scope of this standard and how long it will reasonably take to complete the effort. 8. Multi-Ported RTU (1202) Both operationally and legally, how will the matter of cyber security surrounding use of multi-ported RTU serving multiple organizations be handled? Conflict resolution? While this may not have been an issue in days past involving essentially "hardwired" serial communications lines, the issue will not be nearly as simple should the owner/primary operator convert that part of it's infrastructure to IP communications. Response: This appears to be a contractual issue, which is outside the scope of this standard. If the RTU meets the new definition of critical cyber assets found in the revised SAR, it is included in this standard, regardless of contractual ownership. 9. Citizenship Requirement for Personnel in Positions of Trust (1207) There are two components to this recommendation – one involving direct users of EMS control systems (e.g., dispatchers) along with system administrators of same, and the other concerning software vendor personnel involved in the development and maintenance of EMS and market host software systems. In short, we believe it should be mandated by fiat that only certifiable US citizens be allowed to work in these positions of trust. There is nothing discriminatory about this. It is critical national infrastructure at risk, and it is not unreasonable to require that only US citizens be allowed to operate and work on the internals of the computer and network systems used to safely operate it. Some of the direct participants in the 911 attacks were foreign nationals who had been working in the US for as much as two years and were still awaiting receipt of a Green Card at the time of the incident. We should take a "once bitten twice cautious" approach to the ability of the US Immigration and Naturalization Service (INS) to protect us. Second, just because one has a Green Card, it says nothing about allegiance to our nation. For that matter, neither does naturalization prove allegiance beyond a shadow of a doubt, nor does natural-born citizenship per se. But just because we cannot know what's going on in the back of the minds of either natural or naturalized citizens, this does not invalidate the logic of a minimalist safeguard in requiring citizenship for these positions of trust… Likewise, the news of late has been full of stories about the flood of high tech, particularly programmer, jobs being outsourced to offshore organizations. Given the paucity of competition in the EMS controls software sector and the prices charged for these products, the requirement that only true and naturalized citizens be allowed to work on these system does not in any way appear to make this requirement onerous, burdensome or anti-competitive. It's not a cutthroat market

	– there just isn't enough competition to support any vendor claim that this requirement unduly affects their ability to compete, especially when the requirement is imposed on all EMS software market participants equally. No vendor would be individually singled out for special treatment. Response: It does not appear reasonable or practical to require that all vendors with access to critical cyber assets be US citizens, nor is it within NERC's authority to require this. 10. Background Checks for Personnel in Positions of Trust (1207) We feel that somewhere between the routine commercial $25 felony background check and a tens-of-thousands-of-dollars FBI extended background investigation (EBI) is a correct balance in depth of investigation. The type of check that seeks to uncover "dirty little secrets" that could lead to blackmail exposure are probably a little much. But a fairly rudimentary check to see if an individual has serious financial problems and pending litigation is probably warranted. Attempted bribery is alive and well in the world of corporate espionage, to say nothing of political espionage. The Ames, Walker, and Hanson cases all had money motivation at their roots. We feel the standard drafting team should investigate and contemplate this recommendation earnestly. Perhaps a DOE "Secret" clearance is satisfactory (?). Response: The intent of the standard is to require that some sort of background checks be conducted, without specifying how to conduct the check due to differing federal, provincial, state, local and bargaining unit requirements. The drafting team believes that industry feedback during the development of the urgent action standard supports its contention. 11. Information Protection (1210) The draft standard states that each responsible entity "…shall protect information associated with critical cyber assets and the policies and practices used to keep them secure." It goes on saying, "The responsible entity shall maintain a document identifying the access limitations to sensitive information related to critical cyber assets. At minimum, this document must address access to procedures, critical asset inventories, maps, floor plans, equipment layouts and configurations." These statements certainly imply that the responsible party must first undertake a process to identify what information is sensitive, and second, create a methodology for controlling access to it. This means that there must be at least two gradations of sensitivity of data – sensitive and not sensitive – and opens the way to other questions and considerations:

	a. Are more degrees of sensitivity (than two) at work that need to be attended? b. Does this not imply "compartmentalization" of information, i.e., data classification and sensitivity labeling? c. If so, then does this not also mean that a formal method of controlling individual personnel access to said data relative to classification is required, e.g., "role based access control" to electronic data stores? If this tenet of the draft standard is to be put into play in the final standard, and we believe it should be, then the challenges of the times now require us to embrace established methods of data compartmentalization used by military and intelligence organizations, although not to the level of granularity they employ. We submit that, generally, there are four gradations of data sensitivity at work within our operating processes: a. CRITICAL: All information and systems infrastructure assets used for operational control of EMS/SCADA and related resources that are considered "Critical National Infrastructure," where malfunction, disruption, or other failure can adversely affect human life or public welfare; b. CONFIDENTIAL: Assets involving markets, trading partners, support vendors, and/or other applications where information is made available to or exchanged with external parties on a selective basis, synonymous with "extranet" operations. Examples of CONFIDENTIAL applications and information include that associated with RTO coordination, NERC Security Coordination, market operation, external ftp servers, and any other systems-based business functions that can be characterized as "electronic commerce"; c. PRIVATE: Internal-use-only information and systems infrastructure assets that are intended for use exclusively within the responsible entity, synonymous with "intranet" operations. Examples include applications and databases and/or data warehouses used by Senior Management, Legal, Human Resources, Finance, Engineering, and Marketing departments, etc., and certain other systems and databases as may come to be so designated in virtue of their containing extracts of CRITICAL and/or CONFIDENTIAL data sets;

d. UNCLASSIFIED: All other applications and information that do not clearly fit into any of the three previously defined classifications.

We propose that this model be adopted as a template for classifying and controlling access to sensitive information, as called out by the draft standard.

Response: These comments are more appropriately considered by the standard drafting team and will be forwarded to them.

12. Inconsistency in Specification – "Functional" versus "Technical" (1212)

The scope of the draft permanent standard is generally broad and non-proscriptive, leaving the means to assurance up to the individual organization, except in a few areas – particularly within the section on Systems Management (1212). We feel that the standard should not be selectively proscriptive, i.e., it should be uniformly cast either as "functional requirements" or "technical specifications." This contention is related to comments concerning "How good is good enough," as well as the need to clearly spell out what executives are supposed to self-certify as being compliant. Notable are the following examples:

a. The draft standard states a requirement for having anti-virus (AV) systems in operation. While the value of AV is not generally suspect, how good is good enough? Is AV required just for market facing host systems? EMS hosts? Email servers? Are email proxies and quarantine hosts necessary? Should email hosts be operated within the control systems LAN environment at all? All desktops, or just those used by dispatchers in control centers? Is one AV product adequate, or should two vendor products be used to better assure fail-safe?

b. The requirement for using intrusion detection systems (IDS) is in the draft standard, even though the efficacy and value of it is very much up for debate – some say the value is dubious at best. Again, is network-based IDS adequate, and if so, can it be implemented solely within a DMZ, or should it be implemented on internal LAN where control hosts operate? Both? In addition, or as an alternative, is host-based IDS required? Just for EMS control hosts? Market facing hosts? Other internal hosts with gateway (firewall) interfaces to controls networks? What about RTU? Other permutations? What is it we are asking our fiduciary officers to put their names on the line beneath?

c. Under "Systems Management" it is stated that entities "shall establish systems management

	policies and procedures for configuring and securing critical cyber assets," and continues with an incomplete laundry list of items – that is, if the intent is to be specifically proscriptive in the technical specification sense. The long established rule of thumb is that the scope of cyber security is "anything that affects the confidentiality, availability, and integrity" of systems. The list mentions nothing about file integrity checking capabilities (e.g., something like Tripwire), to assure data has not been intentionally or inadvertently compromised. This is but one example. Three things are recommended: a. Decide whether or not the standard will proscribe technical specifications, or be functional requirements based. If it is to be the former, then it should be more rigorous in identifying exactly what the detailed components of adequate cyber security are, for example, what "adequate" IDS and AV means. b. Separate into another section of the standard those elements of systems management that are specifically about routine care and feeding of systems to keep them operating reliably. These are just as much a part of security. c. In a different section address those elements of systems management that specifically attend to security management processes, procedures and tools. Response: These comments are more appropriately considered by the standard drafting team and will be forwarded to them. 13. Application and Data Base Security (1212, 1213) The pundits tell us that we can anticipate increasingly sophisticated cyber attacks on our systems in the coming years (see www.infosecuritymag.com November, 2002, "Infosec's Worst Nightmares", "Five Things that Keep Me Up at Night"). This article briefly overviews the potential uses of specific current underground tools to infiltrate and compromise systems using super worms, polymorphic code, anti-forensic tools, kernel-level root kits, covert channels, sniffing back doors, and Trojan Horses, among others. At the same time, it is not uncommon within our industry to experience a severe lag between the release of operating system level patches from OS vendors, and the ability to apply them by users to both EMS and market facing systems, because of the need for extensive regression testing of the patches to

	assure that same do not blow up the application code. And this says nothing about application programming level vulnerabilities onto themselves, and widespread use of known-to-be vulnerable CGI scripts (for example). This situation clearly needs to be improved, and the onus should be put on the purveyors of our EMS/market application platforms to rectify the situation. The NSA is worried about "zero-day" attack signatures (ones never seen in the wild until that moment), so we are walking on very thin ice. Can the new cyber standard be used as a vehicle to require – "legislate" – more timely attention to identified/known vulnerabilities at minimum, and further, require that application and data base code be tested and certified as free of recognized poor programming techniques? At a very minimum, we submit that web-based market facing systems should be held to some sort of litmus of this kind, perhaps using guidelines such as those made available by the Open Web Application Security Project (http://www.owasp.org/index). For EMS systems proper, is it not wise to require application vendors to attain certified Common Criteria compliance? Clearly, reliance on "the free play of market forces" is not getting the job done as necessary. Response: NERC standards cannot require vendors to respond to requests from their customers. The standard will require that critical cyber assets be identified and protected by those that own and/or operate them. It is not the intent of this standard to require that vendors be certified. 14. Baseline Forensics Capabilities (1214) a. Under "Electronic Incident Response Actions" the requirement to "…define electronic incident response actions, including roles and responsibilities assigned by individual or job function" is proffered. It goes on to stipulate a requirement to report incidents in accordance with NERC-NIPC IAWP Standard Operating Procedures. Might it be wise to define with some specificity adequate baseline computer forensic practices and procedures, or, would it be better to address those in a NERC Guideline? b. Incidents requiring forensic investigation can often involve two or more organizations, where, for example, email worms are inadvertently spread one to another. It would appear important for some kind of bi-lateral information sharing and confidentiality protection agreement to exist before the fact for ready utilization by affected organizations under rush conditions. Response: A number of forensics guidelines already exist for use by the industry. Reference to these guidelines will be suggested to the standard drafting team when they begin drafting the standard.

