

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Seiki Harada
Organization	BC Hydro
Industry Segment #	1, 3, 5 and 6
Telephone	604 623 3550
E-mail	<a href="mailto:Seiki.harada@bchydro.com">Seiki.harada@bchydro.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative: Representative Phone: Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

According to the present version of the Cyber Asset Definition, a SCADA system may be exempted from the application of the standards if it happens to use a very old networking that is not on a stacked protocol. I would say all SCADA for bulk power system must be included.

Additionally, the detailed description section essentially lists two major purposes for the standards: bulk system reliability and efficient market. Looking at the definitions for Cyber Assets and Critical Cyber Assets, they are defined only for bulk system reliability. If we are truly serving the two purposes, we must include such systems as eTAG, OASIS and other market oriented systems.

The definition of Critical Cyber Assets includes 'black start'. I am not sure if this is pointing to the process to restart the part of the grid that collapsed, or the systems required to start up a generating station that tripped off. Perhaps, we need to qualify the words 'black start'.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments:

44 hours per year is a lot of time to be down for 7x24 critical links. I would say we should shoot for about half of that. Further, the cumulative down time alone is not a good measure. It should be combined with the frequency of the communications link going down. For example, even if the communications link is down for only 10 hours per year, if the link was down five times every day for 10 seconds each randomly, the link would be useless.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for

**partial failures? What level of availability should be required?**

Yes

No

Comments:

A good level of availability is a function of 1) implementing adequate security measures, 2) maintaining/patching software, hardware and data, 3) operating the systems safely and properly, and 4) external forces which try to disrupt orderly operation. Similar to the number of cyber incidents an entity may encounter in a year, most external factors are not under the control of the entity in question. For example, if there is an overwhelming attack on the DNS server in one sector of the Internet, all Internet based systems and networks might feel the impact (and thus the degraded availability). It is not reasonable to set a standard over a measure for which the entity does not have total control over.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

**e. If the above were included, how long would each take to complete?**

Comments:

This will take a long time to implement (> 10 years?) and a lot of money. We may consider implementing these new measures only to the new implementations and major upgrades as of a certain future date.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

---

Yes

No

Comments:

It makes sense to provide redundancy for key SCADA /EMS systems. However, I am not sure if we should be designing in redundancies in ALL the cyber assets declared as 'critical'. It may not be economically feasible to provide redundancy for all components of all critical systems. Also, we may find that some 'critical' systems are 'more critical' than others....

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

This set of standards is much more wide-encompassing than the Urgent SAR standards. We will need to give sufficient lead time for all participants to implement the additional requirements.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Joe Weiss
Organization	KEMA
Industry Segment #	8
Telephone	(408) 253-7934
E-mail	<a href="mailto:jweiss@kemaconsulting.com">jweiss@kemaconsulting.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments:

The Cyber Assets definition states: "This definition applies only to systems or devices that use a network stack protocol for communications." This statement needs to be deleted. Cyber assets are not dependent on specific communication protocols. Cyber assets associated with bulk electric system operation utilize non-network stack (non-TCP/IP) protocols such as Modbus, Profibus, and conventional serial RTU communications. Additionally, dial-up modems and unsecured radio links are obviously cyber vulnerabilities and do not use network stack protocols.

The Security Incident definition states: "...any physical or cyber event of malicious or unknown origin..." This is not inclusive enough. There can be cyber events of known, benign origins that can disrupt functional operation of critical cyber assets and cause security incidents. There have been several confirmed cases of benign origin causing denial of service in the utility and other process industries.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments:

The critical need for communications is during an upset event such as August 14<sup>th</sup>. The requirement should be that communications have a 99.5% availability including during upset events.

### 3. The SAR does not address the availability of critical cyber assets. Should



requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments:

SCADA specifications often require 99.95% availability for critical functions. It is critical that the function be maintained, not necessarily the asset.

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments:

Encryption does not guarantee the critical functions of authentication and message integrity. Encryption may not be practical for certain generation of SCADA systems. It may not be possible to implement encryption for current plant controls and substation equipment.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments: Same

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments: Same

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments: Same

**e. If the above were included, how long would each take to complete?**

Comments: See comment 4a

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments:

Redundancy does not necessarily mitigate cyber vulnerabilities. Two systems on the same compromised network can be equally vulnerable even though there is “traditional” redundancy.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments:

1. Distribution providers should be included since many large transmission substations also include distribution equipment that often communicate with transmission devices (and vice versa) making them equally cyber vulnerable. Additionally, DOE tasked NERC to address the electric utility industry- this includes distribution.
2. Market operators should be included per the second paragraph of the detailed description and also because they are part of the electric industry.
3. Encryption should not be required until is it confirmed by testing that encryption is the appropriate technology to meet the required functional needs. This has not yet occurred.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Keith Fowler
Organization	LG&E Energy Corp.
Industry Segment #	1, 5, 6
Telephone	502.627.2724
E-mail	<a href="mailto:keith.fowler@lgeenergy.com">keith.fowler@lgeenergy.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments We feel the definitions in the current SAR are adequate and do not necessitate an unreasonable amount of company specific interpretation regarding scope.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments This is a reliability issue, not a cyber security issue.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments Availability is not specifically a cyber security issue.

### 4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments While we support the use of encryption, especially in the case where communications are occurring over the Internet, we feel in other cases it may be unreasonable or of limited value to require encryption, especially during the timeframes being considered for the current SAR. As stated in our general comments, a risk management approach should be utilized, in which case the risk involved with not protecting a given communications link would determine how critical it is that encryption technology (in this case) be deployed. Certainly we feel that ICCP communications between control centers over the Internet would be a high priority candidate for encryption.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

(a.) Comments Comments above apply. A lower priority candidate for encryption than

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

(a.) Comments Comments above apply. A lower priority candidate for encryption than

**d. Data collection servers communications to substation IEDs**

Yes

No

(a.) Comments Comments above apply. A lower priority candidate for encryption than

**e. If the above were included, how long would each take to complete?**

Comments Allowing for industry specific standards (defacto or otherwise) to mature, products to be developed and then implemented we estimate 3 - 4 years for all of the above.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments Again, a availability issue, not a cyber security issue.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> International Transmission Company	<b>Group Representative:</b> <i>Jim Cyrulewski</i> <b>Representative Phone:</b> 248-374-7130 <b>Representative Email:</b> jcyrulewski@itctransco.com	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Jim Cyrulewski</i>	<i>ITC</i>	<i>1</i>
<i>Pete Scussel</i>	<i>ITC</i>	<i>1</i>
<i>John P. Flynn</i>	<i>ITC</i>	<i>1</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments Find 99.5 reasonable. In the standard need to define downtime, i.e., what classifies as downtime. For example, a lease line has three substations on it. Say one line goes down for one hour, is it a 3 hour downtime ( one hour downtime per substation) or one hour per line. Do planned outages count against 99.5%?

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments Just as important as secured perimeters. Need minimal availability guidelines.

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

**e. If the above were included, how long would each take to complete?**

Comments Could take a couple of years. This work is very expensive.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments Why wasn't Principal 4 checked?

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>OUC</i>	<b>Group Representative:</b> <i>Richard Kinas</i> <b>Representative Phone:</b> 407-423-9165 <b>Representative Email:</b> rkinas@ouc.com	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Edwin Lopez</i>	<i>OUC</i>	
<i>John Mcgruder</i>	<i>OUC</i>	

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments The SAR should provide "communications" availability requirements, in that communications required to perform a specific task could be primarily data orientated during regular business and possibly voice during emergencies, or specific asset failure. The communications requirement should be specified for the function being performed not on the specific underlying infrastructure.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments Critical cyber assets are used in the performance of functions, and while the reliability of the function must be specified, the particular methods and equipment that provide the reliability should not. As long as some sort of infrastructure and methods exist to provide this function the spirit of the SAR is met.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

- Yes  
 No

Comments Within the energy environment, preventing data from compromise (i.e. encrypting it during transmission) is a much lower concern than verifying that the data was not modified during transit (a.k.a message integrity), that the data did in fact originate from the sender (a.k.a. message authentication) and that it can be proved that the data was sent, from the receivers point of view (a.k.a. non-repudiation). All the above functions use encryption, however the SAR seems to specify only the block cipher (data compromise) portion of the entire process.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

- Yes  
 No

Comments See comments for 4.a .Additionally modification of peer-to-peer connections for encrypted communication would be a very difficult and costly task, if it could be done at all. More than likely, a front end device of some kind would need to be used instead, however the latency which devices such as these could introduce must not adversely affect the time critical communications themselves.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

- Yes  
 No

Comments See comments for 4.a. Additionally this would be fairly easy to implement on the IP stacks running on the RTU's, but in practice, it would probably be implemented through a front end device such as a small VPN firewall located just in front of each device.

**d. Data collection servers communications to substation IEDs**

- Yes  
 No

Comments See comments for 4.a

**e. If the above were included, how long would each take to complete?**

Comments Items 4.a,c, and d could be implemented almost immediately through the use of a front end device, however, item b would take some investigation into the peer-to-peer protocol to investigate the encapsulation possibility and again using the front end device.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

- Yes

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

---

No

Comments Redundant assets do not necessarily provide additional reliability. Redundant assets should not be required but high availability of the function should be.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name            John Horakh 01-14-2004  
Organization    MAAC  
Industry Segment # 2  
Telephone       609-625-6014  
E-mail           john.horakh@conectiv.com

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments The definitions have been significantly improved over those in the Version 1 SAR. The definition of Critical Cyber Assets as a subset of Cyber Assets is a good idea. However, the first sentence of the Critical Cyber Assets definition needs some words added. It should read “Critical Cyber Assets: Cyber Assets whose loss or compromise could adversely impact, **to an unacceptable degree**, the reliability of bulk electric system operations”. It is likely that the loss of all (or almost all) of the Cyber Assets could adversely affect the reliability of the system, to a lesser or greater degree. The Critical Cyber Assets are only those that adversely affect the reliability of the system to an unacceptable degree.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments I have no reason to believe a 99.5% uptime probability is any more reasonable than 99.0% or 99.9%. There is a tradeoff between the cost of increased availability and the cost of the adverse consequences resulting from downtime. Does the downtime cause loss of load? If so, a 99.5% uptime may be too low, since bulk electric systems (at least some) are designed for a loss of load expectation of one occurrence in ten years. In any case, the use of “hard” numbers like 99.5% is not appropriate in the SAR. Those numbers, if appropriate, should be developed and put out for comment in the Standard, when it is written. The SAR should only indicate that a very high level of availability is required.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments If availability of data communications is to be addressed, then availability of Critical Cyber Assets should also be addressed. Availability requirements for Critical Cyber Assets should be on a basis consistent with availability requirements for data communications. These should be determined in the Standard process, not in this SAR.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments These questions are not appropriate to be answered in this SAR. They are too detailed for a SAR. A general statement should be inserted in this SAR to indicate that encryption of communications, in general, should be considered when the Standard is written.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments See comment for a. above

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments See comment for a. above

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments See comment for a. above

**e. If the above were included, how long would each take to complete?**

Comments See comment for a. above

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments Redundancy is really just a way to achieve increased availability. If availability is addressed (see Question # 3), it is not necessary to separately consider redundancy.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments A. In the Purpose / Industry Need section, add the word “data”, to read as follows: “To protect the critical cyber assets (computers, software, **data**, and communications networks) essential to the reliability of the bulk electric system.”

B. In the Brief Description section, add words to make the third sentence read as follows: “Requirements will be included in the Standard for responsible entities to create and implement **at least minimum level** programs and procedures, **to** perform ongoing assessments, and **to** implement .... etc” The Standard should do a lot more than requiring responsible entities to have and implement some sort of cyber security program. There should be some minimum level, measurable program required.

C. In the Detailed Description section, move the word minimum, and add words, in the first sentence. The sentence would then read: “This Standard identifies the requirements to implement and maintain **at least a minimum level** cyber security program to protect cyber assets critical to reliable bulk electric system operation”. See Comment B. above.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

### SAR Commenter Information (For Individual Commenters)

Name	Richard Brooks
Organization	Independent Consultant
Industry Segment #	8
Telephone	602-684-1484
E-mail	<a href="mailto:d.brooks@ieee.org">d.brooks@ieee.org</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial Regulatory or other Govt. Entities



## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

No

Comments:

Regarding the definition for “Cyber Assets”

The phrase “network protocol stack” is open to interpretation and may cause confusion as parties attempt to identify Cyber Assets. As an example, some data communication standards, e.g. IEEE 802.11b may not be associated with a specific “Network Layer” protocol, such as the Internet Protocol (IP), but devices implementing 802.11b may indeed be essential to electric system operations and should possibly be considered a Cyber Asset.

Ref: IEEE 802.11b information is available at  
<http://standards.ieee.org/getieee802/download/802.11b-1999.pdf>

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Qualified - Yes

Comments:

Provided there are efficient and appropriate failover procedures and processes in place to ensure that alternate communication channels are available during such outages.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes



Comments:

Cyber assets, especially those assets used to monitor and/or support system reliability should be included, with respect to availability. Availability requirements of such devices should be assigned according to role and risk factors, i.e. the “impact” on system manageability/control should a security breach occur on the device or if the device should fail.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

- a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

Comments:

If sensitive information travels over a shared network infrastructure it should be encrypted to prevent unauthorized access. The authors may also wish to consider use of digital signatures for authentication of origin and digital certificates for access control authentication.