15. Tunneling for Use of the Internet, Frame Relay Networks, and POTS for EMS Access (1203, 1204, 1209, 1212)

Aside from the potentially adverse real-time performance and reliability experience in use of these types of public networks, we submit that remote access to EMS controls should, by fiat, only be allowed through use of VPN tunneling coupled with (strong) two-factor authentication. We do not see this as logically debatable.

Response: This comment is too specific for the SAR and is more appropriately handled by the standard drafting team when they begin drafting the standard.

16. Internet Use as Standard Operating Procedure for EMS-SCADA Communications (1212)

While attractive from an operating cost perspective, we believe that routine use of the Internet, as a communications vehicle for control operations, is penny wise and pound-foolish. A nefarious compromise of DNS or router code (BGP4, in particular) within the Internet backbone could seriously compromise the viability of this medium, leading to loss of real-time control of SCADA/IED in the field. While discovery of router code vulnerabilities is not frequent, it's not unheard of, as witnessed just within the past month. On the other hand, DNS has a long history of vulnerabilities, as well as the operating system platforms upon which it executes. IETF has expended significant ongoing effort to finalize a Secure DNS standard, but as yet this has not come to fruition. And even when it does, time will be needed for the standard to become real in the form of executables, and also to ferret-out unanticipated security shortcomings in the code. Until the day comes when we can be better assured of the unflinching reliability of these specific elements of Internet operation, we submit that use of the Internet for real-time EMS-SCADA controls should be forbidden.

Response: This comment is too specific for the SAR and is more appropriately handled by the standard drafting team.

17. Recovery Plans (1216)

This requirement of the draft standard says that responsible entities must "…create action plans and procedures to recover or re-establish critical cyber assets following a security incident… and exercise these plans at least annually." Does this statement mean?

a. Full business continuity plans/exercises?

	b. Full IT disaster recovery plans/exercises? c. Plans/exercises pertaining only to those elements deemed to be Critical? Response: The intent of the standard is to require a recovery plan for critical cyber assets, at a minimum.
James Sample – CAISO, Segment 2	Add to SAR: ---An Information Security Framework (e.g., ISO/IEC Standard, Common Criteria) that established a framework and methodology for the Electricity Industry. It should also be expanded to include application level security components (e.g., authentication and authorization methods, boundary checking components, input/output validation, etc.) Response: Common Criteria and ISO 17799 were among the frameworks used in the development of the urgent action standard. They will continue to be referenced in the development of this SAR. Access controls to critical SCADA communication devices and systems (e.g., process control systems, distributed control systems, electronic relays installed in generating stations, switching stations and substations); Response: The definition of critical cyber assets has been revised in response to this and other comments.
Terry Bilke, MISO, Segment 2	There is no "scope" section in the SAR. It appears the standard will solely deal with having a security program in place. This is appropriate. Note: The webcast posted on the Cyber SAR page discussed requirements that were not in the SAR. The process on how these things were added after the fact is unclear. The webcast says the process is managed by the Regions. Entities that participate in multiple Regions should not be subject to multiple reviews. It is expected that the standard would be based on current "norms" for the industry (which implies a survey of existing practices). Any new requirements should be justified on a thoughtful risk assessment that justifies the associated expenditures. Response: The SAR is the scope of the standard, yet to be developed. The standard presumably will include some of what is in the urgent action standard, but is not limited by it. The Regional compliance issue is common to all NERC standards and will be forwarded to the NERC compliance director. The drafting team

	agrees that the requirements of the standard must be technically attainable. For example, the use of SCADA/PCS encryption is desirable, but may not be reasonably achievable at this time. The industry will be asked for input in this area.
Terri Keuhneman, Salt River Project, Segment 1	
Rick Liljegren, Minnesota Power, Segment 1	
MAPP RRC; MAPP Operations Subcommittee Lloyd Linke, WAPA Allan Silk, Manitoba Hydro S2 Paul Brune, NPPD S2 Paul Koskela, Minnesota Power S2 Larry Larson, Otter Tail Power S2 Darrick Moe, WAPA, S2 Joe Knight, MAPPCOR, S2 Dick Pursley, Great River Energy, S2 Martin Trence, Xcel Energy S2 Todd Gosnell, Omaha Public Power District S2	There is widespread recognition that the National Institute of Standards (NIST) Cyber Security Guidelines are excellent tools for measuring, documenting, and improving the security of information systems. Compliance with these guidelines assures a high level of cyber security protections. NERC should review these standards, recognize them where they meet the need, and develop new standards only to fill any gaps when necessary. It would not be appropriate to force entities that are already required to comply with rigorous standards to be held to an additional set of standards developed by NERC for the same purpose. For example, all Federal utilities are subject by Federal mandates to already comply with the NIST Cyber Security guidelines. Response: The drafting team is collecting and reviewing all existing cyber security guidelines as the SAR is being developed. It must be recognized that US Federal guidelines may not apply to Canadian entities, however. It is also challenging to keep a NERC standard in synch with parallel standards over the long haul.
Linda Nappier, Ameren Segment 1	Add to SAR: How, if any, funds can be made available to help companies comply. There needs to be a waiver process developed so that companies can note that although they are not in compliance there is a reason why and a work-around plan. Retention of three years' history is probably overkill. Background checks of other company's employees is not reasonable. Although the contractual relationship can state this, there is very little a company can do to make sure that the vendor is truly following up on this.

	In general we agree with the general positions taken in the standard and feel that it is better for NERC to address these issues rather than to have additional legislation or regulation to control industry-specific concerns. Response: The implementation plan developed when the standard is drafted must take the current state of technology and the time needed to update existing systems into account. It is not within the scope of NERC standards to provide funds to achieve required performance levels. In general, those not in compliance with NERC standards will be asked to provide a mitigation plan that identifies how deficiencies will be corrected. The mitigation plan does not constitute a waiver to the standard. The data retention comment will be forwarded to the standard drafting team for their consideration when they write the standard. The drafting team agrees with the comment regarding vendor employee background checks, although there are ways (such as the right to audit background check files) to verify vendor checks.

Do you believe that this SAR is ready to be developed into a standard? – NO

Scott Weber – Allegheny Energy Segments 1, 3, 5	1. Delete or clarify all references to Market Functions, including references to the wholesale market software and systems contained in the first paragraph located under Item 6 on page SAR-4, to insure that Market Functions are not included in the cyber security standards. This may also impact which Reliability Functions this SAR applies to, as indicated by the checkboxes on page SAR-2. Response: The market function is outside the scope of this NERC reliability standard. The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling. 2. Revise the "Critical Cyber Assets" definition to read, "Those computers, including installed software and electronic data, and communications networks that process or control energy management functions, including bulk system security analysis and the initiation of generation and/or transmission control signals. This definition does not include process control systems, distributed control systems, RTUs (remote terminal units), or electronic relays installed in generating stations, switching stations, and substations." The intent is to remove ambiguity that might cause Market Functions and assets to be included in this SAR. Response: The critical cyber asset definition has been revised to add greater clarity in the revised SAR. Revise the "Cyber Security Incident" definition to read, "Any event or failure (that is of known malicious cause or where there is reason to suspect that the cause might be malicious) that disrupts the proper operation of a Critical Cyber Asset. Response: The incident definition has been revised to add greater clarity in the revised SAR.
Barry Lawson, NRECA, Segment 4	In the Detailed Description section, item 2, the SAR should specify that the frequency and severity of cyber attacks are increasing on elements of the bulk electric system if that is in fact the case. Otherwise, the statement in item 2 is not particularly relevant. Response: The drafting team agrees. The SAR has been revised and these items have been removed. They were in the original SAR as justification for the use of urgent action. In the first paragraph after item 6, first line, replace "a failure of one part of the generation" with "the failure of key/critical element(s) of the generation". In the second line, insert "potentially" between the

	words “can compromise”. In the second paragraph after item 6, third line, insert “substantially” between the words “should mitigate”. In the third paragraph after item 6, last line, replace “for cyber resources” with “for critical cyber assets”. Response: The comments above were considered when the referenced section of the SAR was reworded. In the Definitions section, the definition for “Cyber Security Incident” is unnecessarily broad due to the inclusion of the word “Any” at the beginning of the definition. The definition should be revised to read as follows: An incident involving or failure of a critical cyber asset that negatively affects the reliable operation of the bulk electric system. In the Related SARS section, should the Urgent Action Cyber Security SAR be referenced? Response: The definition of security incident has been revised to add greater clarity. The urgent action standard is now referenced as a related standard in the SAR.
David McCoy, Great Plains Energy, Segments 1,3 5 (14 GPE employees signed the comments)	A cost/benefit study should be performed along with a threat and vulnerabilities study. Vulnerabilities need to be prioritized and benefits of protection need to be compared with associated costs to prioritize cyber security compliance program elements. For example the cost/benefit of protecting large transmission transformers should be compared to some of these requirements to make certain that efforts are given the appropriate priority. The point is to be sure that standards related to physical electrical system security are pursued with appropriate intensity in parallel with the cyber security standards. Relative risks and benefits of mitigation and costs (between physical and cyber) must be kept in mind as standards are developed. Response: The drafting team agrees that each organization has a responsibility to conduct threat and vulnerabilities studies. The drafting team does not agree that development of this standard be suspended until all organizations have completed such analyses or that NERC should conduct an industry-wide threat and vulnerability study. This action would conflict with the industry consensus that lead to the emergency implementation of the urgent action cyber standard. The standards need to clearly address 3rd party owners of critical assets and 3rd party contractors. Response: Any entity that is performing the checked functions listed in the SAR is accountable to this standard. Third-party contractual arrangements are immaterial for compliance to this standard. a) Responsible entities should be given at least 2 years to attain compliance; 1 year is not feasible for

	most companies given the rigorous reporting and data maintenance requirements imposed. If a 2-year compliance plan is not acceptable, then perhaps NERC should require that compliance plans be filed and approved on a case-by-case basis. Those entities that demonstrate significant progress in 2004 and a commitment to complete their effort in 2005 should be deemed compliant. Response: An implementation plan will be developed and published when the standard is drafted. The plan must account for the current state of technology and reasonable timeframes to update existing systems. If the intent of this comment is to modify the implementation plan associated with the urgent action standard, that is outside of the scope of this SAR. b) Presumably, Urgent Action SAR 1200 will be the starting point for drafting the permanent standard. Accordingly, we offer the following comments that are based on the language in SAR 1200: i) 1201 needs to specifically list who the responsible entities are. It should clearly denote whether buyers and sellers of power and distribution providers are governed by this policy. Switching large blocks of load and capacitor banks could have a serious impact on system integrity, so this should at least be addressed, and if these entities are not included, the policy should state specific reasons for their exclusion. Response: Those entities performing the functions checked on the SAR form are accountable to this standard for the cyber assets they own or operate that meet the definition of critical cyber asset included in the revised SAR. ii) 1202 needs to list specific examples of critical assets. This standard should also clearly denote whether energy marketing, purchasing and sales systems, tagging, OASIS, scheduling and related operations should be defined as critical. Response: The definition of critical cyber asset has been revised to add greater clarity. iii) 1207 needs to be revised. More specifics are also needed on background checks. What is required? Should these include credit, criminal, DWI, etc and how far back should one search and how often should these checks be performed? iv) 1208 and 1209 should be revised to indicate that only “unknown and malicious” intrusions be logged and reported. These otherwise conflict with the NIPC guidelines. Response: The definition of security incident has been revised to add greater clarity. v) 1210 needs additional language giving responsible entities assurance that their audit and certification information will remain confidential. There also needs to be language clarifying that

	sensitive information can be maintained on company servers. 1212 needs to be clarified to indicate how patch management is to apply on vendor specific applications, which the vendors will not be motivated to modify. Response: The 1207, 1210, and 1212 comments above are too specific for the SAR and will be referred to the standard drafting team for consideration when they draft the standard.
Gerald Rheault, Manitoba Hydro, Segments 1,3,5,6	Manitoba Hydro believes that the scope of the "urgent Cyber Security Standard" which was recently developed and approved, is a good starting point to address cyber security. However the scope in the SAR, should be significantly expanded to ensure that the new Standard addresses the need to safeguard all the critical cyber assets that support bulk electric system operations. This Standard should only apply to cyber assets which could impact the reliability of the interconnected bulk electric system. Comments Manitoba Hydro believes that the scope of this SAR should be expanded to include the following: 1. elements such as process control systems, distributed control systems and electronic relays installed in generating stations, switching stations and substations where misoperation or failure of these elements can impact the reliability of the interconnected electric system. 2. vulnerabilities within the communications circuits associated with cyber assets, including loss of redundancy, hidden problems in leased circuits and common mode failures. Response: The drafting team agrees with these comments and has revised the definition of critical cyber assets accordingly. The SAR does not require redundancy. This standard is focused on the identification of critical cyber assets and their protection from malicious events. It is assumed that the availability of cyber assets and other equipment necessary for the reliable operation of the bulk electric system will be addressed in other standards. Communication systems between secure perimeters are outside the scope of this SAR (it is assumed that the perimeter will be protected from the connecting communication system). These are good comments and the industry will be asked for input in handling them. 3. application of a security criteria to reflect the impact of the cyber assets on operation of the interconnected electric transmission system. For example, the level of cyber security to be applied to an element should be predicated on the element's impact on operation of the bulk electric system; ie maximum security if failure of that element results in a major system disturbance and a lesser level of security if the failure results in a minor disturbance. Response: This approach would require that the degrees of impact be identified for each critical cyber asset and that a set of metrics for each be developed. Simply differentiating between 'major' and 'minor' impacts will be difficult. The SAR assumes that only cyber assets critical to bulk electric system reliability are

	addressed. 4. impacts common systems that are in widespread use. For example, a vulnerability in the design of a specific EMS system could have multiple, simultaneous impacts on the bulk system or on another cyber asset such as the state estimator system at an RTO. Such a failure could be seen as only an N-1 case (since contingency), for any specific entity, yet have very serious implications if applied in a large region. 5. clarification of the statement, in 4 above, that the cyber system should operate correctly for an N-1 case for a cyber asset (not a normal design criteria for such systems) and some development of this concept (the present wording introduces but does not expand on the concept). Response to items 4 &5: Even if the impacts are widespread, the source remains the specific EMS system and it is the responsibility of the owner of that system to correct/protect against security incidents. The following are Manitoba Hydro comments related to the documentation of the SAR: 1. The listing of critical cyber assets contained in the "Purpose/Industry Need" section is not complete. It should include other assets such as process control systems, distributed control systems and electronic relays as discussed in item 1 of No. 2 above. Response: The definition of critical cyber assets has been modified in response to this and other comments. 2. The "Brief Description" section of the SAR does not adequately reflect or summarize the elements addressed in the detailed description. It primarily lists the elements which are addressed in the Urgent cyber security standard. Response: The brief description has been revised in response to this and other comments. 3. The Reliability Functions applicability table, on page 2, should be modified so this SAR is applicable to the Transmission Owner and Distribution Provider functions. This change is partly predicated on the assumption that the scope of the SAR will be expanded to include process control systems, distributed control systems and electronic relays installed in generating stations, switching stations and substations. Communication systems and RTU's are likely to be under the responsibility of the Transmission Owner. Response: Applicability to the Transmission Owner has been added to the SAR. The distribution provider is outside of the scope of this SAR, as it deals with bulk electric system reliability. Those upstream of the

	distribution provider must properly protect themselves from any harm the distribution provider may cause. 4. The definition of "Critical Cyber Assets" in the definitions section of the SAR should be modified to include all elements which could impact the reliability of the bulk electric power system. It should also include all cyber assets as discussed in item 1 above. Response: The definition of critical cyber assets has been modified in response to this and other comments.
WECC EMSWG Erika Ferguson, Idaho Power S1 Jim Hiebert, CAISO, S2 James Sample CAISO, S2 Terry Doern BPA S1 Dave Ambrose, WAPA S1 Larry Shivers, Tri-State S1 Bruce Oliver SMUD S1 Israel Gonzalez IID S1 Chuck Nichols BCTC, S1 Bob Mathews, PG&E S1 Gary Nielson, TEP S1 Gray Wright, SPPC-NP S1 Randy Schimka, San Diego G&E, S1	1. Wide Area Networks (WAN) security and controls between control centers;\ Response: ICCP security requirements will be referenced in the SAR as something that the standard drafting team should consider when drafting the standard. 2. Access controls to critical SCADA communication devices and systems (e.g., process control systems, distributed control systems, electronic relays installed in generating stations, switching stations and substations); Response: The definition of critical cyber assets has been revised in response to this and other comments. 3. Protocols (e.g. peer-to-peer versus stack); Response: see response to item 2. 4. Need to expand on where, when, and what type of security technologies (e.g., firewalls, IDS, ACL's, etc.) should apply; 5. Needs more clarity around compliance and sanctions; Response to 4-5: These comments will be provided to the standard drafting team for their use when drafting the standard. 6. In the Definition section, need to eliminate the following from "Critical Cyber Assets": This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations. Response: See item 2.

	7. The SAR should provide more clarity around which systems are subject to standard (e.g. SCADA, OASIS, Tagging, Scheduling & Accounting, Merchant, etc.). There also needs to be clarification of what is a Load-Serving Entity. The effect of this standard should be to improve overall security of our systems, not to just create an oversight function. Response: See item 2. 8. In the SAR form, under Applicable Reliability Principles, item 6, the assumption is this is meant to address the training aspect included in the Cyber Security Standard 1211. Response: This item has been checked because it includes personnel responsible for operating the bulk electric system. 9. Cyber Security Incident definition needs to be changed from "malicious or otherwise" to just "malicious". The term "otherwise" seems too broad. Response: The definition has been revised in response to this and other comments.
Terry Doern, BPA, Segment 1	1. Add to the Definition of Critical Cyber Assets: "Other systems on the same network as Critical Cyber Assets must also meet the NERC CYBER Security standard." A system on a network is only as good as its weakest link. 2. In the Definition CYBER ASSETS, eliminate the exclusion "This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations." Response to 1-2: The definition of critical cyber assets has been revised in response to this and other comments. Any cyber assets within the electronic security perimeter must be equally protected and subject to the same incident response as critical cyber assets, as suggested. The SAR has been modified in an attempt to make this more clear. 3. Cyber Security Incident definition needs to be changed from "malicious or otherwise" to just "malicious". Response: The definition has been revised in response to this and other comments.