- b. SCADA master station to RTU communications using peer-to-peer communications protocols**

No

Comments:

Communications occurring over private network connections are less vulnerable to unauthorized access using “man in the middle” tactics, which encryption is designed to address.

- c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Qualified - No

Comments:

Provided such communications are performed over a peer-to-peer, private network connection. If the communications are occurring over a shared network then encryption should be used.

- d. Data collection servers communications to substation IEDs**

Qualified - No

Comments:

Provided such communications are performed over a peer-to-peer, private network connection. If the communications are occurring over a shared network then encryption should be used.

- e. If the above were included, how long would each take to complete?**

Comments:

In many cases hardware level encryption devices can be installed using a phased approach with

minimal impact to existing processes and procedures. Implementation time and effort vary depending on the number of network nodes requiring encryption.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

Comments:

If a disruption or security breach of such assets could affect system reliability then they should require the same level of redundancy as other critical components.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Jack Hobbick
Organization	Consumers Energy
Industry Segment #	3, 4 and 5
Telephone	517-788-2427
E-mail	<a href="mailto:jwhobbick@cmsenergy.com">jwhobbick@cmsenergy.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments:

Needs more clarification of what was intended, recommend that focus should be on the cyber assets that impact the most critical or greatest number of physical assets. Also the concept of defense in depth should be considered to build layers of security and allow entities to utilize their resources in proportion to the perceived risk. Consideration should be given to levels of criticalness that would allow for different levels of security based on the risk.

Also, the definition list should be expanded to include many more of the terms used in the scope such as Special Protection Systems, Communication Network, Market systems, etc

The last sentence of critical cyber assets should state “should be considered at a minimum”

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments:

This is a reliability requirement, not a security requirement

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments:

This is a reliability requirement, not a security requirement

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments:

Each entity deploying ICCP need to access the risk of that link. Situations such as using public communication system or passing control signals may warrant additional precautions which may be encryption.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments:

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments:

Using a risk analysis based on the criticalness of the device and the type of communication rather than a hard requirement makes more sense.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments:

If someone has already gained physical access to the substation, physically controlling the switches would be far easier than trying to utilize the cyber assets

**e. If the above were included, how long would each take to complete?**

Comments:

At least 5 years depending upon availability of technology and level of expenditures required

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

---

No

Comments:

This would be a reliability requirement.

### **6. Please enter any other comments you have regarding this SAR in the space below.**

Comments:

Narrow the focus to those assets that directly affect the reliability of the grid, specifically cyber assets that can impact multiple physical locations vs. those cyber assets that can only impact a single physical location

Ensure that any future standard is coordinated with Department of Homeland Security requirements.

Endeavor to tightly restrict the scope of the cyber security standard to security.

Avoid setting reliability standards (Items 2,3, and 5) as part of the security standard, this will defer attention away from critical security issues.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Neil Shockey
Organization	Southern California Edison
Industry Segment #	5
Telephone	626-302-2669
E-mail	<a href="mailto:neil.shockey@sce.com">neil.shockey@sce.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## **Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

---

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

**1. Do you agree with the definitions included in the SAR?**

Yes

No

Comments

**2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

- a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control

**centers**

Yes

No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments As with Urgent Action Standard 1200, this SAR is unclear on its applicability to nuclear facilities. The SAR and permanent standard should explicitly exclude nuclear facilities, as this segment of the industry is governed by NRC regulations/standards. The drafting team's response to SCE's concern with this in standard 1200 ("Nuclear plants are not subject to this standard") should be explicitly stated in the SAR and permanent standard to prevent any misinterpretation that nuclear facilities would be subject to the permanent standard.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Robert Metcalf
Organization	MidAmerican Energy Company
Industry Segment #	3
Telephone	515/242-4379
E-mail	<a href="mailto:rsmetcalf@midamerican.com">rsmetcalf@midamerican.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b>	
	<b>Representative Phone:</b>	
	<b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments: The last sentence of the definition of "Cyber Assets" adds more confusion than value. We suggest the definition for Cyber Assets be, "Those systems (including hardware, software, and data) and communication networks (including hardware, software, and data) associated with bulk electric system operation. This definition applies only to systems or devices that use an IP based protocol."

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments:

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments: It rightfully addresses the availability of the data communication facilities between critical cyber assets, why wouldn't it address the availability of critical cyber assets? We measure partial availability on our business systems by looking at the number of affected users during the duration of the partial failure. A similar approach measuring the loss of control or the loss of

visibility to the number of MW is a possible solution. The target should start at 99.9%.

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

X  No

Comments: More important than encryption is authentication or non-repudiation.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

X  No

Comments: More important than encryption is authentication or non-repudiation.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

X  No

Comments: More important than encryption is authentication or non-repudiation.

**d. Data collection servers communications to substation IEDs**

Yes

X  No

Comments: More important than encryption is authentication or non-repudiation.

**e. If the above were included, how long would each take to complete?**

Comments:

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

X  Yes

No

Comments: One easy way to convince yourself that redundancy should be required is to look at all the utility business systems that have redundant facilities. The critical cyber assets should be held to the same or higher standard.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments: It would be beneficial for our planning purposes to know what the final cyber security standard will look like. Presumably this is just the first step of an evolving standard. If we had the complete plan in front of us, even if it was a staged implementation, we would be making more efficient investment decisions in our cyber infrastructure.



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	Everett Ernst
Organization	OG&E Electric Services
Industry Segment # 1	
Telephone	405-553-8102
E-mail	ernstee@oge.com

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments Different parts would need different reliability levels.

### 4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:

- a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control

**centers**  
 Yes  
 No  
Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**  
 Yes  
 No  
Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**  
 Yes  
 No  
Comments

**d. Data collection servers communications to substation IEDs**  
 Yes  
 No  
Comments Yes only if network protocol stack and the communications circuit extends outside the substation fence.

**e. If the above were included, how long would each take to complete?**  
Comments (a) 1 yr (b) no (c) 2 yrs (d) no These are budget issues if the time frame is under 2 years.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes  
 No  
Comments

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	Cory Cipra
Organization	Burns & McDonnell Engineering <a href="http://www.utility-security.com">www.utility-security.com</a>
Industry Segment #	8
Telephone	816.822.4266
E-mail	<a href="mailto:ccipra@burnsmcd.com">ccipra@burnsmcd.com</a>

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b>	
	<b>Representative Phone:</b>	
	<b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

Cyber Assets:

The statement "This definition applies only to systems or devices that use a protocol stack for communications" should be removed.

Second, the definitions also include the applicability only to those assets that are "associated with bulk electric system operation." It is recommended that the definitions exclude the word "bulk" as to expand applicability to those entities (distribution) and other assets effecting not only bulk electricity but the equally important downstream entities that are present.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

A similar practice and goal associated with most critical networks and systems in other industries, including telecommunications, is "5 Nines" (99.999%). Although this is the case, there are considerable contrasts and differences between availability and reliability. Further definition of "data communications between secure perimeters" is required.

To further expand on the definition of "data communications between secure perimeters," the availability or uptime of this communications should be a function of the level of criticality associated with those communications. It should also include a factor that determines the influence on the continued delivery of service.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments

Availability references the total amount of time the product, asset, or system was "up." In most cases, the system collectively should be the focus of address vs. the individual asset. The goal is continued delivery of service. Most well-engineered systems have redundant safeguards in place and are not dependent on a single cyber asset for availability.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

This is very important when any communications occurs between "untrusted" networks.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

This is equally important as in many instances, this type of communication traverses potentially unsafe traffic areas including wireless mediums. In many cases, this traffic traverses corporate networks and other types of ubiquitous networks. It should also be noted that this may not be required in every circumstance as the encryption requirement should include a factor that takes into account the criticality of the communications including sensitivity of information.

For example, the communications between a SCADA master station and a RTU that, in downstream, operates with a substation that only feeds a few residential homes, the need for encryption on that communications may not be warranted given the cost, benefits, and potential impact from a compromise. Encryption on this path may be needed however if there could be sensitive information on that communications link that could be used for the compromise of other communications or systems that may be considered critical.

In other words, this should be based on a factor of criticality, sensitivity, and other factors on a case-by-case basis. The criteria has not yet been determined for that and the above are just few along with a very simple example.



**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

See comments 4b.

**d. Data collection servers communications to substation IEDs**

Yes

No

See comments on 4b.

**e. If the above were included, how long would each take to complete?**

The length of time to complete is a function of the size and scope of each network/system. In general, overlaying encryption technologies is not usually an extremely extensive and intrusive process. There are products available today which make this fairly easy to accomplish even in situations where many feel products and technologies do not exist for the “legacy” environments.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

The redundancy of critical cyber assets should not be a requirement for this standard, however most well engineered systems have some method of redundancy in place. The goal should be, as stated, the protection, reliability, and availability of the systems to deliver their function not the assets themselves.

Although this is true, the redundancy of critical cyber assets would, in many cases, directly correlate with total availability of continued delivery of service.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

In general, it is recommended that the SAR be expanded to include distribution providers. As the goal and spirit of the SAR is to address the security, integrity, stability, availability, and reliability of the nation’s critical electrical infrastructure, many large security consequences can occur due to pieces of distribution being affected while at the same time not affecting the entire grid. A good example is many distribution providers that cover large metropolitan/regional areas. Also in reference to this, weak downstream security could potentially result in weak upstream security as cyber assets may be interconnected.

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative: <i>William Lucas</i></b> <b>Representative Phone:</b> 414-221-2220 <b>Representative Email:</b> william.lucas@we-energies.com	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>William Lucas</i>	<i>We Energies</i>	<b>5</b>
<i>Kimberly Pons</i>	<i>We Energies</i>	<b>5</b>
<i>Randy Bredin</i>	<i>We Energies</i>	<b>5</b>
<i>Steve Karolek</i>	<i>We Energies</i>	<b>5</b>
<i>Steve Rohrbach</i>	<i>We Energies</i>	<b>5</b>
<i>Bill Kante</i>	<i>We Energies</i>	<b>5</b>
<i>James Bougie</i>	<i>We Energies</i>	<b>5</b>
<i>Pete Minns</i>	<i>We Energies</i>	<b>5</b>
<i>Tom Wick</i>	<i>We Energies</i>	<b>5</b>

Background Information:

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

*Inclusion of power plant control systems and other monitoring and control systems may place an undue burden on utilities to comply with the standards. Establishment of cyber and physical perimeters with auditing and monitoring for changes at all power plants and substations will require significant funding and time to implement control and isolation changes. While we agree with the concept of including only routable protocol devices, It would be less onerous to require a less restrictive controls measure than what is required for control centers. Especially if the routable protocol field devices can be certified to be directional in nature with no external network access.*

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

*This is not an unreasonable expectation. Increasing availability may be difficult for some.*

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments

*Performance monitoring would be required for all cyber assets. Not only would this be costly, it may not exist for certain equipment. Not to mention the time required to implement such monitoring.*

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

*A critical vulnerability for exploit.*

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

*Not routable, not subject to "man in the middle" attacks.*

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

*Network routable, subject to attack/exploit.*

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

*No network connections between IED and RTU path*

**e. If the above were included, how long would each take to complete?**

Comments

*This could take 6 years or more and will be significant in cost. We are not currently encrypting SCADA data. That would require a change to the SCADA front-ends and software, EMS software, all RTU's, and possibly the MAS radio system we utilize as a transport. This could have a potential price tag in excess of \$10M.*

*There needs to be some uniformity with encryption standards selected to match multiple vendor equipment deployed on a single network. Do we use 3DES or AES? Key management is another issue. No small task here.*

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

*This really is addressed in section 16 "recovery plan and testing" for the interim standard. Redundancy is an outcome of recovery time objectives that should be established as part of the BCP with system availability determined by the various entities.*

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

- *Primary focus should be energy management systems and their respective interconnections with other control entities. Any system using network routable protocol should be considered.*
- *Getting external communications carriers to comply with the standard may not be achievable. A blanket assumption requiring encrypted carrier based circuits may be too restrictive. One could argue that point-to-point circuits have no access from the public, therefore do not need encryption. The statement of 'leased-permanent' implies a DS1/DS3 line for internet access, as point-to-point circuits do not use the 'shared public network' resources (bottom of page SAR-4). Provide more definition and clarification around these terms.*
- *Phase-in time should be identified (is this for new systems or all systems?).*
- *Getting the EMS and SCADA vendors to comply with the standard will take some time, depending on interpretation of what needs encryption.*

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	Stuart Brindley
Organization	IMO (Ontario)
Industry Segment #	2
(Telephone	905) 855-6108
E-mail	<a href="mailto:stuart.brindley@theIMO.com">stuart.brindley@theIMO.com</a>

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b>	
	<b>Representative Phone:</b>	
	<b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.



## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

- Yes  
 No

Comments

For “Cyber Assets”, delete the sentence “This definition applies only to systems or devices that use a network protocol stack for communications.” As it is unnecessarily detailed and limiting.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

- Yes  
 No

Comments

Such technical detail would more properly be part of the Standard, not the SAR.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

- Yes  
 No

Comments

Availability is an important, but completely separate requirement from Cyber Security.

### 4. The SAR does not require that SCADA or PCS communications be encrypted.

**Should this requirement be added for:**

a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers

Yes

No

Comments

b. SCADA master station to RTU communications using peer-to-peer communications protocols

Yes

No

Comments

c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)

Yes

No

Comments

d. Data collection servers communications to substation IEDs

Yes

No

Comments

e. If the above were included, how long would each take to complete?

Comments

This level of technical detail is not appropriate for this SAR, and would be more appropriate as part of the Standard itself.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

- 1<sup>st</sup> sentence – in order to ensure SCADA “monitoring” functionality is included, revise to: “This standard shall primarily focus on electronic systems including: hardware, software, data, related communications networks and monitoring and control systems...”
- Delete the sentence beginning “This standard shall require that third-party...” as it is too limiting and, instead, add to the last sentence “This standard shall require that the responsible entities that must comply with the standard identify and protect themselves from threats from other connected cyber systems, including those provided by contractors and service providers.”
- Delete the last paragraph entirely, as it adds nothing to the scope or intent of the SAR. Further, it includes a level of detail that is inappropriate for a SRA, but would be more appropriate in

the standard itself.

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> Southern Co. Generation and Energy Marketing	<b>Group Representative:</b> <i>Roman Carter</i> <b>Representative Phone:</b> 205.257.6027 <b>Representative Email:</b> jrcarter@southernco.com	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Roman Carter</i>	<i>SCGEM</i>	<i>5,6</i>
<i>Joel Dison</i>	<i>SCGEM</i>	<i>5,6</i>
<i>Tony Reed</i>	<i>SCGEM</i>	<i>5,6</i>
<i>Lucius Burris</i>	<i>SCGEM</i>	<i>5,6</i>
<i>Terry Crawley</i>	<i>SCGEM</i>	<i>5</i>
<i>Roger Green</i>	<i>SCGEM</i>	<i>5</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments: **Cyber Assets:** This definition applies only to systems or devices that use a network protocol Stack for communications. This statement seems to exclude most SCADA host to remote terminal unit communications, power plant control system bus communications, substation automation communications, etc. Therefore, the Critical Cyber Assets definition would seem to be broader than the Cyber Assets definition.

**Critical Cyber Assets:** The response of the drafting to the industry comments made on the Draft SAR Version 1 clearly recognizes the near term impracticality of meeting cyber security requirements for power plant control, remote terminal units, and other field devices. Placing such requirements in a standard with the hope that technologies will develop in a timely manner to meet some projected implementation schedule is unacceptable. The Critical Cyber Assets definition should specifically exclude power plant control, remote terminal units, substation automation control, protective relays, etc.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments- Different assets have different requirements, so it depends on the exact asset. Would it be acceptable for a critical cyber asset to be offline continuously for 43 hours on August 14<sup>th</sup>? It really depends on the criticalness of the equipment.

I believe this question pertains more to Reliability than to Cyber Security.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments- Again as in question #2, this sounds more related to Reliability than Cyber Security. If a Critical Cyber Asset is offline, then it is safe from a Cyber Security Standpoint. However, the stability of the Bulk Electric system may be jeopardized if it is offline.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments- It should be required when encryption technology is commercially available say within 1-2 years. At that point, we feel that ICCP communications between control centers over the internet would be a priority candidate for encryption.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments –Technology is not there yet. It would also require an intensive costly infrastructure to implement.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments – Depends on the type of equipment-private or public. This would be a lower priority candidate.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments – Same as C. above, lower priority.

**e. If the above were included, how long would each take to complete?**

Comments- Anywhere from 2-10 years.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

X No

Comments – This is an availability issue and a Reliability issue more than a Cyber security issue. Redundancy does not necessarily mitigate cyber vulnerabilities. Two systems on the same network can be equally vulnerable, so redundancy does not necessarily equate to better security. Therefore, it should only be required if redundancy can be shown to improve security.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments -Encryption should not be required until it is confirmed by testing and industry agrees it is required to meet security needs.

This Standard is much more wide-encompassing than the Urgent Action Standard. Therefore, it will need to provide ample lead time for all participants to implement any additional requirements.

"The nuclear industry is already developing its own initiatives to perform Cyber Security assessments and measures at nuclear facilities. These are being addressed through the NRC and the Nuclear Energy Institute (NEI). Therefore, nuclear plant systems should be specifically excluded from the scope of this NERC standard."



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	John Lim
Organization	Con Edison
Industry Segment #	1,3,5,6
Telephone	212-460-2712
E-mail	<a href="mailto:limj@coned.com">limj@coned.com</a>

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

*The definition of “Security Incident” is too broad. Change “unknown” to “suspected malicious”.*

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

*Availability requirements are beyond the scope of this SAR, which addresses cyber security and protection, not availability. The requirement must be reworded to address the security aspect. In the Detailed Description section, in the paragraph starting with “Reliable and secure data communications...”, suggest removing sentences starting with “Whether the means...” to the end of the paragraph. Because data communications facilities are often not owned or operated by the responsible entity, the requirement should be that the entity must ensure, where the data communication assets meet the criteria of critical cyber assets for bulk electric power operation, that a single compromise of a data communications component will not compromise the operation of the related critical cyber assets.*

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments

*Availability is not within the scope of this SAR.*

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

*If encryption is required, it should be within the protocol.*

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

**e. If the above were included, how long would each take to complete?**

Comments

*These comments apply to the whole question 4. Encryption is not a requirement, it is a technology employed to achieve certain goals. In the context of the operation of cyber assets related to bulk electric operation, the requirements are authentication of communicating parties, integrity of the data transmitted (i.e that the data has not been modified or corrupted) and in some cases, confidentiality or privacy of the data. Encryption is not always required to achieve these goals. One would expect that for bulk electric operation, these communication links are either privately owned, or dedicated virtual or leased facilities.*

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

*See previous comments. The scope of this SAR should address protection and security of cyber assets, not availability.*

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

*This SAR should scope the standard so that it does not include requirements which cannot be met using technical solutions available today. As much as possible, it should make scope requirements in terms of functions or objectives, rather than technologies used to achieve these functional objectives.*

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>Aquila, Inc.</i>	<b>Group Representative:</b> <i>Phil Sobol</i> <b>Representative Phone:</b> 816-467-3303 <b>Representative Email:</b> phil.Sobol@aquila.com	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Larry Baldwin</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Dwight Burt</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Bob Callegari</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Gary Condict</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Carl Fulbright</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Dennis Greashaber</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Steve Hillman</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Mathew Irwin</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Rick Krepps</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Mitch Krysa</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>John Mason</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Tim Raines</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Mike Sauber</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Aaron Smallwood</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Trudy Stonacek</i>	<i>Aquila, Inc.</i>	<i>1,5</i>
<i>Jim Zorn</i>	<i>Aquila, Inc.</i>	<i>1,5</i>

Background Information:

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

---

### Notes to Industry Commenters:

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments:

Should have a comma after “automatic generator control” for Critical Cyber Assets definition. Under “Security Incident”, I would replace “that” with “with intent to”.

Additionally, we question the inclusion of power plants and substations with automated controls. Older systems are not as vulnerable to attacks since they are not using an IP stack to communicate nor are they communicating over the public network. In some power plant cases, these are stand-alone systems which have no connectivity to the Internet or back to the corporate network. Same with substation communication. The task to comply is very large. Adding in power plants and substations at this time expands the scope of the requirements making it more difficult to reach compliance in the specified timeframe. It would be better if these requirements were phased in later giving the industry time to do the work and consider how to recover costs.



**2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments

This is usually the case. However there are instances of solar activity and equipment failure that might reduce that number. Most communication paths are non-redundant due to the cost involved. This goal is achievable, however I am not sure that this is a "Security Issue". This is more of a business continuity issue. The 99.5% uptime would only apply to normal operating conditions per control area. Force majeure would have to be excluded since these conditions cannot fully guarantee a 99.5% uptime.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments:

Most SCADA systems are redundant and are designed to continue operation with the failure of one piece of equipment. It is our experience that the SCADA master station has an availability much greater than 99.5%. Systems can be redundant with dual power supplies and such. NERC Policy 6 Section E already covers the need to redundancy. A reference to this requirement would probably be sufficient. The availability of these critical assets falls more under the business continuity umbrella than that of cyber security.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

X Yes

No

Comments:

The standard has been developed and could easily be implemented. However, the reason is not as much for security as it is for restricting access to market sensitive data. This would have to be done as an entire industry so that all participants are using compatible technologies to communicate with and be able to move forward with this as a unified group.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

X No

Comments:

On a closed system we don't believe the risk is great enough to warrant the expense of doing this. The communications path would have to be broken and a device inserted to communicate with the RTUs the same way the master station does using the correct protocol. It would require knowing the RTU address and data base point id's. This would be very unlikely. Another consideration is timing. It takes time to encrypt and decrypt the data stream. When you are polling your devices at a rate of once every four seconds, the possibility of getting behind and dropping some data is a real threat. Dropping or missing information in a real-time system is not an option. However, if the utility were using the public Internet to communicate over, then the need for some type of encryption is necessary. A better solution here would be VPN over public networks rather than trying to encrypt the communications on the RTU or PCL.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments:

This is assuming that communications are on a potentially public accessible network.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments:

These servers would be inside the substation on a dedicated network to the IEDs and should not require encryption. If this communications is stacked, and via a public accessible network the answer would be Yes.

**e. If the above were included, how long would each take to complete?**

Comments:

ICCP has already been developed. As far as the other forms it would take, in many cases there hasn't been a standard developed. This could take a year to develop the standard and several more years to develop, fabricate, test and implement the equipment and protocols necessary to be able to work within a real-time system effectively.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments:

It depends on what cyber assets you are talking about. Most SCADA systems and front ends are redundant. However it would be unreasonable to have redundant communication paths to RTUs due to the cost. In most cases the loss of one or two RTUs is not a major problem and can be handled until the problem is corrected. Again, we would recommend referencing NERC Policy 6 Section E.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments:

Our concern is the data encryption requirements placing an undue cost burden on the industry with out offering any real value. My concern is establishing un-realistic requirements which are of no, or limited value. Putting too much on the table too soon will result in too many errors and possible failures to comply. The cyber assets should first be prioritized and then work from there. Prioritization should come from the industry with guidance from the various security sectors.

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group: Cleco Power</b>	<b>Group Representative: <i>Keith Comeaux</i></b> <b>Representative Phone: 318-838-3176</b> <b>Representative Email: keith.comeaux@cleco.com</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Terry Whitmore</i>	<i>Cleco Power</i>	<i>1</i>
<i>Raymond Savoie</i>	<i>Cleco Power</i>	<i>1</i>
<i>Michael Veillon</i>	<i>Cleco Power</i>	<i>1</i>
<i>Keith Comeaux</i>	<i>Cleco Power</i>	<i>1</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

---

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments: Responsible Entity, we would like to see clarification on this point. Today we would see it as the Control Area and in the future stemming from the Reliability model functions. If this is correct we would suggest making the language change for implementation to reflect that and make a change to the definition when the model is implemented.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments If the above were included, how long would each take to complete?

Comments It would take years due to cost issues, studies performed, planning efforts and

RFP's

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments This standards scope is broader than the current one and would like to see a phase-in period to implement the new standard.

\* What sanctions are to be attached for non-compliance?

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>Southern Company Services, Inc</i>		<b>Group Representative:</b> <b>Marc Butts</b> <b>Representative Phone:</b> 205-257-4839 <b>Representative Email:</b> mmbutts@southernco.com
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Marc Butts</i>	<i>Southern Company Services</i>	<i>1</i>
<i>Mike Oatts</i>	<i>Southern Company Services</i>	<i>1</i>
<i>Roger Lee</i>	<i>Southern Company Services</i>	<i>1</i>
<i>Jay Cribb</i>	<i>Southern Company Services</i>	<i>1</i>
<i>Frank Buttler</i>	<i>Southern Company Services</i>	<i>1</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments :

**Cyber Assets:** This definition applies only to systems or devices that use a network protocol Stack for communications. This statement seems to exclude most SCADA host to remote terminal unit communications, power plant control system bus communications, substation automation communications, etc. Therefore, the Critical Cyber Assets definition would seem to be broader than the Cyber Assets definition.

**Critical Cyber Assets:** The response of the drafting to the industry comments made on the Draft SAR Version 1 clearly recognizes the near term impracticality of meeting cyber security requirements for power plant control, remote terminal units, and other field devices. Placing such requirements in a standard with the hope that technologies will develop in a timely manner to meet some projected implementation schedule is unacceptable. The Critical Cyber Assets definition should specifically exclude power plant control, remote terminal units, substation automation control, protective relays, etc.