	4. The effect of this standard should be to improve overall security of our systems, not to just create an oversight function that just adds documentation work. Focusing on section 1212 Systems Management will help. Response: The drafting team agrees whole heartedly and believes the scope set forth in the SAR will meet the suggested objective. 5. The SAR should provide more clarity around which systems are subject to standard (e.g. SCADA, OASIS, Tagging, Energy Scheduling & Accounting, Merchant, etc.). Response: The definition of critical cyber assets has been revised in response to this and other comments. 6. Duplicate reporting should be minimized if possible. Accepting forms or combining forms with other from other cyber security oversight entities may help. Response: Requirements of other entities will be reviewed and incorporated, if possible. The drafting team agrees with the concept, but feels that reporting is outside the SAR scope. 7. Where there are conflicts in cyber security policy, government standards must take precedence for governmental entities. Response: Please see response to item 6. 8. Addressing accidental cyber security problems should be a secondary focus to malicious problems. Accidental cyber security problems are normally solved by improving procedures and not applicable to others. Response: The definition of security incident has been revised to add clarity. Known, accidental events are not included in the revised definition. 9. This SAR should allow entities to make a judgment on whether to add security enhancements based on cost and risk, compared to other power system risks. For example, rebuilding an overloaded line may be more important to power system reliability than resolving minor cyber incidents. Response: The SAR drafting team believes this conflicts with the overall intent of NERC standards, which is

	to develop rules that must be followed to maintain bulk electric system reliability. The rules must all be followed. 10. Marketing systems should be considered for inclusion since they could have a tremendous impact on the financial costs of electricity which will ultimately impact reliability. Response: The market function is outside the scope of this NERC reliability standard. The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling.
Albert DiCaprio, PJM, Segment 2	Overall Response to Mr. DiCaprio's comments: The purpose of the SAR is to define the scope of the cyber security standard. This draft SAR was accepted by the NERC SAC as the starting point for a standard dealing with cyber security, not data and communications reliability. Data and communications reliability questions have been posed to the industry in the comment form that accompanies the revised SAR. When drafted, the standard must include clear, measurable requirements, as generally suggested by the commenter. All of the comments below were considered and used as appropriate in further refining the SAR. 1. NERC Reliability Standards are defined in the *NERC Reliability Standards Process Manua*l (ver. 2.1) as follows: A Reliability Standard shall have the following characteristics: • **Material to Reliability** – A Reliability Standard shall be material to the reliability of the bulk electric systems of North America. If the reliability of the bulk electric systems could be compromised without a particular standard or by failure to comply with that standard, then the standard is material to reliability. • **Measurable** – A Reliability Standard shall establish technical or performance requirements that can be practically measured. This proposed SAR is the basis for a great Reference Guide, but this reviewer questions whether the proposed SAR rises to the level of a NERC Reliability Standard as defined above. The term *guideline* should not be considered as a dismissive word. Guidelines are important and valuable; they just may not be things that can be measured or quantified in the absolute terms of performance and compliance. NERC's new Reliability Process is not directed to the level of compliance of the old Policies and Standards. New Standards are expected to be backed by the 'rule of law' as well as significant financial penalties. As

	such, the Industry should not apply the term casually. Cyber Security IS important. Without data and communications the power system would not work. But can security be quantified and measured? If the proposed standard were to require that all control rooms have a 'security level' that ensured that no data be lost with a probability of one data item per hour per fortnight – that would be a standard. But a standard to "reduce risk" from "any compromise" is not a standard. Reduction requires a baseline. How that baseline is defined, is what a standard should address. Quantifying the relative effects of 'compromises' is what a standard should address. While the Industry can agree to any guideline and decide to call it a standard, the industry should be careful in not opening a door that would degrade the quality of the standards it is now creating. This standard may unintentionally lower the threshold for what a NERC Reliability Standard should be. **2. PURPOSE Statement** A NERC Reliability Standard deals with: • Technically supported measures • Measures of Performance • Bulk Power System The stated **PURPOSE** is to "…reduce the *risks* to the reliability of the bulk electric systems from *any* compromise of critical cyber assets …. that *support* those systems." Had the PURPOSE been to *define* the level of acceptable risk then that could be a legitimate NERC Standard objective. Had the PURPOSE limited its scope to *a defined level of performance* (as opposed to *any* compromise) then that could be a legitimate NERC Standard objective. As written the PURPOSE statement uses terms such as '*reduce'* (reduce from what?) and '*any compromise'* (even a monitor outage is 'a' compromise). Indeed the PURPOSE references any asset that '*supports*' reliability systems (that's broad enough to include the mailman!).

	The first comment is that the PURPOSE statement, as written, is well outside the aegis of the NERC Standard process. Even accounting for the fact that a SAR PURPOSE statement is intended to be at a high level, this scope should be reviewed. There are several options recommended for the requestor: • *As written this SAR should be returned and submitted as a scope for a NERC Reference Manual.* • *Submit the proposal as comments to the Reliability Authority Certification Standard* • *Rewrite the PURPOSE to more focus on NERC's sphere of influence, for example:* *To ensure an acceptable level of data and communications reliability.* The above example focuses the objective on **acceptable** data and communications **quality** and would in turn require the industry to define the level of acceptability. {It is not the security that is the problem; it is the resultant impact on carrying out the reliability responsibilities that NERC is concerned with.} **3. <u>Brief Description Comments</u>** The BRIEF DESCRIPTION states: "…requires that critical cyber assets …be identified and protected. *Requirements* will include: • Identification of *responsible* people • Procedures to *thoroughly* assess cyber security • Implement *appropriate improvements* *NERC's Standard Process is to develop measurable standards that deal with reliability.* *What kind of standard is "Identifying responsible people? That is a great guideline but having a name or job title written on a piece of paper is hardly a performance standard. Does identifying as person 'reduce the risk of compromise? Should the Industry reduce its standards process to have a name on a piece of paper? This may be a great idea but it is hardly worthy of what NERC standards were designed for.* *Performing an assessment is also a good practice. It does help in finding long-standing problems, but doing periodic assessments is hardly a protection against cyber 'attacks'. Of course the word periodic is never mentioned in the Brief Description, but this reviewer does not believe that the requestor envisioned continuous assessments (or did he?) This standard seems to be regressing to the old NERC Policies and Standards that defined good practices. The current set of SARs has (appropriately) avoided defining*

	'procedures'. Procedures are not standards. Procedures often become outdated without notice. And to those who say, "NERC will update the procedure when needed", they are reminded that NERC is seeking Regulatory and financial penalties for these new Reliability standards. You will be punished for any non-compliance until the Standard is changed. *Implement 'appropriate improvements' is definitely outside the concepts of NERC standards. Leaving out the obvious question of How would one define a measure of 'appropriateness'; improvement standards beg the question of improvement from what base? A Reliability standard should be defining the base level of data security and running away from words like 'improvements'. Consider this: Some entity that has no procedures can dramatically 'improve' whereas the entity that has the best of all security systems may not be able to 'improve' at all.* *If the PURPOSE is to 'reduce risks' then the BRIEF DESCRIPTION should have some statements about defining 'levels of risks' or at least some risk reducing suggestions. Identifying people, implementing changes serves as temporary 'adjustments' but they do not serve the industry's needs to protect itself against cyber attacks.* *The BRIEF DESCRIPTION does not address the concepts in the PURPOSE statement (or maybe the PURPOSE statement does not articulate the scope that is in the BRIEF DESCRIPTION. Either way the two should be coordinated.* **4. <u>Detailed Description Comments</u>** *The DETAILED DESCRIPTION should also be tied into the PURPOSE and the BRIEF DESCRIPTION. Unfortunately that does not occur in this draft SAR. The first half of the DETAILED DESCRIPTION provides a weak justification for the SAR. Incidents and frequency or severity are 'relative' terms. They are relative to the base line (1822, 2001, June 2003?) they are relative to the sophistication of measurements (hearsay, occurrences for each control area?) The justification interestingly says the SAR is based on Guidelines. Starting from guidelines and raising the bar to a standard would be a good thing – to stay at the level of a Guideline makes this "draft SAR "a draft GUIDELINE".* *This standard is proposed to:* • *Make entities understand role of cyber security* • *Identify critical assets*

	• *Have a program. A program that will include:*
	  o *Governance*
	  o *Incident response*
	  o *Business continuity*
	• *"FOCUS" on*
	  o *hardware*
	  o *software*
	  o *data*
	  o *communications*
	  o *control systems*
	  o *personnel*
	(Thank goodness the SAR is limited to just a handful of small items!)
	• *Define Terms*
	
	The above items are all good ideas, but they are hardly measurable. How is 'understanding' a Standard? Why is a 'list' (of critical assets) a standard? A standard that mandates Business continuity is a NERC goal. But focusing on 'everything' is hardly a reasonable objective.
	
	The requestor should be asked to reconsider this SAR in light of what the NERC standards are supposed to cover. And just as importantly to reconsider this in light of what the current SARs already cover. The current SARs require RA to get data and do reliability analysis that will ensure that the bulk power system stays up (as defined in terms of frequency or voltages or other such measures) To do these analyses they will need good data – that is covered by the requirement to do the analyses. Hardware and software are options for the entities to carry out their responsibilities – if these 'assets are compromised the entities will fail the compliance to analysis standards and be punished there. There should not be redundant punishments. NERC must focus on outcomes and not on processes. This standard while well meaning and even a good idea as a Reference – it does not rise to the level of NERC standard – at least as is it proposed in this draft.
	
	Following Procedures should not be a NERC Reliability Standard objective. Measures can be established to identify if a given procedure were followed but that is not what was envisioned in the NERC Reliability Standards Process.