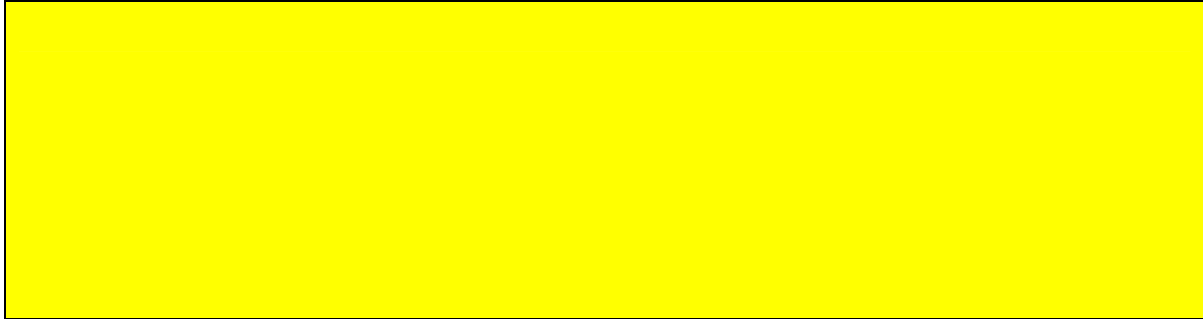
### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments --- Different assets have different requirements, so it depends on the exact asset. Would it be acceptable for a critical cyber asset to be offline continuously for 43 hours on August 14<sup>th</sup>? It really depends on the criticalness of the equipment.

I believe this question pertains more to Reliability than to Cyber Security.



**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments -- Again as in question #2, this sounds more related to Reliability than Cyber Security. If a Critical Cyber Asset is offline, then it is safe from a Cyber Security Standpoint. However, the stability of the Bulk Electric system may be jeopardized if it is offline.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments -- It should be required when encryption technology is commercially available say within 1-2 years. At that point, we feel that ICCP communications between control centers over the internet would be a priority candidate for encryption.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments --Technology is not there yet. It would also require an intensive costly infrastructure to implement.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments -- Depends on the type of equipment-private or public. This would be a lower priority candidate.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments -- Same as C. above, lower priority.

**e. If the above were included, how long would each take to complete?**

Comments -- Anywhere from 2-10 years.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments -- This is an availability issue and a Reliability issue more than a Cyber security issue. Redundancy does not necessarily mitigate cyber vulnerabilities. Two systems on the same network can be equally vulnerable, so redundancy does not necessarily equate to better security. Therefore, it should only be required if redundancy can be shown to improve security.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments -- Encryption should not be required until it is confirmed by testing and industry agrees it is required to meet security needs.

This Standard is much more wide-encompassing than the Urgent Action Standard. Therefore, it will need to provide ample lead time for all participants to implement any additional requirements.

The nuclear industry is already developing its own initiatives to perform Cyber Security assessments and measures at nuclear facilities. These are being addressed through the NRC and the Nuclear Energy Institute (NEI). Therefore, nuclear plant systems should be specifically excluded from the scope of this NERC standard.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Wayne R. Mackenzie
Organization	VELCO – Vermont Electric Power Co.
Industry Segment #	1
Telephone	802 770-6213
E-mail	<a href="mailto:wmackenzie@velco.com">wmackenzie@velco.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## **Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### **1. Do you agree with the definitions included in the SAR?**

No

Comments The existing definitions are reasonable. The term “bulk electric system functions” used in the Critical Cyber Assets definition should be clarified. This document is being interpreted by many users unfamiliar with the precise interpretation of this term. This definition alone sets the scope for inclusion or exclusion of many assets depending on the interpretation. National and Regional conference calls have previously spent a good deal of time on this issue in the Urgent Action Standard (with varied interpretations) so it seems reasonable to include it here even if it is a duplication of another NERC document. If there are regional differences then regions should be required to attach their definitions to this SAR.

### **6. Please enter any other comments you have regarding this SAR in the space below.**

Comments The SAR needs to be completed so that it does not leave islands of critical bulk transmission cyber assets that are not protected under this SAR. Market Systems, SCADA Masters, EMS systems, Generators, local control systems and ICCP systems where these systems cyber security failures may affect the reliable operation of the bulk transmission system need to be included. While the current definition could be interpreted to include all of these systems there are several comments to reduce the scope of this definition or move some systems into separate SARs. Any of the above systems (and some others) may need specific detail, but should remain part of this SAR insofar as they can negatively impact the reliability of the bulk transmission system through cyber security events.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



# Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>Allegheny Energy</i>	<b>Group Representative:</b> <i>Grant McDonald</i> <b>Representative Phone:</b> 724-830-5824 <b>Representative Email:</b> <i>jmcdon2@alleghenypower.com</i>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Grant McDonald</i>	<i>Allegheny Energy</i>	<i>1</i>
<i>Larry Duvall</i>	<i>Allegheny Energy</i>	<i>5</i>
<i>Bob Reeping</i>	<i>Allegheny Energy</i>	<i>3</i>

### Background Information:

### Notes to Industry Commenters:

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments:

- Cyber Assets/Critical Cyber Assets: A definition needs to be provided for “bulk electric system operation”. Also, suggest modifying the last sentence under Critical Cyber Assets to read “should be considered at a minimum” instead of “are included at a minimum”. There could be Cyber Assets that perform these functions that do not impact the reliability of bulk electric system operations. Each utility should have the responsibility to identify it’s own Critical Cyber Assets.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments:

- There should be no availability requirements in this SAR as availability is not directly related to cyber security. This is a reliability issue rather than a security issue. End-users and application-based working groups (NERC, ECAR, Reliability Coordinators, individual companies, etc.) should determine availability requirements.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments:

- Same comments as #2 above

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments: As per the definition of Critical Cyber Assets, this would not apply if it is not an IP stack.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments:

- This is a reliability issue rather than a security issue. End-users and application-based working groups (NERC, ECAR, Reliability Coordinators, individual companies, etc.) should determine redundancy requirements.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

- Substation RTU's should not be included as a Critical Cyber Asset unless they provide a means to which a compromise of the RTU would allow uncontrolled access to Critical Cyber Assets.
- Suggest including a clarification that market functions are excluded from the SAR.
- Critical Cyber Asset security measures, as mentioned in the standard, must be flexible enough to allow for differences in facility physical layouts, operational considerations, and geographic boundaries (i.e. substations, power stations, corporate centers).
- Suggest eliminating last paragraph of the Detailed Description section of the SAR (page SAR-4) starting with "Reliable data communications...". This paragraph is mixing reliability and security concerns. The elimination of this paragraph is consistent with our response to Questions 2 and 4 above. Furthermore, it appears that the last sentence of the paragraph "Where the data communications..." directly conflicts with the statement in Question 4 that the SAR does not require that SCADA or PCS communications be encrypted.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>MAPP Regional Reliability Council, assisted by the MAPP Operations Subcommittee (members listed below)</i>		<b>Group Representative:</b> <i>Lloyd Linke</i> <b>Representative Phone:</b> <i>(605) 882 - 7500</i> <b>Representative Email:</b> <i>lloyd@wapa.gov</i>
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>John Swanson</i>	<i>Nebraska Public Power District</i>	<i>2</i>
<i>Robert Coish</i>	<i>Manitoba Hydro Electricity Board</i>	<i>2</i>
<i>Paul Koskela</i>	<i>Minnesota Power</i>	<i>2</i>
<i>Larry Larson</i>	<i>Otter Tail Power</i>	<i>2</i>
<i>Darrick Moe</i>	<i>Western Area Power Administration</i>	<i>2</i>
<i>Dick Pursley</i>	<i>Great River Energy</i>	<i>2</i>
<i>W. Todd Gosnell</i>	<i>Omaha Public Power District</i>	<i>2</i>
<i>Martin Trence</i>	<i>Xcel Energy</i>	<i>2</i>
<i>Joe Knight</i>	<i>MAPPCOR</i>	<i>2</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

**The definition of “Critical Cyber Assets” requires refinement. First, the two sentences are somewhat conflicting in presenting a clear definition for this term. Next, the criticality of Cyber Assets will vary with location and application, therefore the level of risk associated shall vary as well. If the intent of this Standard is directed at removal of vulnerability from external threats, it should be better addressed. Along similar lines, if the focus is on particular layers of protocol, this should also be made clear.**

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments

Unless there are clear, uniform, industry based ( e.g. National Institute of Standards – NIST) guidelines that are available to use in development of Critical Cyber Asset availability, pursuit of this endeavor would be fruitless, due to the wide variety of Assets in use today.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers

Yes

No

Comments

Encryption will slow the communication speed of vital ICCP data between Reliability Coordinators and Control Area entities required to preserve Regional Reliability. At present thousands of values are updated via ICCP on a four-second basis, necessary for the Reliability Coordinators to monitor and validate Regional System Stability and provide enough time to act in mitigation of System Contingencies.

b. SCADA master station to RTU communications using peer-to-peer communications protocols

Yes

No

Comments

Most communications protocols used for this purpose encompass some form of encryption format, so no additional encryption techniques are required.

c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)

Yes

No

Comments

d. Data collection servers communications to substation IEDs

Yes

No

Comments

e. If the above were included, how long would each take to complete?

Comments

Unknown at this time, due to the diversity of Cyber Asset infrastructures in place owned by the Region's Members

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes



No

Comments

**Redundancy requirements should be left to the Cyber Asset Owner's own risk analysis of respective infrastructures, and their subsequent System impact due to failure.**

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

**The requirements should be set out in this SAR in a clear manner. Industry Standards based risk analysis processes must be incorporated into this standard, as a guide for Cyber Asset Owners to provide prudent and justifiable means to determine the level of risk and subsequent necessary protective measures to be applied to their Cyber Assets.**

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name            Alan Johnson  
Organization    Mirant Corporation  
Industry Segment # 6  
Telephone       678-579-3108  
E-mail           [alan.r.johnson@mirant.com](mailto:alan.r.johnson@mirant.com)

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

- Yes  
 No

Comments: Think that a couple of the definitions are still too vague. They leave too much open to interpretation. For example, under the definition of Critical Cyber Assets, what entity determines whether the loss of a Cyber Asset could adversely impact the reliability of bulk system operations? Is it the RA, or does the RA have to accept the determination of each entity? Regarding the definition of "Cyber Asset", believe that either a definition of "bulk electric system" or a reference to a source of the definition should be included. In addition, wondering why the definition applies only to systems or devices that use a network protocol stack for communications? Assume this is in reference to using TCP/IP to communicate over the internet. Don't non-internet communication methods need to be secured as well?

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

- Yes  
 No

Comments

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

- Yes  
 No

Comments: Don't think it's necessary to address the availability of critical cyber assets within the standard. If an asset is defined as a critical cyber asset, then by definition, it must be available to maximize the reliability of the bulk power system, which in turn is designed for a 1 day in ten-year loss of load criteria. It should be left to the asset owners to assure the integrity of the design standard.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

- Yes  
 No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

- Yes  
 No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

- Yes  
 No

Comments

**d. Data collection servers communications to substation IEDs**

- Yes  
 No

Comments

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

- Yes  
 No

Comments: The SAR and the resulting standard should only require the protection of the critical cyber assets. Probably need to define "protection" (is this the 99.5% availability per annum?) as there are different possible levels of protection, which gets into the redundancy issue. Once the required level of protection is defined, an entity should be able to decide how said level is accomplished. Maybe it's through redundancy; maybe it's accomplished some other way.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments: Although still have some concerns, believe this SAR is ready to move to the standard development stage where more of the details can be worked out.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>NPCC CP9 Reliability Standards Working Group</i>		<b>Group Representative:</b> <i>Guy V. Zito (Chair)</i> <b>Representative Phone:</b> 212-840-1070 <b>Representative Email:</b> <i>gzito@npcc.org</i>
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Roger Champagne</i>	<i>TransEnergie (Quebec)</i>	<i>1</i>
<i>Ralph Rufrano</i>	<i>New York Power Authority</i>	<i>1</i>
<i>Dan Stosick</i>	<i>ISO New England</i>	<i>2</i>
<i>David Kiguel</i>	<i>Hydro One Networks</i>	<i>1</i>
<i>Barry Gee</i>	<i>National Grid US</i>	<i>1</i>
<i>Al Miller</i>	<i>The IMO (Ontario)</i>	<i>2</i>
<i>Guy Zito</i>	<i>Northeast Power Coordinating Council</i>	<i>2</i>
<i>Kathleen Goodman</i>	<i>ISO New England</i>	<i>2</i>
<i>Tony Elacqua</i>	<i>New York ISO</i>	<i>2</i>

Background Information:

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.



## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments:

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments; Does this requirement belong in a Cyber-Security Standard or a Reliability-Communication Standard? NPCC feels that if this ultimately is retained that 99.5% is too low or insufficient.

NPCC feels that entities who rely on Data Communication provided by third parties that non-compliance due to third party should not be assessed as such but be recognized and dealt with through contractual agreements and revisions thereof.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments: Encryption Standards can run on top of existing ICCP. Integrity and authentication are needed but confidentiality is not always necessary.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

**e. If the above were included, how long would each take to complete?**

Comments: NPCC feels that it is vital that the data being referred to has integrity ( i.e. not corrupt and has a trusted source). NPCC feels that encrypting does not sufficiently accomplish this. NPCC feels encryption, depending on where it may be proposed would represent a costly and ineffective solution.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

NPCC feels the question, as written, is subject to a number of different interpretation.

NPCC would like the SAR drafting team to clarify its request. The interpretations of this question may mislead the drafting team to a false result.

6. Please enter any other comments you have regarding this SAR in the space below.

Comments:

NPCC Suggests the following change be made to the following Sections to read as follows;

**Brief Description:** This standard is based on the Urgent Action Cyber Security Standard that was adopted by the NERC Board of Trustees on August 13, 2003. The standard requires that critical cyber assets related to the *real-time* reliable operation of the bulk electric systems are identified and protected. Requirements will be included in the standard for responsible entities to create and implement *security* programs and procedures, perform on-going effective assessments, and implement appropriate and technically feasible improvements necessary to meet the requirements of this standard *to insure cyber-security*. Security programs include the responsible entity's policies, standards, procedures, training, and auditing controls for the implementation of this standard. The standard is intended to replace the Urgent Action Cyber Security Standard.

**Detailed Description: (starting with 2<sup>nd</sup> paragraph)**

Reliable bulk electric system operations are highly interdependent, and the failure of key/critical elements of the generation, transmission, or grid management system can potentially compromise the reliable operation of major portions of the regional grid. Similarly, 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. Because of this ~~mutual vulnerability and~~ interdependence, it is necessary to safeguard the critical cyber assets that support bulk electric system operations ~~by establishing standards to provide a level of assurance that even a single compromise of a critical cyber asset does not compromise system security, and, thus, risk grid or market failure.~~

This standard shall primarily focus on electronic systems including: hardware, software, data, related communications networks, and control systems as they impact bulk electric system operations ~~and personnel~~. *Also, personnel shall be addressed for 1) access to critical assets, 2) training for their access to critical assets and 3) background screening as legally and contractually feasible.* In addition, physical security shall be addressed to the extent that it is necessary to assure a secure physical environment for critical cyber assets and their operation. If a network consisting of critical cyber assets also includes non-critical cyber assets, those non-critical cyber assets must comply with the requirements of this standard. ~~This standard shall require that third party providers of services used to ensure reliability (e.g. Interchange Distribution Calculator data) must comply with the standard for systems providing those services.~~ This standard shall require that the responsible entities that must comply with this standard identify and protect themselves from threats from interconnected cyber systems.

This standard shall require that entities identify and protect critical cyber assets related to the reliable operation of the bulk electric system and have an ongoing program in place to ensure their protection. This program must at a minimum, meet the requirements set forth in the standard as they relate to ~~governance~~ *program administration*, planning, prevention, operations, incident response, and continuity of operations. As a result, this program will mitigate the effect of acts of malicious or *suspected to be of malicious* ~~unknown~~-origin that could cause wide-ranging, harmful impact to the bulk electric system.

**Detailed Description (6<sup>th</sup> paragraph);**

Reliable and secure data communications networks are key to continuity of operational control and ongoing management of critical cyber assets. Some organizations own and operate their own data communications infrastructure, others acquire network services from the Telecommunications Sector, and some meld both private and public resources to create the data communications capabilities necessary to reliably operate and control critical cyber assets. ~~Whether the means of data communications are of private or public origin, be they physical or logical in operation, it is incumbent upon owners and/or operators of critical cyber assets to design and provision data communications capabilities to be reliably available. Accordingly, data communication systems joining two or more distinct electronic security perimeters must be provisioned to a level of reliability at least equal to 99.5% availability per annum.~~ Where the data communications capability utilizes shared public network resources (e.g., POTS, frame relay, the Internet, etc.), using either leased-permanent or temporary dial-up methods, all data must be **transmitted with encrypted** appropriate measures ~~must be taken~~ to ensure authorized use of the data communications capability through authentication, confidentiality, integrity, and (as appropriate) non-repudiation.

**Definitions Section: (NPCC Suggests the existing language read as follows)**

Security Incident: Any physical or cyber event of ~~possible~~ malicious or **suspected to be of malicious** ~~unknown~~ origin that disrupts the functional operation of a critical cyber asset or compromises the electronic or physical security perimeters.

## FRCC Comments 1/21/04

### Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with "Standard Comments" in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

#### **SAR Commenter Information (For Individual Commenters)**

Name Patti Metro on behalf of FRCC members

Organization Florida Reliability Coordinating Council (FRCC)

Industry Segment #

Telephone 813-289-5644

E-mail [pmetro@frcc.com](mailto:pmetro@frcc.com)

#### **Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial Regulatory or other Govt. Entities

**FRCC Comments 1/21/04**

**Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>FRCC</i>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Patti Metro</i>	<i>FRCC</i>	<i>2</i>
<i>Linda Campbell</i>	<i>FRCC</i>	<i>2</i>
<i>Alan Gale</i>	<i>City of Tallahassee</i>	<i>5</i>
<i>Tim Beyrle</i>	<i>Utilities Commission New Smyrna Beach</i>	<i>3</i>
<i>Roger Westphal</i>	<i>Gainesville Regional Utilities</i>	<i>3</i>
<i>John Giddens</i>	<i>Reedy Creek Improvement District</i>	<i>3</i>
<i>Ray Crooks</i>	<i>Reedy Creek Improvement District</i>	<i>6</i>
<i>Jeff Nicely</i>	<i>Reedy Creek Improvement District</i>	<i>4</i>
<i>Bernie Budnik</i>	<i>Reedy Creek Improvement District</i>	<i>5</i>
<i>Ron Donahey</i>	<i>Tampa Electric Company</i>	<i>3</i>
<i>Jose Quintas</i>	<i>Tampa Electric Company</i>	<i>6</i>
<i>Paul McClay</i>	<i>Tampa Electric Company</i>	<i>3</i>
<i>John Currier</i>	<i>Tampa Electric Company</i>	<i>5</i>
<i>Herman Dyal</i>	<i>Clay Electric Cooperative</i>	<i>3</i>
<i>Bob Remley</i>	<i>Clay Electric Cooperative</i>	<i>3</i>
<i>Wayne Lewis</i>	<i>Progress Energy</i>	<i>5</i>
<i>T.C. Thomas</i>	<i>Progress Energy</i>	<i>5</i>
<i>Steve Wallace</i>	<i>Seminole Electric Cooperative</i>	<i>4</i>
<i>Tom Turke</i>	<i>Seminole Electric Cooperative</i>	<i>4</i>
<i>Jim Larsen</i>	<i>Seminole Electric Cooperative</i>	<i>4</i>
<i>Bill Cross</i>	<i>Seminole Electric Cooperative</i>	<i>4</i>
<i>Paul Elwing</i>	<i>Lakeland Electric</i>	<i>5</i>
<i>Mark Bennett</i>	<i>Gainesville Regional Utilities</i>	<i>5</i>

## FRCC Comments 1/21/04

### Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

---

<b>Joel Degrada</b>	<b>Florida Power and Light</b>	<b>1</b>
<b>Ray Falcon</b>	<b>Florida Power and Light</b>	<b>1</b>
<b>Ted Hobson</b>	<b>JEA</b>	<b>1</b>
<b>Garry Baker</b>	<b>JEA</b>	<b>1</b>
<b>Richard Gilbert</b>	<b>Lakeland Electric</b>	<b>3</b>
<b>Bill May</b>	<b>Florida Municipal Power Agency FMPA</b>	<b>4</b>

#### Background Information:

#### Notes to Industry Commenters:

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

#### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments:

The basis for the entire standard setting process is reliable operation and planning of the Bulk Electric System. Until the industry clearly and concisely defines, Bulk Electric System, this process is burdened with questions of applicability.

One of the problems with the urgent action standard is that the definitions required too much interpretation. While the new SAR definitions are improved, we feel that the definition of Critical Cyber Asset needs further clarity to ensure that it is consistently applied across the industry. We suggest referencing a methodology that would be created by each Region based on factors such as transmission voltage, % of load, size of generating units. This type of methodology would be used to determine which assets if compromised would have an impact on reliable operations of the system. It would answer such questions as:

- Power plant control systems are critical cyber assets, but how does an organization make a determination of which generating units are applicable?
- What is an appropriate amount of load shedding that would be considered a Critical Cyber Asset?
- Substation automation control systems that have an impact to the reliability of bulk electric systems are covered under the standard, but there is no guideline for an organization to follow to identify which substations might impact reliability.

As to inclusion of power plant control systems, while eventually these systems might belong in the standard, we do not agree that they should be included in this standard since the intent is to replace the Urgent Action Standard as soon as possible. However, if the power plant systems are included, we feel that consideration must be given for older legacy systems within power plants where upgrades or specific controls may not be technically or financially feasible. These systems should still conform to some level of security, but this may be through compensating controls such as network isolation, rather than the full set of requirements.

In addition, there should be a comma after "automatic generation control" to separate it from "load shedding" in the definition of Critical Cyber Assets

In the definition of Cyber Asset, the use of the term network protocol stack is vague. If network protocol stack is meant to be TCP-IP, the definition should be modified to include this specific protocol stack.

The following re-wording on the definition of Security Incident is provided for consideration: Any physical or cyber event of malicious or **possibly suspect** origin that disrupts the functional operation of a critical cyber asset or compromises the electronic or physical security perimeters.



**2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments: The scope of this SAR and future standard should be limited to cyber-security requirements. Items such as data communications availability, and availability and redundancy of critical cyber assets address the design and engineering of the system and network; therefore, additional standards should be developed to address these items.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments: The scope of this SAR and future standard should be limited to cyber-security requirements. Items such as data communications availability, and availability and redundancy of critical cyber assets address the design and engineering of the system and network; therefore, additional standards should be developed to address these items.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

FRCC Comments: There is disparity between the questions being asked in this section and the actual Detailed Description in the associated SAR. The following excerpt from the SAR already indicates the inclusion of the technology described in this section: "Where the data communications capability utilizes shared public network resources (e.g., POTS, frame relay, the Internet, etc.), using either leased-permanent or temporary dial-up methods, all data must be encrypted to ensure authorized use of the data communications capability through authentication, confidentiality, integrity, and (as appropriate) non-repudiation." As indicated below FRCC commenters do not think there should be a requirement for encryption of SCADA or PCS communications. In addition, any reference to encryption should be removed from the SAR scope and future standard until proven technology is available.

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments: See Above

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments: See Above

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments: See Above

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments: See Above

If the above were included, how long would each take to complete?

Comments: The time-lines provided are dependent on the development of appropriate technology.

a: ICCP – industry wide, 6 to 12 months for basic hardware point to point (IPSEC VPN). Secure ICCP 18 to 24 months.

b: Peer to peer would require R&D and product development, we are not aware of existing technology, we expect 24 to 36 months.

c: IPSEC VPN 12 to 24 months for implementation. Encryption within DNP3 24 to 36 months. Other products/solutions 24 to 36 months???

d : 12 to 24 months.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments: The scope of this SAR and future standard should be limited to cyber-security requirements. Items such as data communications availability, and availability and redundancy of critical cyber assets address the design and engineering of the system and network; therefore, additional standards should be developed to address these items.

As a part of ongoing activities related to the blackout investigation, NERC will likely address redundancy through standards for backup control plans. These will likely be much more stringent, and will possibly conflict with recovery and redundancy requirements in this standard.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments:

**Comments Regarding Reliability Functions Portion of SAR:**

In the following excerpt "...Similarly, 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..." if this is included in the SAR shouldn't the Market Operator and PSE be included as applicable entities?

Please provide clarification on why this SAR is applicable to the LSE.

**Comments Regarding Applicable Reliability Principles:**

Since the SAR deals with information availability in a secure manner. It has to get to the System Operators, therefore, should include #3.

Since the SAR does not address or impact the System Operators training, qualification, responsibility or authority. Even if a background check is required, it does not affect the principles listed, therefore, should NOT include #6.

**Comments Regarding Detailed Description Portion of SAR:**

There are several terms used in this portion of the document that require more clarity and are technical terms that should either be included in the SAR or a supplemental glossary of terms:

- non-repudiation
- In the following excerpt: "... set forth in the standard as they relate to governance..." what is the intent with regard to governance?
- In the following excerpt "...and control systems as they impact bulk electric system operations and personnel ..." what is meant by personnel?

It is important that this SAR focus on cyber security issues related to transmission SCADA systems. The addition of redundancy, availability, backup and recovery should be developed in specific standards on those topics. If there is a continuous effort to add more requirements and expand the scope of Cyber Security Standard, the SAR process and the Standards drafting will be prolonged and it will be difficult to gain an industry consensus. If it is the intent of NERC and the drafting team to include all of the requirements that were discussed on this comment form into one standard, then the standard should be renamed to Cyber Operation Control Standards to reflect a scope that is beyond cyber security.

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	John G. Maguire
Organization	PJM Interconnection, LLC
Industry Segment #	2
Telephone	610-666-4420
E-mail	<a href="mailto:maguij@pjm.com">maguij@pjm.com</a>

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>PJM</i>	<b>Group Representative:</b> <i>John Maguire</i> <b>Representative Phone:</b> 610-666-4420 <b>Representative Email:</b> maguij@pjm.com	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>John Maguire</i>	<i>PJM Interconnection, LLC</i>	<i>2</i>
<i>Bruce Balmat</i>	<i>PJM Interconnection, LLC</i>	<i>2</i>
<i>James Cella</i>	<i>PJM Interconnection, LLC</i>	<i>2</i>
<i>Joseph Willson</i>	<i>PJM Interconnection, LLC</i>	<i>2</i>
<i>Michele Dickinson</i>	<i>PJM Interconnection, LLC</i>	<i>2</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments Security Incident: Even if the origin is not "malicious or unknown", and even if it does not have a security impact, it should be handled through proper incident response. Every incident (especially cyber) should be responded to, as due diligence to verify the integrity of the infrastructure. The term "Security Incident" should be removed, and replaced by just "Incident"; and updated as described above.