Joe Willson, PJM, Segment 2	1. The proposed Scope seems to have already pre-disposed the specifics of this Standard as being only those elements already included in the urgent action cyber security standard. In doing so the requestor has really defined this SAR work as the development, not of a Standard, but as the creation of a needed

	reference manual on cyber security. This is a task needed by the industry, but does not come up to the level of a NERC Reliability Standard. The sixteen areas in the urgent action standard require an entity to develop documentation but do not require the entity to meet any real compliance measurements. If the requestor wishes to develop any of these areas into reliability standards I'd suggest the SAR focus on compliance measurements based on observations against an acceptable risk levels, and not on having a document in place. Response: The drafting team agrees that simply having a document available is not enough to demonstrate full compliance. The document must also contain core items, be disseminated to affected personnel, be understood and periodically updated. When the standard is written, it will require all of these items. 2. The SAR needs to include specific elements that can be measured (and are meaningful) for cyber security. The detailed description section infers that the proposed standard will ensure system reliability without defining that this will be done within an agreed upon risk level. The electric system is operated today to withstand only a defined risk criteria, the same approach needs to be clear with this work. The standard will also need to define what constitutes the critical cyber assets. The term "mitigate" needs to be better defined in the SAR. Response: The definition of critical cyber assets has been revised in response to this and other comments. The other points made are more appropriately shared with the standard drafting team and will be forwarded to them. The Purpose statement contains the phrase "to reduce risks to the reliability . . " but the SAR doesn't provide any insight as to what it is reduce from or to? The statement indicates that risk will be defined but the detailed description section, elements 4, 5, and 6, all refer back to the development of documentation. The Purpose may need to be revised to state "to define the minimum risk levels for cyber security assets that support the Interconnected Bulk Electric Power System". Response: The intent of the SAR is not to define acceptable levels of risk to cyber security assets, but rather to ensure that critical cyber assets are identified and protected from malicious events. There is likely not a universally acceptable minimum risk level for such assets. 3. Market security issues may be important issues but should not be included in this reliability standard. If

	the concern is that the real time monitoring and security systems may be impacted by data, then the Coordinate Operations and Coordinate Interchange SARs and their respective standards need to address these areas. Response: The market function is outside the scope of this NERC reliability standard. The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling. 4. The standard will need to define measurements which can be publicly released. Items such as an entities' processes, procedures, critical assets, and response actions to an attack will probably not be made public. Response: This comment will be forwarded to the standard drafting team for their consideration when drafting the standard. A NERC reference document suggesting what could be included in an entity's cyber security program is what this SAR is about. Procedures must not be considered standards. No one should be evaluated on how a procedure was implemented but should be evaluated on the end results. Entities should be permitted to use any and all appropriate procedures. NERC standards should be based on the "what" and not on the "How". Response: The drafting team believes that these comments are based upon a review of the urgent action cyber security standard. Please bear in mind that this SAR will set the scope for a permanent replacement standard. The urgent action standard was developed only to establish a minimum threshold for cyber security.
Mark Kuras, MAAC, Segment 2	1. I know some detail is in the referenced documents but further work needs to be done to refine exactly what is covered by the SAR. Response: The SAR has been revised to add more detail, in response to this and other comments. 2. During the balloting of the Urgent Action Standard, a multitude of comments were received as is noted in the SAR. These comments were never incorporated in the Urgent Action Standard that was approved. These comments should be specifically mentioned as being considered during Standard drafting.

	Response: The comments submitted during the development of the urgent action standard were reviewed by the SAR team and will also be reviewed by the standard drafting team. 3. Noting the interdependence of electric markets and transaction should be eliminated. Focus should only be given to reliability. Response: The interdependence cannot be denied. The standard will focus only on the reliability aspects, though, and NAESB will be asked to consider the market aspects. 4. The term and definition of a Cyber Security Incident encompasses too many events. Normal operations would inundate a Cyber Security report with superfluous information and possibly hide useful data. I recommend that this definition be used for a Cyber Event. A Cyber Event would then be investigated to determine if it was a Cyber Security Incident. This relationship is similar to the investigation of system protection "operations" and after an investigation, determination of a "misoperation" or normal intended operation. A misoperation would then be further investigated and reported on. Response: The definition has been revised in response to this and other comments. I believe that it is important to the Compliance Program that any Cyber Security documentation created or Cyber Security information gathered is independently auditable. I am not implying that it be gathered by a region or NERC but it should be viewable by an auditor either on-site or by other secure means. I can foresee some organizations being so concerned about reveling these documents or data that a Region could never verify if an organization has implemented their program. Response: This comment will be shared with the standard drafting team, as it is too specific for the SAR.
John Horakh, MAAC, Segment 2	a. Change the Purpose/Industry Need to the following: To manage, to below an acceptable level, the risks to the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems. We don't know if cyber security risks need to be reduced, but they do need to be managed to below an acceptable risk level. Response: The intent of the SAR is not to define acceptable levels of risk to cyber security assets, but rather to ensure that critical cyber assets are identified and protected from malicious events. An acceptable level of

	risk may be very difficult to quantify. b. Change the second sentence in the Brief Description to the following: Requirements will be included in the standard for the responsible entities to have and implement minimum level cyber security programs and procedures, perform a thorough assessment of cyber security, and implement appropriate and technically feasible security improvements if needed. It is the entities performing the reliability functions (e.g. the Balancing Authority) that need to have the programs and procedures, not the individual persons. Improvements do not need to be made unless they are needed. Response: The brief description has been revised to reference entities, instead of individuals. c. Make the following changes under Detailed Description: Move the last sentence in this section to become the first sentence in this section. The sentence reads "This standard provides definition of terms and the minimum requirements to implement and maintain a cyber security program to protect cyber assets critical to reliable electric system operation." This sentence describes the heart of what the standard should do, and should be in a more prominent place. The specification of minimum requirements in the standard is essential. Response: Agreed. The change has been made. Change the first sentence of the second paragraph to the following: This standard requires that responsible entities …. have identified their critical cyber assets related to bulk electric system operations, and have a minimum level security program in place, with the program implemented. The responsible entities' understanding of the role of cyber security in not directly measurable, but if they have identified their critical assets, and have in place and implemented a minimum level security system, that is proof of understanding. Response: This comment has been used to revise the referenced sentence. Change the first sentence of the third paragraph by deleting "and personnel" at the end. Although personnel operate the electronic systems, they should not be a primary focus of this standard. Response: Personnel must be included due to the tie-in to background checks and training.

John Maguire, PJM, Segment 2	1. Perhaps the sixteen items that will be addressed in the standard should be included, so that there is an understanding of "what" will be addressed. That does, however, limit the permanent standard from being dynamic and corresponding to the exact needs of the industry at an arbitrary point in time. Response: The SAR has been modified to state that the urgent action standard be used as a starting point for the drafting of the permanent standard in response to this comment. 2. First, the standard should apply only to the RTO-based functions (the Balancing, Interchange, and Reliability Authorities), because the reliability of the system will continue so long as these key functions continue. Conversely, the absence of any of the other functions, while important to sustain business activities and the operation of the market, will not harm reliability unless the losses are multiple, simultaneous, and continuous. The system is built and operated to ride through other losses of operational elements, generators, and markets. Therefore, while the inclusion of other functions will facilitate reliability, they are not necessary to preserve basic overall system reliability. This approach is appropriate with regard to the concerns NERC has as a compliance monitor, but is certainly the case for the near-term permanent standard. Any expansion of the standard to cover additional entities should be accomplished at the next iteration, if at all. Response: Based upon the comments received on the SAR, the drafting team does not believe that the industry agrees that only the BA, IA and RA need comply with this standard. Second, with regard to the "Brief Description" the statement "…[implementing] appropriate and technically feasible security improvements" is an unclear statement. What does it mean to be "technically feasible", and who will decide what requirements are "technically feasible"? With regard to "improvements" it is unclear how a standard will implement "improvements". It is reasonable to believe that moving from non-compliance to compliance with the standard is an improvement in state, but the standard should not define improvements. If there is a need for improvement beyond compliance with the standard, then the standard should be revised to "raise the bar". Response: The phrase 'technically feasible' was included in recognition that it may not be technically possible (now) to secure all critical cyber assets. Since this is the SAR, not the standard, this phrase will be left in and will be addressed further when the standard is written. Clarity regarding improvements has been added to the brief description.

	Third, the six items listed in the introductory portion of the detailed description are unsubstantiated and could be viewed as incendiary. It is not necessary to instill a sort of panic in order to motivate the creation of the standard. Simply referencing the FERC SMD NOPR, which included Section M and Appendix G regarding Cyber Security, and that FERC approached NERC to create their own industry specific standard should be sufficient. That along with the "National Strategy to Secure Cyberspace", which identifies the electricity industry specifically, should be enough to justify the need, and convince the board to authorize the development of the standard. Response: The referenced items were a carry over from the justification used to request the development of the urgent action standard. These items have been removed from the revised SAR, in response to this and other comments. Fourth, the rest of the description should be stricken from the SAR. The more information that is added to the detailed description, the more limiting the standard will become. Definitions should be removed, and placed into a glossary reference/appendix to the standard. All other detail is either redundant, supplemental, or superfluous, but not vital to setting the scope of the standard. A suggestion is to include the sixteen items that will be addressed in the standard so that there is an understanding of "what" will be addressed. That does, however, limit the permanent standard from being dynamic and corresponding to the exact needs of the industry at an arbitrary point in time. Response: A reference to the urgent action standard (the '16 items') was added to the detailed description, because much was learned in the drafting of that standard that will be useful in developing the permanent version. The drafting team is modifying some portions of the detailed description, but does not think it is prudent to minimize the amount of guidance this section provides to the standard drafting team. 3. In general, the Standard lacks a sense of urgency due to the lack of precise, deliberate, and measurable performance metrics. In order for the standard to motivate change in the industry each compliance requirement should be discrete. That is, each item within the standard must be written in such a way that the interpretation of the standard is consistent across the entities required to comply, and to assure understanding of the exact compliance/non-compliance threshold. An industry standard without consistent interpretation, consistent implementation, and consistent measurement is not a very convincing "standard". Response: Metrics are necessary and required by the NERC standards development process, but are a component developed in the standard drafting phase, as opposed to the SAR phase.