Cyber Assets: The line "This definition applies only to systems or devices that use a network protocol stack for communications" should be removed. There is little prescription for implementing cyber security in the Urgent Action Standard; and to be an industry standard, it is unlikely the permanent standard would pass if it was overly prescriptive; thus, applying cyber security management processes to every asset must be enforced. In addition, network security should not be the limit to the definition's scope. Assuming that devices with non-standard communication protocols need not comply, is exactly the opposite of what is necessary... Devices using communication protocols that cannot implement current network security techniques should be scrutinized above and beyond devices that can implement current network security techniques. This definition gives legacy devices a "Get Out of Jail Free" card. This cannot be the industry's intention.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments A specific uptime requirement is not expressly a security concern. The security concern is "availability". As this is a scope document, the language should be written to indicate that security requirements in the standard should not hinder the operational performance or operational availability requirements of the critical cyber assets, and in the SAR should be scoped as such.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments As with #2 above, this is a scope document, the language should be written to indicate that security requirements in the standard should not hinder the operational performance or operational availability requirements of the critical cyber assets, and in the SAR should be scoped as such. The measure of compliance should be indicated through specific and tested business continuity plans, redundancy of devices, hot backup sites, etc. Verifying availability through penetration or stress testing only shows the device's point-in-time durability against known attacks. BCP and redundancy can theoretically withstand any N-minus-1 attack.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments If this is supposed to be an industry standard, the SAR should not be scoped to include specific requirements for a subset of the entities that are to be in compliance. ICCP is a particular communication protocol for a specific purpose, used by specific entities. Regulating a technology should not be a goal of a broad baseline industry standard. Confidentiality is the tenet to be assured, not encryption; and in the control system arena confidentiality takes a back-seat to data integrity and availability.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments Regulating a technology should not be a goal of a broad baseline industry standard. Confidentiality is the tenet to be assured, not encryption; and in the control system arena confidentiality takes a back-seat to data integrity and availability.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments Regulating a technology should not be a goal of a broad baseline industry standard. Confidentiality is the tenet to be assured, not encryption; and in the control system arena confidentiality takes a back-seat to data integrity and availability.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments Regulating a technology should not be a goal of a broad baseline industry standard. Confidentiality is the tenet to be assured, not encryption; and in the control system arena confidentiality takes a back-seat to data integrity and availability.

**e. If the above were included, how long would each take to complete?**

Comments Approximately two years after the technology became available, to ensure the practical integrity of the technology.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments Redundancy as it applies to the physical assurance of the availability of systems. Essentially, in a black-hole scenario, the ability to recover is essential to the bulk-electric system; in this case, redundancy would be the only way to ensure availability.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments The entire last paragraph of the Detailed Description should be removed as, in conjunction with comments above, it does not contribute to the scope of the standard.



## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>ISO/RTO Council - Standards Review Committee</i>		<b>Group Representative:</b> <i>Karl Tammar</i> <b>Representative Phone:</b> 518-356-6205 <b>Representative Email:</b> ktammar@nyiso.com
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Dale McMaster</i>	<i>AESO</i>	<i>2</i>
<i>Ed Riley</i>	<i>CAISO</i>	<i>2</i>
<i>Sam Jones</i>	<i>ERCOT</i>	<i>2</i>
<i>Don Tench</i>	<i>IMO</i>	<i>2</i>
<i>Dave LaPlante</i>	<i>ISO-NE</i>	<i>2</i>
<i>Bill Phillips</i>	<i>MISO</i>	<i>2</i>
<i>Karl Tammar</i>	<i>NYISO</i>	<i>2</i>
<i>Bruce Balmat</i>	<i>PJM</i>	<i>2</i>
<i>Carl Monroe</i>	<i>SPP</i>	<i>2</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments    No Comments

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments Where availability is one of the three major concepts of information security (e.g. Confidentiality, Integrity, and Availability (CIA)), broad reliability requirements and metrics do not belong in this security standard. Due to the nature of the industry, there are many different scenarios where loss of data communications is not due to any malicious event. One example was the loss of communications due to hurricane Isabelle.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate). While the relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link. It is critical to remember that "appropriate" or "adequate" levels of availability

depend on the context. Based on the context of this security standard, it is not appropriate to include availability.

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments The Cyber Security Standard should not mandate a particular technology such as encryption. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments The Cyber Security Standard should not mandate a particular technology. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments The Cyber Security Standard should not mandate a particular technology. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments The Cyber Security Standard should not mandate a particular technology. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments Depending on a responsible entities' environment, redundancy may not be the most effective solution. The standard should mandate security requirements, not technical solutions.

**6. Please enter any other comments you have regarding this SAR in the space below.**

1. Comments Under “Detailed Description”, 3<sup>rd</sup> paragraph, 1<sup>st</sup> sentence – in order to ensure SCADA monitoring functionality is included, revise to: “This standard shall primarily focus on electronic systems including: hardware, software, data, related communications networks and monitoring and control systems...”
2. Under “Detailed Description”, 3<sup>rd</sup> paragraph, delete the sentence beginning “This standard shall require that third-party...” as it is too limiting and add to the last sentence “This standard shall require that the responsible entities that must comply with the standard identify and protect themselves from threats from other connected cyber systems, including those provided by contractors and service providers.”
3. Delete the last paragraph entirely, as it adds nothing to the scope or intent of the SAR. Further, it includes a level of detail that is inappropriate for a SAR, but would be more appropriate in the standard itself.

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	MARK A. CREECH
Organization	Tennessee Valley Authority
Industry Segment #	
Telephone	423-751-6264
E-mail	macreech@tva.gov

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group: <i>Tennessee Valley Authority</i></b>		<b>Group Representative: Representative Phone: Representative Email:</b>
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Russell Robertson</i>	<i>TVA</i>	
<i>Ruth Hunt</i>	<i>TVA</i>	

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments Availability could be significant critical system failure

### 4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:

- a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control



**centers**

Yes

No

Comments This statement depends on the vendor software

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments This statement depends on the security channel, if public or not.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments This statement depends on the security channel, if public or not.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments This statement depends on the security channel, if public or not.

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Gerald Rheault
Organization	Manitoba Hydro
Industry Segment #	1,3,5,6
Telephone	204-487-5423
E-mail	<a href="mailto:gnrheault@hydro.mb.ca">gnrheault@hydro.mb.ca</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative: <i>Gerald Rheault</i></b> <b>Representative Phone: 204-487-5423</b> <b>Representative Email: gnrheault@hydro.mb.ca</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Greg Fraser</i>	<i>Manitoba Hydro</i>	<i>1</i>
<i>Doug Chapman</i>	<i>Manitoba Hydro</i>	<i>1</i>
<i>Murray Matiowsky</i>	<i>Manitoba Hydro</i>	<i>1</i>
<i>Barry Malowanchuk</i>	<i>Manitoba Hydro</i>	<i>1</i>
<i>Ron Dacombe</i>	<i>Manitoba Hydro</i>	<i>3</i>
<i>Gerald Koroscil</i>	<i>Manitoba Hydro</i>	<i>5</i>
<i>Jacqueline Collett</i>	<i>Manitoba Hydro</i>	<i>1</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

**1. Do you agree with the definitions included in the SAR?**

Yes

No

Cyber assets:

Must include regional and area control centres as per Urgent Action Cyber Security Standard implementation regardless of the technology used within those control centres.

In the second sentence of this definition the words “network protocol stack” should be changed to “network layer protocol”.

Agree with the intent of the second sentence to limit, at this time, the scope of the proposed cyber standard to externally vulnerable networks. However, physical barriers to external access, such as isolated organization-owned and operated communications systems and networks, should provide compliance with the proposed cyber security standard.

All the above comments would be better included in the detailed description rather than in this definition. This would permit a clearer definition and allow a separate implementation program which could be revised in the future without changing the basic definition of cyber asset.

Critical Cyber Assets:

There should be direction given to the standards drafting team to clarify by definition or reference to other NERC documents what is included in “...impact the reliability of the reliability of the bulk electric system.” i.e. networked 110 kV lines, generators greater than xx MW, etc.

The responsible entity should determine their list of critical assets of the bulk electric system subject to review by the reliability region.

“Black start” would be better described by “black start capability”.

“Voltage stability” should be included in the list of functions.

Remote access must be included in the scope of the proposed cyber security standard.

Security incident:

Reporting events of “unknown origin” will result in numerous and perhaps needless reports for systems including communication systems provided by other suppliers or systems in remote locations which take considerable time to investigate. “Unknown origin” events resulting in a functional loss to a bulk electric system component will be reported via a normal operations report.

**2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments

Manitoba Hydro questions the basis for 99.5% availability (43 hours per year unavailable) of the communications assets? How was this number arrived at? Availability is a performance indicator and not security, so Manitoba Hydro has difficulty in seeing the relevance of this availability value in this SAR.

Within the context of this value, is it preferable to have few longer duration outages, or many short duration outages. The impacts of the outage of the communication systems is important; sometimes the equipment/systems within the secure parameter will continue to operate satisfactorily after the loss of the communication system whereas in other designs, loss of the communication system will lead to undesirable or unsatisfactory responses of the equipment within the secure perimeter. The requirement for a reliable and secure communication system should be predicated on these factors.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments

Manitoba Hydro believes that because of the variety of different critical cyber systems referenced here, it would be very difficult to define a common availability value for all the different critical cyber systems. The most important requirement is to provide a level of reliability such that even a single compromise of a critical cyber asset will not compromise system security. New critical cyber facilities should be designed to a level of robustness, fault tolerance, security, and criticality that will ensure that reliability of the bulk electric system is not compromised. Existing systems should be modified to meet this same level of security within a clearly defined reasonable time horizon subsequent to implementation of the Standard. Also, as stated above in 2, we believe that availability is a performance indicator and is not relevant in defining the cyber security requirements.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers

Yes

No

Comments The use of encryption should not be added as a requirement to this SAR if the

entity uses dedicated communications systems which are physically isolated from external influences. For an entity using a shared public network resource (eg POTS, frame relay, the internet, etc), using either leased-permanent or temporary dial-up methods, all data should be encrypted to protect the data from being tampered with and ensure the security of the communication. Authorized use of the data communications capability must be ensured through authentication, confidentiality and integrity. The computing systems generally used in present SCADA or PCS communications would be inadequate to satisfy the data transfer and scan rates required in the operating environment, if encryption was required. Encryption would greatly increase the security of the data being monitored and transmitted, but for most existing systems, the cost to increase the computing power of the hardware would be prohibitive. Therefore encryption should be added to the Standard, only for communication systems which use the public network.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments +same as a).

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments same as a).

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments same as a).

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments The SAR states that the critical cyber assets that support bulk electric system operations should be safeguarded by establishing standards “to provide a level of assurance that even a single compromise of a critical cyber asset does not compromise system security, and thus, risk grid or market failure”. The SAR should be flexible enough to allow this criteria to be met in any way possible including redundancy if required. This will allow entities to implement solutions which are both cost effective and synchronized with their existing facilities and systems. However, redundancy should be incorporated if it is the best solution to meet the criteria.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments High reliability between electronic security perimeters should be required only for critical cyber assets. Non-critical cyber assets (for example, remote monitoring with no control capability or internal station control systems) that do not use public communications media should not be subjected to the same mandated security and documentation requirements.

Cyber assets within a generating station or substation that do not communicate outside of that station for control purposes should only require a physical security perimeter and a low level electronic security perimeter (password etc) without extensive documentation requirements.

Direction to the standard drafting team on the cyber security standard implementation should be included in the SAR. New purchased systems or upgraded systems must comply once the standard is approved. For existing systems, a proposed implementation timeline, before applying penalties, should be suggested for the standards drafting team, since systems upgrade costs for the responsible entity could be considerable and require a multi-year implementation.

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group: WECC EMSWG (partial group)</b>	<b>Group Representative: Jim Hiebert Representative Phone: (916) 608-1254 Representative Email: jhiebert@caiso.com</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<b>Jim Hiebert</b>	<b>CAISO</b>	<b>2</b>
<b>Erika Ferguson</b>	<b>Idaho Power Company</b>	<b>1</b>
<b>Chuck Nichols</b>	<b>BC Hydro</b>	<b>1</b>
<b>Alan Chang</b>	<b>BC Hydro</b>	<b>1</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

- Yes  
 No

Comments The definition of 'Cyber Assets' needs further clarification. The definition seems somewhat vague.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

- Yes  
 No

Comments Broad reliability requirements and metrics do not belong in this security standard. Due to the nature of the industry, there are many different scenarios where loss of data communications is not due to any malicious event. One example was the loss of communications due to hurricane Isabelle.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

- Yes  
 No

Comments For the scope of this standard, availability of critical cyber assets should only be included for devices and/or applications that are directly related to cyber security (e.g., firewalls, intrusion detection devices, etc.) technologies. Reliability of all critical cyber assets should not be addressed in this standard.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

- Yes  
 No

Comments We agree with the intent to provide secure (encrypted) communications for ICCP; however, this assumes that a product to encrypt ICCP communications is fully designed, tested, and readily available.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

- Yes  
 No

Comments Most RTU communications using peer-to-peer or "bit oriented" protocols utilize RS232 communications, voice circuits, tone telemetry, etc. The cost of implementing encryption on these systems may be prohibitive. If the communications takes place over an easily accessible public network then the owner should consider upgrading the system to IP based communication and include encryption.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

- Yes  
 No

Comments Particular priority should be given to SCADA master stations communicating over a public network to RTU's (especially SCADA master stations sending "control" signals to RTU's).

**d. Data collection servers communications to substation IEDs**

- Yes  
 No

Comments Further clarification of data collection servers is required. Are these the relay devices and are they communicating using TCP/IP? Over public network (Internet)? Are these devices used for control purposes? If the answer to these is "yes" then these should be considered for encryption.

**e. If the above were included, how long would each take to complete?**

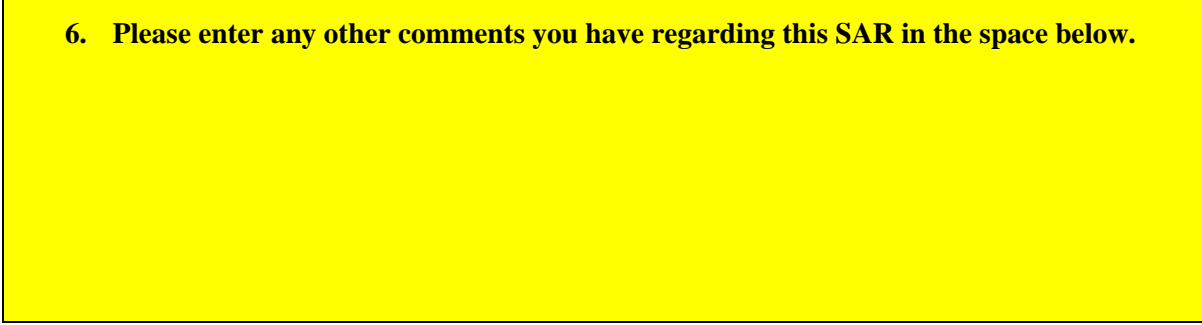
Comments No comment.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

- Yes  
 No

Comments Depending on a responsible entities' environment, redundancy may not be the most effective solution. The standard should mandate security requirements, not technical solutions.

**6. Please enter any other comments you have regarding this SAR in the space below.**



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>Great Plains Energy (GPE) and it's susidiary Kansas City Power &amp; Light (KCPL) Cyber Security Task Force</i>		<b>Group Representative:</b> <i>David M. McCoy</i> <b>Representative Phone:</b> (816) 420-4707 <b>Representative Email:</b> david.mccoy@gp-power.com
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Bob Brewer</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Pat Brown</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Gerry Burrows</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Stephen Diebold</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Joe Doetzl</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Larry Dolci</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Steve Easley</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Brad English</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Kenny Geier</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Scott Harris</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>David McCoy</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Judy Petroll</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>
<i>Alana Pierce</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Trudy Smith</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Ron Spicer</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Richard Spring</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Chuck Tickles</i>	<i>GPE</i>	<i>1,3 &amp; 5</i>
<i>Rogers Tuck</i>	<i>GPE</i>	<i>1, 3 &amp; 5</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

**1. Do you agree with the definitions included in the SAR?**

Yes

No

**Comments:** YES, however, we need clarification on the meaning of “bulk electric system functions” and of “power plant control”. Does “bulk electric system functions” mean “functions related to the high voltage electric system” or does it mean “a lot of electric system functions”? Does “power plant control” mean plant Distributed Control Systems (DCS’s) or the Energy Management Systems (EMS’s) that perform automatic generation control (AGC) functions?

2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

**Comments:**

3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

**Comments:** YES, but we would suggest using the availability of all critical functions as the measure. Many critical cyber assets will perform both critical and non-critical functions. The availability measure should be based on only the critical functions. We suggest that all critical functions should be available 99.5% of the time. For the purposes of calculating availability, if any critical function were missing, then the critical cyber asset would be considered not available.

4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:

a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers

Yes

No

**Comments:** YES, if it is a "critical" communications implementation. In general, the electrical system impact of the loss or compromise of SCADA type data (field information and device control requests) appears to be dependent on:

- The type of communication that is occurring (control request compromise is more severe than data compromise)
- The characteristics of the devices being communicated about (types of device, voltage levels, electrical system locations, etc.)
- The magnitude of data being communicated over a particular communication path

One possible approach would be to classify any communications implementation as "critical" if it carried control requests on power switching devices (eg. breakers) at 161 kV or above. Then encryption would be required only of "critical" communications implementations.



**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

**Comments:** Do you mean by "Peer to peer communications" those that are not network protocol stack communications? If so, YES, if it is a "critical" communications implementation. However, we see this as of less importance for the older, less common protocols and of more importance for the more common protocols, especially DNP

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

**Comments:** YES, if it is a "critical" communications implementation.

**d. Data collection servers communications to substation IEDs**

Yes

No

**Comments:** YES, if it is a "critical" communications implementation and if the communications goes out of the substation perimeter itself. Data could intentionally "leave" the substation perimeter over a specific communications path or could unintentionally "leak" because of the use of a wireless network. Both of these conditions, and any others like them, should be protected by encryption.

**e. If the above were included, how long would each take to complete?**

**Comments:**

- a. We do this routinely already on "critical" communications implementations
- b. Potentially a major effort (several years) and might imply RTU changeout
- c. We will do this as a matter of policy on "critical" communications implementations
- d. We would encrypt outside the substation perimeter as a matter of policy for "critical" communications implementations

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

**Comments:** In our opinion, availability of the critical cyber asset is the goal and redundancy (in its various forms) is one of the means of achieving that availability. We would prefer to see availability requirements specified and be given the flexibility to meet the requirements using whatever solution we deem best. Presumably, if a company can meet the availability requirements, on a continuing basis, year after year, that in itself demonstrates that they are devoting sufficient resources to the problem.

In our view, the above strategy works for the “production” critical cyber asset. In the case of a “backup “ critical cyber asset, however, it seems very appropriate to explicitly specify that a backup system exist and be tested on a routine basis.

**6. Please enter any other comments you have regarding this SAR in the space below.**

**Comments:**

**Reliability Functions**

Why are the “Purchasing-Selling Entity” and “Market Operator” functions not included? The 2nd paragraph of the Detailed Description seems to indicate that they should be covered.

**Other:**

- a) 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.
- b) The standards need to clearly address 3rd party owners of critical assets and 3rd party contractors.
- c) 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.
- d) 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.
- e) 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?

- f) 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.
  
- g) 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.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Kathleen Goodman
Organization	ISO New England Inc.
Industry Segment #	2
Telephone	(413) 535-4111
E-mail	<a href="mailto:kgoodman@iso-ne.com">kgoodman@iso-ne.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

**1. Do you agree with the definitions included in the SAR?**

Yes

No

Comments

Cyber Assets: Delete the sentence, "This definition applies only to systems or devices that use a network protocol stack for communications." As it is unnecessarily detailed and limiting.

Security Incident: Change to read as, "Any physical or cyber event of malicious or suspected to be malicious origin that disrupts the functional operation of a critical cyber asset or compromises the electronic or physical security perimeters."

**2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments

Where availability is one of the three major concepts of information security (e.g. Confidentiality, Integrity, and Availability (CIA)), broad reliability requirements and metrics do not belong in this security standard. Due to the nature of the industry, there are many different scenarios where loss of data communications is not due to any malicious event. One example was the loss of communications due to hurricane Isabelle.

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments

Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate). While the relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link. It is critical to remember that "appropriate" or "adequate" levels of availability depend on the context. Based on the context of this security standard, it is not appropriate to include availability.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

The Cyber Security Standard should not mandate a particular technology such as encryption. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

The Cyber Security Standard should not mandate a particular technology. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

The Cyber Security Standard should not mandate a particular technology. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

The Cyber Security Standard should not mandate a particular technology. It should address the security requirements to be met for protecting critical cyber assets. It should be left to the responsible entity to select the technology appropriate for their environment.

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

Depending on a responsible entities' environment, redundancy may not be the most effective solution. The standard should mandate security requirements, not technical solutions.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments:

1. Under “Detailed Description”, 3<sup>rd</sup> paragraph, 1<sup>st</sup> sentence – in order to ensure SCADA monitoring functionality is included, revise to: “This standard shall primarily focus on electronic systems including: hardware, software, data, related communications networks and monitoring and control systems...”
2. Under “Detailed Description”, 3<sup>rd</sup> paragraph, delete the sentence beginning “This standard shall require that third-party...” as it is too limiting and add to the last sentence “This standard shall require that the responsible entities that must comply with the standard identify and protect themselves from threats from other connected cyber systems, including those provided by contractors and service providers.”
3. Delete the last paragraph entirely, as it adds nothing to the scope or intent of the SAR. Further, it includes a level of detail that is inappropriate for a SAR, but would be more appropriate in the standard itself.



**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name	Bill Wagner
Organization	Calpine
Industry Segment #	5
Telephone	916-608-3799
E-mail	<a href="mailto:wwagner@calpine.com">wwagner@calpine.com</a>

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments: The standard requirements are a bit vague around reliability issues. Is this a reliability standard or a security standard?

Consider enhancing the first sentence (or adding a new first sentence) to emphatically state the objective of the SAR as stated in the last sentence of paragraph 4, e.g., “The intent of this standard is to focus on the basic requirements to prevent and/or minimize impact to generation and transmission of electricity through malicious and/or unethical tampering of computer based communications, control, monitoring, and protection systems”.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

Yes

No

Comments: Consider adding additional text to emphasizing this is lowest acceptable availability requirement for secure communications. Other “Operational Reliability Standards” may dictate and

supercede with a higher availability requirement for specific cyber assets and their functions, which may be communication dependent. For example, 99.95% availability for EMS and its respective functions, implying a higher availability requirement for the communications infrastructure supporting EMS.

Perhaps in addition to overall availability requirements, the standards drafting team should consider defining minimum performance thresholds that support acceptable levels of degraded operation.

For example, normal communication thresholds may be 2 second control signal response. However, during a cyber incident like a denial of service attack, that may impact the performance of the communications network to which the EMS and plant DCS are connected, a combination of operational procedure of frequency driven governor control (over economics or schedules) and a traffic prioritization scheme to provide for minimum communication performance message delivery preference, can maintain “functional availability”, which is not captured through specific asset availability.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments The standard should detail requirements for ensuring the integrity of data transmission within expected operational performance requirements, be it through encryption, encapsulation, insulation, or isolation.

The Standards Team needs to be cautious to avoid detailing technical requirements that may unnecessarily extend the use of sunset technologies, inhibit the development of new approaches that provide the functional solution at a lower cost, or force premature retirement of older equipment and systems where the risk is mitigated simply through the limited access and proprietary industrial communications protocols.

For example, VPN may provide for a more cost effective encapsulation approach to ensuring the integrity of the data transmission than retrofitting specific communication protocols with encryption algorithms. Or, an existing private microwave link strictly used for generation control and transmission network monitoring probably provides sufficient insulation from unauthorized access simply through it’s limited accessibility.

The “integrity” requirement should apply to all cyber assets listed below that utilize or leverage any form of “open” communications infrastructure, from the internet to a POTs line with “hot” modems connected to the cyber asset.

**SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**b. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**c. Data collection servers communications to substation IEDs**

Yes

No

Comments

**d. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

The SAR should be flexible enough to allow for a redundancy scheme to satisfy the availability requirement and thereby providing respective functional protection.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

Keep it simple.

The SAR needs to provide a reasonable level of prevention requirements while encouraging the design and development of standards for a resilient cyber environment that continues to function through adverse conditions/events. For example, the security program should include steps for keeping up with OS security patches and anti-virus profiles (process) and/or installation of a mitigating appliance that buffers the respective system from network based threats while supporting the desired business functionality that is enabled through networked capabilities.

Reasonable can be defined as security program ROI does not exceed cost of a “realistic” failure scenario, e.g., equitable magnitude to recent “worst case” blackouts. Ideally, there should be enough latitude in the standard that a company can satisfy these requirements with a mix of operational process and technology to addresses their risk profile within their financial abilities.