Robert Mullen, Con Edison, Segments 1,3,4,5	1. Title of Proposed Standard: *Change to* Security of Critical Cyber Assets – Bulk Electric Systems *This change better reflects the intended scope of the standard.* Response: NERC standards only apply to the reliability of the bulk electric systems of North America. The title was not changed because it implies that only bulk system critical cyber assets, as opposed to those that can *adversely affect* the bulk system are included. 2. Brief Description: *Change sentence stating with* "Requirements will be …" to "Requirements will be included in the standard to identify the responsible person(s), create and implement the elements of a cyber security program to continuously secure these assets." *The standards will define the elements of the security program according to cyber security practices.* Response: The drafting team believes that the original version adds more clarity. 3. Detailed Description: *In the paragraph starting with* : "The standard requires that responsible entities…", *in the sentence starting* with "A basic cyber security program…", *replace* "and business continuity" *with* "and recovery of these critical cyber assets or continuity of operations related to these assets." *"Business continuity" is a term which can extend the scope beyond that intended for the standard.* Response: Business continuity has been replaced by operations continuity in response to this comment. 4. Detailed Description: *In the paragraph and sentence starting with* "This cyber security standard shall primarily…", *replace* "as they impact electric system operations…" *with* "as they impact bulk electric system operations…". *In the same paragraph, in the sentence starting with* "In addition…", *replace* "cyber resources" *with* "critical cyber assets and their operation." *These changes clarify the scope of the standard.* Response: The suggested changes have been made in the SAR. 5. Detailed Description: *In the paragraph starting* "This standard provides definition…", *replace* "reliable electric system operations." *with* "reliable operation of bulk electric systems." *This clarifies the scope of the standard* Response: The suggested changes have been made in the SAR. 6. Definitions: *These should be moved to the standard itself.* Response: Definitions are not a formal part of a NERC standard and will be housed in a separate glossary.

	As standards are written, defined terms are attached for reference. *Note on Critical Cyber Assets: The definition should clarify that the definition* "does not include systems that support or interact with market operations unless such systems otherwise interact with bulk electric system operations." Response: The definition of critical cyber assets has been reworded in the revised SAR. Please see if this addresses your concern.
Richard Kafka, Potomac Electric Power Co, Segment 3	The SAR states that it applies to LSEs. Many LSEs interface with the system only through internet based applications maintained by the RTO/Market Operator. Any impact of local cyber breaches would primarily affect the LSE financially, and the Market Operator would need to meet cyber security objectives for the entire market. LSEs should either be eliminated from this standard or be specially addressed regarding cyber security issues affecting reliability. Response: The standard will apply to whoever performs the LSE function, only to the extent that they have critical cyber assets as defined.
Mitchell Needham, TVA Segment 1 Gary L. Jackson & Thomas McGrath, TVA Segment 6	During discussion sessions concerning the Urgent standard, there were comments stating certain 'understood' exclusions, including Nuclear Power Generation facilities. The reasons as discussed were that these entities fall under another federal regulatory agency (NRC), believed to have more strict requirements. As was commented by TVA and others, other utility industry entities are likewise subject to requirements issued by federal agencies (e.g. DOE, OMB, NIST, NRC) based on legislation. The scope of the SAR should clarify this in a manner similar to NRC issued requirements. Care should be exercised in understanding the impacts of multiple cyber security standards on non-jurisdictional entities to avoid the need to comply with multiple, possibly conflicting standards. Response: The drafting team is collecting and reviewing all existing cyber security guidelines as the SAR is being developed. It must be recognized that US Federal guidelines may not apply to Canadian entities, however. It is also challenging to keep a NERC standard in synch with parallel standards over the long haul. The drafting team agrees that the NRC will have jurisdiction over nuclear plants in the US. Numerous comments on the Urgent standard were submitted regarding the need to clarify the definition/scope of 'critical cyber assets' and the definition of 'cyber security incidents', but the SAR does not address this. TVA believes this would be a valid inclusion in the SAR (rather than awaiting the first draft of the new standard) in order to allow industry attention and appropriate comment. Clear definitions as suggested would help to define the functions to which the standard applies. The definition could be written so that certain criteria would be used to define assets as critical. This would allow flexibility so that as the technology changes that the new systems could be properly defined in or out of

	scope. Response: The definition has been revised to add more clarity in response to this and other comments. Perhaps this is not the correct block for this comment. The SAR should be revised to contain a statement that a basis for the standard will be the industry comments submitted on the Urgent standard. This will eliminate the need for entities to make identical comments at this time. The SAR does note that the work done previously on the urgent action standard would be the basis for the new standard, but resolution of those comments is not specifically mentioned. Response: A reference to the urgent action standard has been included in the detailed description portion of the SAR.
FRCC OC/EC/MIC----- Linda Campbell, Patti Metro FRCC, S2 Paul Elwing, Richard Gilbert Lakeland Electric S3 Amy Long, Lakeland Electric, S1 Paul McClay, Tampa Electric Co, S1 Marty Mennes, Joel DeGranda, Don McInnis, Pedro Modia, FP&L, S1 Ronnie Hunnicutt, Roger Westphal, Gainesville Regional Utilities, S5 Tom Calabro, Orlando Utilities Commission, S3 Joe Roos, Ocala Electric Utility, S3 Steve McElhaney, FMPA, S3	1. The scope should clarify for the industry the applicability of the standard. This applicability must be clearly defined to include only cyber assets that affect bulk electric system reliability. In addition, since the scope of this SAR is unchanged from the Urgent Action Cyber Security SAR, please refer to the comments provided by FRCC for the originally posted SAR and Standard. The purpose statement of the SAR is extremely important. It clearly explains the intent of the proposed standard. The verbiage "from any compromise of critical cyber assets" could include non-malicious production glitches that broaden the scope of the standard to not only the reliability of the overall system, but also the reliability of each cyber asset. A possible alternate purpose is: To reduce risks to the reliability of the bulk electric systems from intentional and/or malicious acts that significantly compromise the reliability of the system. Response: The definition of critical cyber assets has been revised, to add greater clarity. The definition of cyber security incident has also been modified to add clarity, in response to this and other comments. 2. The definitions for the following remain unchanged from the Urgent Action Standard and therefore still require additional clarification: Cyber Security Incident: The words "any" and "otherwise" lead to broad interpretations. In addition, the term "failure" must be clearly defined to prevent the unnecessary reporting of non-malicious activities such as: software testing or hardware failure. A possible alternate definition is: An event of unknown origin or a significant failure that disrupts the proper operation of a critical cyber asset, causing the reliability of the bulk electric system to be adversely affected. Response: The definition of cyber security incident has been modified to add clarity.

Robert Miller, Greg Woessner, Kissimmee Utility Authority, S3 Bob Remley, Clay Electric Coop, S4 Steve Wallace, Seminole Electric Coop, S4 Fred Krebs, Calpine, S6 John Giddens, Reedy Creek Improvement District, S3 Eric Grant, Progress Energy- Florida, S1 Garry Baker, JEA, S1 Ron Donahey, Beth Young, Tampa Electric Co, S3 Jose Quintas, Tampa Electric Co, S5 Rusty Foster, City of Tallahassee, S3	
Laurant Webber, WAPA, Segments 1, 9	The scope of the NERC Cyber Security SAR should include the evaluation of other cyber security standards, such as NIST guidelines, for adoption by NERC or for consideration as equivalent to NERC cyber security standards. Response: The drafting team is collecting and reviewing all existing cyber security guidelines as the SAR is being developed. It must be recognized that US Federal guidelines may not apply to Canadian entities, however. It is also challenging to keep a NERC standard in synch with parallel standards over the long haul. National Institute of Standards (NIST) Cyber Security Guidelines are excellent tools for measuring, documenting, and improving the security of information systems. Compliance with NIST guidelines assures the quality of Federal cyber security protections. It is appropriate to equate compliance with NIST cyber security guidelines and compliance with NERC cyber security standards. Western Area Power Administration (WAPA) suggests that the scope of the NERC Cyber Security SAR include the evaluation of

	other cyber security standards, such as the NIST guidelines, for adoption by NERC or for consideration as equivalent to NERC cyber security standards. The final NERC cyber security standard should include language such as this: "The Federal Information Security Management Act of 2002 (FISMA) and the Information Technology (IT) Management Reform Act of 1996 (i.e., ITMRA or the Clinger-Cohen Act) both require all Federal Computer Systems to comply with NIST Cyber Security Guidelines. "All Federal utilities, which are subject to Federal Cyber Security mandates formulated in NIST Cyber Security publications, shall fulfill the requirements of this NERC standard by self-certification that they are subject to such Federal mandates."
Larry Bugh, ECAR, Segment 2	The scope should be expanded to include the use of PKI through eMARC for securing applications. At a minimum, the applications to be secured with eMARC should include; ETAG, IDC, ICCP, CIPIS, and the Spare Equipment Database. Response: PKI is an implementation as opposed to a requirement to protect critical cyber assets. The NERC standards try to avoid requiring the use of a single protocol, application, or method for obtaining the desired outcome where possible. The use of PKI would certainly be permitted by the standard, but not required.
Kathleen Goodman, ISO-NE, Segment 2	1. ISO-NE suggests the title of the SAR be changed to **"Protection of Critical Cyber Assets".** The original title could apply to protection of all Cyber assets even non critical ones such as websites, payroll, billing, etc. Response: The drafting team feels the title is accurate. The SAR and its associated definitions have been clarified in terms of which cyber assets are critical to bulk electric system reliability and therefore included in the SAR. 2. In the "Description" we suggest changing the second sentence to the following; *Requirements will be included in the standard to identify the responsible person(s), create and implement Security programs, perform a thorough assessment of cyber security, and implement appropriate and technically feasible security improvements.* And add the following new sentence to the end of the "Description"; *Security programs include the organization's policies, standards, procedures, training and auditing controls for the implementation of the NERC Protection of Critical Cyber Assets.*

	Response: The brief description has been modified in response to this and other comments. 3. In the "Standard will apply to …" Section wISO-NE e suggests; **Check the Transmission Owner box on the SAR**. The TO's in many cases own the cyber critical assets in an area, or portions therof, and, due to future compliance concerns, we believe it is appropriate to place the responsibility with adherance to the standard on the entity that actually owns the equipment. Response: The transmission owner *function* has been checked. **Check the Planning Authority box on the SAR**. ISO-NE believes that, although the Planning Function has not been finalized in the NERC Functional Model, the information and systems utilized in the planning area could be of a confidential nature and contain sensitve information that could represent a security issue. Response: The intent of this standard is to protect critical cyber assets. Planning information can be used to compromise the physical electric system, but planning information is not a critical cyber asset as defined in the SAR. For this reason, the PA box has not been checked. Perhaps a separate standard is needed to address protection of confidential reliability-related information. 4. In the "Applicable Reliability Principles" Section we suggest; **Check Box # 3 relating to Planning**. As stated previously, planning computer systems and their associated data might contain confidential/sensitive information about the reliable/secure operation of the BES and should be secured as well. **Check Box # 4 relating to Emergency**. This section is also pertaining to confidential/sensitive information/systems/procedures that should be secured/protected. **Uncheck Box # 7 relating to Transmission System Security**. ISO-NE does not believe that this standard is applicable to BES Security. We believe the word "security," since it is not capitalized, was misconstrued to mean cyber security as opposed to operational security. Response: The planning function box has not been checked, for the reason stated above. The 'Emergency' box is not applicable in this SAR. The drafting team believes that the term 'security' was not misconstued and did not remove the check for this box. 5. In the "Detailed Description" Section ISO-NE suggests; **Removal of the 6 numbered bullet items**. These bullets pertain to justification and are brought into this SAR from the Urgent Action SAR. If any further justification needs to be noted we suggest refreshing the

	reasons with any recent pertinent developments/occurances. Response: The referenced items were a carry over from the justification used to request the development of the urgent action standard. These items have been removed from the revised SAR, in response to this and other comments. In the paragraph that begins with "Reliable electric system operations…" strike from the last sentence **"by establishing standards to assure that a lack of cyber security for one critical asset does not compromise security and risk grid or market bulk electric system failure.** The last sentence would now be **"Because of this mutual vulnerability and interdependence, it is necessary to safeguard the critical cyber assets that support the operation of the bulk electric system."** It is not clear what the proposed strikeout language was meant to say. Does it imply full redundancy of all Cyber Critical Assets or does it imply a lack of installed/designed security for a critical asset is OK under system performance based standards? ISO-NE believes this should not be detailed out at this point in the development of the SAR. Additionally, references to market failures do not justify the need for a Reliability Standard. In the paragraph that begins with "This standard requires that … ISO-NE suggests removing the reference to governance and business rewriting its associated sentence to "**A basic cyber security program for bulk electric system operations shall address program administration, planning, prevention, operations, incident response, and operation continuity.** Governance has many other industry connotations. If program administration was meant by the term "governance", then it is perhaps a more appropriate term. Business should be stricken and replaced with "operation" if the drafters meant business to mean economic or Market continuity. The focus of all NERC Reliability Standards should be maintaining reliability while not violating Market Principles. In the paragraph that begins with "This cyber security standard shall… ISO-NE suggests striking the last sentence of this paragraph. There is a very broad range of issues and opinions on how far the physical security aspect of the standard should permeate or to what degree of granularity should be specified in the SAR. ISO-NE believes that it should be left to the affected parties to determine to what extent physical security is required for protection of Critical Cyber Assets. In the paragraph that begins with "This Standard provides…" We suggest removing the reference to "electric system operations" as this term is too broad. We suggest replacing it with "operation of the bulk electric system". The sentence would now be **"This standard provides definition of terms and the minimum requirements to implement and maintain a cyber security program to protect cyber assets critical to reliable operation of the bulk electric system."** Response: The detailed description has been reworded using input from this and other comments.

	Removal of those terms listed that do not appear in this SAR document. They are not pertinent to this SAR and may not be utilized in the Reliability Standard. If additional terms are utilized/introduced in the Reliability Standard then they may be defined there. Alternatively, if the drafting team believes it is important to provide some common understanding of these terms to the Standards Drafting team then we suggest providing them as discussion points in the "Detailed Description" section of the SAR. We also suggest revising the definition of Cyber Critical assets to be; "Critical Cyber Assets are any system or combination of computer and electronic systems, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the operation of the bulk electric system. This includes Supervisory Control and Data Acquisition (SCADA) systems, Energy Management Systems (EMS), process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations whose loss, failure or compromise could have a significant adverse impact on the bulk electric system (i.e. the ability to serve large quantities of customers for an extended period of time, have a detrimental impact to the reliability or operability of the bulk electric system, or would cause significant risk to public health and safety)." Response: Definitions for terms not used in the SAR have been removed, as suggested. The definition of critical cyber assets has been revised to add greater clarity and scope. ISO-NE also would like to note that this SAR and its resultant Reliability Standard will NOT apply to Nuclear Units as their security requirements are separate and developed by the Nuclear Regulatory Commission, (NRC). We therefore believe it should be stated somewhere in the document. Response: The drafting team is collecting and reviewing all existing cyber security guidelines as the SAR is being developed. It must be recognized that US Federal guidelines may not apply to Canadian entities, however. It is also challenging to keep a NERC standard in synch with parallel standards over the long haul. The drafting team agrees that the NRC will have jurisdiction over nuclear plants in the US.
Joseph Krupar, Florida Municipal Power Authority, Segment 3	1. The Scope is too broad including the term "any" and "communication network". The Purpose should be changed to "To reduce risks to the reliability of the bulk electric system from intentional and/or malicious acts that result in malfunction of critical cyber assets." Response: The drafting team believes that the revised definition of critical cyber assets and other changes to the SAR sufficiently addresses this comment. 2. In the Brief Description "change bulk electric systems" to "bulk electric system". There is only one bulk electric system where there are three interconnections (East, West and ERCOT). The Functional Model also has the term "bulk electric system".

	Response: It is NERC's philosophy that the North American grid is made up of multiple bulk electric systems. 3. In the Detailed Description a sentence should be changed. "This standard will apply to entities performing the Reliability Authority…….. and Load Serving Entity and functions." The last and before functions should be eliminated so the sentence reads "This standard will apply to entities performing the Reliability Authority…….. and Load Serving Entity functions." Response: The typo has been corrected. Thank you. 4. In the Definition of Critical Cyber Assets the "currently" in the last sentence should be eliminate. If any of these are to be included in the future a new standard will be needed. Also specifically define what is a Critical Cyber Asset like EMS and SCADA. Response: The definition of critical cyber assets has been revised to add greater clarity and scope. 5. The Definition of Cyber Security Incident is too broad using the term "any" and "otherwise". Definition should be changed to "An intentional and/or malicious act that result in malfunction of a Critical Cyber Asset." Response: The definition has been revised to add greater clarity.
Joe Weiss, KEMA Inc, Segment 8	The SAR states that: "Reliable electric system operations are highly independent, and a failure of one part of the generation, transmission, or grid management system can compromise the reliable operation of a major portion of the electric regional grid. " Generation control systems (fossil, nuclear, hydro, and even inter-connected distributed generation) and substations/switching stations have been conclusively demonstrated to be vulnerable to cyber intrusions and can have a potentially significant impact on grid and/or market operations. They must be specifically addressed, particularly since the Urgent Action SAR explicitly excluded them. Response: The definition of critical cyber assets has been revised to add greater clarity and scope. DOE tasked NERC to be the coordinator for the electric power industry for responding to critical infrastructure protection. This did not limit NERC to transmission only. Distribution substations can be vulnerable to cyber intrusions and potentially could have reliability and/or market impacts on the regional grid. Distribution substations also need to be included and addressed Response: NERC is responsible for the reliability of the bulk electric system. The definitions in the SAR have been revised to make this clear. **The scope contained in this SAR should be expanded to include the following:**

	Generation control systems as they impact grid control and/or market operations Transmission substations and switching stations including all cyber-connected equipment Distribution substations including all cyber-connected equipment Please see responses above.
NPCC CP9 ----- Guy Zito, NPCC, S2 Ralph Rufrano, NYPA, S1 Barry Gee, US National Grid, S1 Dan Stosick, ISO-NE, S2 Dave Little, Nova Scotia Power, S1 Roger Champagne, HQ, S1 David Kiguel, Hydro One Networks, S1 Jim Ingelson, NYISO S2	Response: Please see the responses to these comments, submitted by Kathleen Goodman on behalf of ISO NE. 1. We suggest the title of the SAR be changed to **"Protection of Critical Cyber Assets".** The original title could apply to protection of all Cyber assets even non critical ones such as websites, payroll, billing, etc. 2. In the "Description" we suggest changing the second sentence to the following; *Requirements will be included in the standard to identify the responsible person(s), create and implement Security programs, perform a thorough assessment of cyber security, and implement appropriate and technically feasible security improvements.* And add the following new sentence to the end of the "Description"; *Security programs include the organization's policies, standards, procedures, training and auditing controls for the implementation of the NERC Protection of Critical Cyber Assets.* 3. In the "Standard will apply to …" Section we suggest; **Check the Transmission Owner box on the SAR**. The TO's in many cases own the cyber critical assets in an area, or portions therof, and due to future compliance concerns NPCC feels it is appropriate to place the responsibility with adherance to the standard on the entity that actually owns the equipment. **Check the Planning Authority box on the SAR**. It is felt that although the Planning Function has not been finalized in the NERC Functional Model the information and systems utilized in the planning area could be of a confidential nature and contain sensitve information that could represent a security issue. 4. In the "Applicable Reliability Principles" Section we suggest; **Check Box # 3 relating to Planning**. As stated previously, planning computer systems and their associated data might contain confidential/sensitive information about the reliable/secure operation of the BES and should be secured as well.

	Check Box # 4 relating to Emergency. This section is also pertaining to confidential/sensitive information/systems/procedures that should be secured/protected. 5. In the "Detailed Description" Section we suggest; **Removal of the 6 numbered bullet items**. These bullets pertain to justification and are brought into this SAR from the Urgent Action SAR. If any further justification needs to be noted we suggest refreshing the reasons with any recent pertinent developments/occurances. In the paragraph that begins with "Reliable electric system operations…" strike from the last sentence **"by establishing standards to assure that a lack of cyber security for one critical asset does not compromise security and risk grid or market bulk electric system failure.** The last sentence would now be **"Because of this mutual vulnerability and interdependence, it is necessary to safeguard the critical cyber assets that support the operation of the bulk electric system."** It was not clear to a wide cross-section of industry experienced people what the proposed strikeout was meant to say. Does it imply full redundancy of all Cyber Critical Assets or does it imply a lack of installed/designed security for a critical asset is OK under system performance based standards? We thought it best if this was not detailed out at this point in the development of the SAR. In the paragraph that begins with "This standard requires that … We suggest removing the reference to governance and business rewriting its associated sentence to "**A basic cyber security program for bulk electric system operations shall address program administration, planning, prevention, operations, incident response, and operation continuity.** Governance has many other industry connotations. If program administration was meant by the term "governance", then it is perhaps a more appropriate term. Business should be stricken and replaced with "operation" if the drafters meant business to mean economic or Market continuity. The focus of all NERC Reliability Standards should be maintaining reliability while not violating Market Principles. In the paragraph that begins with "This cyber security standard shall… We suggest replacing the term cyber resources with critical cyber assets and their operation. The last sentence of this paragraph would now read **"In addition, physical security shall be addressed to the extent that is necessary to assure a secure physical environment for critical cyber assets and their operation."** There is a very broad range of issues and opinions on how far the physical security aspect of the standard should permeate or to what degree of granularity should be specified in the SAR. The suggested wording represents a compromise. In the paragraph that begins with "This Standard provides…" We suggest removing the reference to "electric system operations" as this term is too broad. We suggest replacing it with "operation of the bulk electric system". The sentence would now be **"This standard provides definition of terms and the minimum**

	requirements to implement and maintain a cyber security program to protect cyber assets critical to reliable operation of the bulk electric system." 6. In the "Definitions" Section we suggest; **Removal of those terms listed that do not appear in this SAR document.** They are not pertinent to this SAR and may not be utilized in the Reliability Standard. If additional terms are utilized/introduced in the Reliability Standard then they may be defined there. Alternatively, if the drafting team feels it is important to provide some common understanding of these terms to the Standards Drafting team then we suggest providing them as discussion points in the "Detailed Description" section of the SAR. We also suggest revising the definition of Cyber Critical assets to be; "Critical Cyber Assets are any system or combination of computer and electronic systems, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the operation of the bulk electric system. This includes Supervisory Control and Data Acquisition (SCADA) systems, Energy Management Systems (EMS), process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations whose loss, failure or compromise could have a significant adverse impact on the bulk electric system (i.e. the ability to serve large quantities of customers for an extended period of time, have a detrimental impact to the reliability or operability of the bulk electric system, or would cause significant risk to public health and safety)." NPCC also would like to note that this SAR and its resultant Reliability Standard will NOT apply to Nuclear Units as their security requirements are separate and developed by the Nuclear Regulatory Commission, (NRC). This group felt it should be stated in the document however achieved no consensus as to where a "Shall not apply" statement might appear.
Greg Stone, Duke Power, Segment 1	1. There is no clearly discernable "scope" to this SAR. While it generally describes a need for a "cyber" standard and provides a brief description of its intentions, it does not provide sufficient descriptive detail to clearly describe the scope/breadth of the proposed standard. This SAR needs to be amended to more clearly describe its intended depth and breadth. The full paragraphs in the "Detailed Description" section would be a good starting point. Further, there does not appear to be any proposed implementation plan as is described in the Standards Process Manual as being a portion of a SAR. Response: The SAR has been revised and a reference to the urgent action standard has been included. This should clarify the scope of the SAR. The final implementation plan will have to be

	developed when the standard is written because this is the point at which the compliance elements are written, but some guidance has been included in the SAR. 2. Suggest that the opening "bullets" in the Detailed Description be deleted; that the remaining language be amended so as to not read as though a standard has already be developed (Such as changing: "This standard requires …" to "This standard would require…"); that the lessons learned from the urgent action Standard be referenced; and that the beginnings of an implementation plan be included. Response: The referenced items were a carry over from the justification used to request the development of the urgent action standard. These items have been removed from the revised SAR, in response to this and other comments. 3. In addition, this SAR needs to be expanded to include the PSEs. Because of their critical function, essentially acting as a "bridge" between the generators and the LSEs, to the extent that a PSE may also have critical applications, then these standards must also apply. As the detailed described indicates: " … the wholesale electric market as a network of economic transactions and interdependencies relies on the continuing reliable operation of not only physical grid resources, but also the operational infrastructure of monitoring, dispatch, and market software and systems." This fairly describes the critical role of not only those cyber assets which control the physical grid, but also those cyber assets which control the "economics" critical to today's operations. Response: The PSE function is outside the scope of a NERC reliability standard. The drafting team will encourage NAESB to adopt comparable standards for market systems such as OASIS, tagging, and scheduling. 4. Eliminate the numbered items in the detailed description section. Also, eliminate the defined terms. Again, this presupposes that these terms will be used, with the listed definitions, by the SAR drafting team, One of the lessons learned during the creation of the existing urgent action cyber standard is that these definitions need improvement. Response: It is important that terms used in the SAR be defined so that industry commenters have a clear understanding of what is intended. Definitions will not appear in the final standard, but will be housed in a separate glossary. The detailed description has been revised. Several additional items need to be addressed:

	1) How will the requirements of this standard apply to critical infrastructure not directly owned or controlled by the electric sector, for example communication systems? Response: The drafting team believes the clarity added in the revised SAR related to security perimeters addresses this comment. Communication systems between perimeters are not required to comply with this standard. This has been stated in the SAR. 2) Delete the paragraph in the detailed section that begins: "This standard will apply to …."This is redundant with the matrix on page 2. Response: Although this is redundant, it has been left in to reemphasize the applicability. Applicability was questioned repeatedly during the development of the urgent action standard. 3) The SAR drafting team should be encouraged to review the existing urgent action Cyber Standard and base their work on the foundation being laid by that standard. As we move toward compliance with the existing Cyber Standard, the industry needs some level of assurance that the replacement permanent standard will at least be directionally compatible with the current standard Response: The drafting team agrees. A reference to the urgent action standard has been included in the revised SAR.

Other Comments:

-----Original Message-----
From: Bauer, Kathleen M [mailto:Kathleen.Bauer@northwestern.com]
Sent: Tuesday, August 05, 2003 10:13 AM
To: Tim Gallagher
Cc: Patterson, M LeRoy; Leland, R J (John)
Subject: NERC Cyber Security SAR
This response meets your request for comments by August 8,2003. Questions or comments on the following NorthWestern Energy comments should be directed to either LeRoy Patterson or Mark Weiss.
While several sections raise concerns, NorthWestern Energy (NWE) has significant concerns with sections 1207 - Personnel and 1208 - Monitoring Physical Access regarding the ambiguous intent of the Standard. The document must clarify who falls under this requirement and how these measures are intended to be implemented. For example: the

proposed language is not explicit regarding personnel requiring background checks. NERC must revise the Standard to clarify the intent and not depend on a 'Common Questions' supplement to define intent. As another example: the physical monitoring measure might be interpreted to require video surveillance of access doors. While this solution may be acceptable at a Control Center, it will quickly become impossible as the 'cyber boundary' expands to include corporate networks, substations, etc. In addition, the Standard might be interpreted to require multiple personnel to continuously view these videos, and keep them for multiple years, to ensure compliance. There must be a better way to verify compliance with physical access controls.

Regarding the 'audit' provisions of the SAR, NWE supports the concept of cyber security standards. However, the provisions related to verifying compliance with this standard are ambiguous and, if interpreted in the most rigorous sense, are more onerous than necessary or appropriate. These 'audit' provisions must more explicitly state the requirements since it is not acceptable for an entity to find itself out of compliance during an audit because it interpreted the language differently than those 'judging' compliance.

Thank you for the opportunity to comment.

Kathy Bauer
NorthWestern Energy
40 East Broadway
Butte, MT 59701
(406) 497-3576
Kathleen.Bauer@northwestern.com

Response: These comments will be shared with the standard drafting team. The comment deals with detailed items that are beyond the SAR.

----Original Message-----
From: John Marschewski [mailto:JMarschewski@SPP.ORG]
Sent: Thursday, July 17, 2003 5:02 PM
To: Michehl R. Gent
Cc: NERC Regional Managers; SPP BOD (Members Only)
Subject: NERC Cyber Security Standard

Mike,

Southwest Power Pool is a strong supporter of the NERC efforts on cyber security and voted for passage of the recent Urgent Action Cyber Security Standard. We also are pleased that NERC has already initiated the development of a permanent cyber security standard.

To that end, I would ask you to use your best efforts to ensure that the permanent cyber security standard and accompanying implementation and compliance plan are as broad and robust as possible. The Urgent Action Cyber

Security Standard and implementation plan did not cover some critical issues that the industry needs to address immediately in promoting the security of the cyber assets that we depend on to support reliability of our interconnected electric systems. Our hope is that the permanent standard and associated implementation and compliance plan will address several issues that we see as shortcomings in the Urgent Action Cyber Security Standard:

Background Checks - The response to comments regarding background checks diluted the original intent of the standard. Given the fact that the majority of security problems that our industry and others experience are attributed to "insiders," this is an important area to cover in the permanent standard.

Applicability and Compliance - The Urgent Action Cyber Security Standard applies to all entities performing various electric system functions, as defined in the functional model. Until the standards are developed for certifying the entities responsible for these functions, the standard will apply to reliability coordinators, control areas, transmission owners and operators, and generation owners and operators. However, for reasons addressed in the response to comments, the implementation plan indicates that the NERC Compliance and Enforcement Program will evaluate only control areas and reliability coordinators for compliance with this standard in 2004. Other entities are expected to work to meet the requirements of the standard; however, self-certification forms will not be required. It is critical, in our opinion, that NERC apply the permanent standard and associated implementation and compliance plan across the board to all entities responsible for performing reliability functions.

Thanks in advance for your consideration of these comments and your efforts to see that the permanent cyber security standard and associated implementation, and compliance plan addresses them. Please pass these comments on to other appropriate entities.

Sincerely,
John Marschewski
President,
Southwest Power Pool

Response: These comments will be shared with the standard drafting team. The comment deals with detailed items that are beyond the SAR. The SAR has been revised to increase the breadth and robustness of the standard.