Finally, the standards development team may consider using a social science context from which to influence and encourage the development and application of technology to address the cyber security issue. This standard is attempting to address a dysfunctional human behavior problem that is an unfortunate reality of our modern society. If everyone played by the rules, linked arms and sang happy songs, this would be a non-issue. The reality is there are groups of people with unethical motives who will exploit communications networks and computer systems for personal gain or to further violent intentions. This is different than the technical realities of the power system running outside of stated frequency tolerances.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name

Organization

Industry Segment #

Telephone

E-mail

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>Members of ECAR Critical Infrastructure Protection Panel</i>		<b>Group Representative:</b> <i>Larry Conrad</i> <b>Representative Phone:</b> 317-838-2022 <b>Representative Email:</b> larry.conrad@cinergy.com
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Larry Conrad</i>	<i>Cinergy</i>	<i>1</i>
<i>Wayne Jansen</i>	<i>DP&amp;L</i>	<i>1</i>
<i>Daniel Powell</i>	<i>Indianapolis Power &amp; Light</i>	<i>1</i>
<i>Grant McDonald, Donna Bursick</i>	<i>Allegheny Power</i>	<i>1</i>
<i>Michael Chambliss</i>	<i>Vectren</i>	<i>1</i>
<i>Keith Fowler</i>	<i>LG&amp;E Energy LLC</i>	<i>1, 5, 6</i>
<i>Don Miller</i>	<i>FirstEnergyCorp</i>	<i>1</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

Yes

No

Comments

The revised definitions substantially increase the scope and may cause significant cost to society without commensurate benefit. UAS 1200 and this SAR set a tone that assets either could or could not “adversely impact the reliability of bulk electric operations” with very little room for any measured approach to security. For example, a security breach to one substation that only affects that substation has a much smaller probability of adverse impact when compared to breaching the substation in a way that could disable an entire EMS system. Unfortunately, the definitions seem to direct the same security standard to both possibilities because either event “could” and because substations are “included at a minimum.” We suggest the scope “considers” rather than “includes” substations and power plants at a minimum. We further suggest that this SAR requires the final standard will provide some degree of flexibility based on assessment of risk and other factors that affect cost/benefit.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

Yes

No

Comments

A statistical reliability requirement is inconsistent with the stated Purpose/Industry Need of protecting critical cyber assets. Limit the scope of this standard to protection. If necessary, NERC should develop a new SAR to cover reliability and update Policy 7, which is already in place.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for



**partial failures? What level of availability should be required?**

Yes

No

Comments Same as comment 2

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments As per the definition of Critical Cyber Assets, this would not apply if it is not an IP stack.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments See the general comments at the end of this document.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments See the general comments at the end of this document.

**e. If the above were included, how long would each take to complete?**

Comments Indications are that completion would take several years. See general comments for more detail.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments Develop a new SAR to cover reliability and update Policy 7, which is already in place.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

Realistically ensuring that each of the Reliability Functions specified in the latest revision of the SAR complies with the standards already defined in the Urgent Action Standard 1200 - Cyber Security will require 12 - 24 months. Broadening the scope to include 99.5% availability per annum for all data communications joining 'two or more critical cyber assets' and encryption of all data communications utilizing public networks in the same time frame constitutes an arduous burden. While we recognize that reliability of networks is important, reliability should be handled as a separate SAR to update Policy 7. Adding reliability to this SAR will substantially increase the complexity and delay standard development. This will develop standards and prescribe time frames that are more realistic.

Further, we feel that technology should not be introduced for technologies sake. Prescribing the broad use of encryption for all data communications that traverse public network resources fails to recognize the relative risk associated with the various communications involved. For example, encryption of closed loop data traffic to and from a RTU offers protection, but the risk associated with not protecting communications to individual RTUs is much less than the risk of unprotected communications between EMS ICCP nodes. The current SAR does not prioritize protection of communications based on risk. In general, we feel a risk management approach would be more practical and offer greater protection in a shorter period of time. Ideally, the permanent standard would require that the highest risk communications would be protected first, regardless of the technologies applied. A permanent standard should focus on deployment of readily available solutions such as antivirus and strong patch management - which are proven to mitigate known high risk attacks - to be deployed in ALL effected business areas FIRST, while requiring the timing of implementation of other protective measures commensurate with risk associated with not protecting specific cyber assets.

On a technological note, we also feel that stronger authentication and verification of critical cyber devices in the absence of, or in conjunction with, encryption would greatly enhance the integrity of data communications. Encrypting data communication traffic between weakly authenticated or identified devices is of limited value. While encryption does offer protection against 'sniffing', without strong authentication rogue devices using 'spoofed' addresses are still a threat.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Alan Boesch
Organization	Nebraska Public Power District
Industry Segment #	1
Telephone	402-845-5210
E-mail	agboesc@nppd.com

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative:</b> <b>Representative Phone:</b> <b>Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## **Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

---

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### **1. Do you agree with the definitions included in the SAR?**

- Yes  
 No

Comments The Critical Cyber Assets definition is too broad. The criticality of the cyber assets will vary with location and how they are used. For example, substation automation at a rural 115 kV substation may not be critical to the reliability of the interconnected system. Similarly the loss of a special protection system may not be critical to the reliability of the Eastern Interconnection. In addition, depending upon the use of data in inter-utility data exchanges, that link may not be critical to the real-time operation of the power system. These systems should not all be subject to the same requirements.

### **2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

- Yes  
 No

Comments This SAR is to address security of the cyber assets. Availability is a different subject and if needed should be covered in a separate SAR.

### **3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

- Yes  
 No

Comments This SAR is to address security of the cyber assets. Availability is a different subject and if needed should be covered in a separate SAR.

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments Depends on how the communication is done between Control Centers. If on a private network, encryption may not be required.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments Depends on the communications system used to communicate between the servers and the IEDs.

**e. If the above were included, how long would each take to complete?**

Comments

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments Redundancy like availability is a separate issue and should be covered under a separate standard.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments The detailed description of the SAR contains a lot of justification that should not be in this section of the SAR. In addition, the requirements intended by the SAR should be spelled out and they are not. The risks and amount of damage that can be done by penetrating each cyber asset should be a factor in the level of security that is required. Physical protection at individual substations may not be feasible given the level of risk that is involved. If a hacker can only attack a local site, less damage can be done. A one size fits all approach to critical cyber assets is not feasible or desired. The SAR should recognize this and provide for such distinctions. The SAR is not real clear on the difference

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

*Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).*

*E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.*

***Please review the SAR and answer the questions in the yellow boxes.***

*If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).*

**SAR Commenter Information (For Individual Commenters)**

Name

Organization

Industry Segment #

Telephone

E-mail

**Key to Industry Segments:**

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities



**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b> <i>Southwest Power Pool</i>	<b>Group Representative:</b> <i>Kevin B. Perry</i> <b>Representative Phone:</b> (501) 614-3251 <b>Representative Email:</b> <i>kperry@spp.org</i>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>
<i>Kevin B. Perry</i>	<i>Southwest Power Pool</i>	<i>2</i>
<i>Todd Thompson</i>	<i>Southwest Power Pool</i>	<i>2</i>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## **Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### **1. Do you agree with the definitions included in the SAR?**

Yes

No

Comments

### **2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments: Engineering a data communications circuit to assure uptime is not a cyber security issue. Data circuit availability is a continuity of business operations issue. The cyber security standard should require consideration of continuity of operations issues while not specifying technical approaches or minimum design goals. At the same time, the cyber security standard should not impose any requirements that would interfere with the ability to maintain a high availability of a system or data circuit.

### **3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments: Systems and system components fail for any number of reasons, most of which are not cyber security related. System availability is a continuity of business operations issue. The cyber security standard should require consideration of continuity of operations issues while not specifying technical approaches or minimum design goals. At the same time, the cyber security

standard should not impose any requirements that would interfere with the ability to maintain a high availability of a system.

**4. The SAR does not require that SCADA or PCS communications be encrypted.**

**Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments: The cyber security standard should require data confidentiality and integrity along with ICCP node authentication. The cyber security standard should not prescribe technical solutions such as encryption.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments: The cyber security standard should require data confidentiality and integrity along with master-to-RTU authentication where technically feasible. The cyber security standard should not prescribe technical solutions such as encryption.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments: The cyber security standard should require data confidentiality and integrity along with master-to-RTU authentication where technically feasible. The cyber security standard should not prescribe technical solutions such as encryption.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments: The cyber security standard should require data confidentiality and integrity along with server-to-IED authentication where technically feasible. The cyber security standard should not prescribe technical solutions such as encryption.

**e. If the above were included, how long would each take to complete?**

Comments: There is a technical solution for assuring ICCP node authentication and data confidentiality and integrity that has undergone interoperability testing. Implementation of this technical solution would require a minimum of a year, much longer for some companies with aging legacy systems and out-of-sync budget cycles. Assuming technical solutions exist for the other technologies, implementation will require several years due to the large number of systems or devices to be protected and the need to assure uninterrupted reliability and economic operations.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments: The cyber security standard should require consideration of continuity of operations issues while not specifying technical approaches such as system redundancy.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments: The entire last paragraph of the Detailed Description should be deleted. This section defines a technical approach or technical design requirements that have no business in a security standard.

The scope of this cyber security standard should be limited to critical cyber systems typically found in the utility operations center and should not attempt to include systems found in substations or generation plants. Plant/substation systems are different in their design, functionality, and protection requirements and should be addressed in a separate security standard specific to their needs. Trying to address every conceivable system in one standard introduces confusion and diminishes the overall effectiveness of the standard.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Allen Chang
Organization	BCTC
Industry Segment #	2
Telephone	604 699 7371
E-mail	Allen.Chang@bctc.com

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative: Representative Phone: Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

## Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

### 1. Do you agree with the definitions included in the SAR?

- Yes  
 No

We feel that the definitions of *Cyber Assets* and *Critical Cyber Assets* needed further clarification and refinement. The loss of a non-stack protocol communication system could still adversely impact the reliability of bulk electric system operation. However the stack protocol communication are at a higher risk in likelihood and impact from cyber attacks than the non-stack protocol.

### 2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

- Yes  
 No

- a) The design of % uptime should be based upon the importance of the data communications between secure perimeters on a per case basis. On a critical link between secure perimeters, the 99.5% uptime may not be sufficient.
- b) The % uptime design for data communications is a separate issue from Cyber Security and should not be within the scope of a Cyber Security Standard.
- c) The % uptime/availability for "cyber security" applications or devices (eg. firewalls, intrusion detection system, etc.) has relevance for a Cyber Security Standard.

### 3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

- Yes

No

See 2c response. The availability for critical cyber assets should be addressed in a different standard.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Yes, provided that the ICCP encryption products are matured and readily available.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Our understanding of peer-to-peer communications is referring to the old legacy RTU protocol utilizing RS232 communication, voice circuits, tone telemetry, etc. Generally, these legacy systems are deemed at a low risk except where the communication takes place over an easily accessible "public network" (or any network not privately owned/operated by one's own company). The owner should consider upgrading the system to IP based communication with encryption, as the cost of implementing encryption on legacy systems may be prohibitive.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Communication to RTU's over a "public network" should be given a priority.

**d. Data collection servers communications to substation IEDs**

Yes

No

Further explanation of this question is warranted. If the communication is using TCP/IP and especially if the traffic goes over the "public network", then encryption is needed. If the communication is to send control or access relay devices, then again encryption is needed.

**e. If the above were included, how long would each take to complete?**

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Redundancy and % available are addressing similar issues. Redundancy of critical cyber assets should be addressed in another standard. Redundancy and availability for "cyber security"



applications or devices has relevance for a Cyber Security Standard.

**6. Please enter any other comments you have regarding this SAR in the space below.**

As the scope of this standards is much more wide-encompassing than the Urgent SAR standards, consideration should be given to allow participants more time to implement the additional requirements.

## Comment Form — 2nd Posting of the ‘Cyber Security’ Standard Authorization Request

*Note* — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: [sarcomm@nerc.com](mailto:sarcomm@nerc.com) with “Standard Comments” in the subject line.

**Please review the SAR and answer the questions in the yellow boxes.**

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to [timg@nerc.com](mailto:timg@nerc.com).

### SAR Commenter Information (For Individual Commenters)

Name	Marcus W. Nichols
Organization	Omaha Public Power District
Industry Segment # 1& #5	
Telephone	402-636-3613
E-mail	<a href="mailto:mnichols@oppd.com">mnichols@oppd.com</a>

### Key to Industry Segments:

- 1 – Trans. Owners
- 2 – RTOs, ISOs, RRCs
- 3 – LSEs
- 4 – TDUs
- 5 - Generators
- 6 - Brokers, Aggregators, and Marketers
- 7 - Large Electricity End Users
- 8 - Small Electricity Users
- 9 - Federal, State, and Provincial  
Regulatory or other Govt. Entities

**Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request**

---

<b>SAR Commenter Information (For Groups Submitting Group Comments)</b>		
<b>Name of Group:</b>	<b>Group Representative: Representative Phone: Representative Email:</b>	
<b>List of Group Participants that Support These Comments:</b>		
<b>Name</b>	<b>Company</b>	<b>Industry Segment #</b>

**Background Information:**

**Notes to Industry Commenters:**

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC’s Functional Model
- Removal of ‘justification’ items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

**1. Do you agree with the definitions included in the SAR?**

Yes

No

Comments

The Critical Cyber Assets definition is too broad. The criticality of the cyber assets will vary with location and how they are used. For example, substation automation at a rural 115 kV substation may not be critical to the reliability of the interconnected system. In addition, depending upon the use of data in inter-utility data exchanges, that link may not be critical to the real-time operation of the power system. These systems should not all be subject to the same requirements. The following “terms” listed in the proposed definition of “Critical Cyber Assets” are vague and therefore open to interpretation:

- Black Start
- Special Protection Systems

The proposed definition of “Critical Cyber Assets” expands the scope from the definitions in the Urgent Action Request to specifically include the following.

- Power Plant Control
- Substation Automation Control

Inclusion of these types of assets raises the criticality to the same level as system control centers, and energy management systems. Although important on an individual basis, generating stations and many substations, if tripped, will not cause cascading outages or other wide-area impacts. Existing system design allows for these contingencies. As a result, including such facilities may tend to divert resources from more important assets.

Expanding the proposed definition of “Critical Cyber Assets” to include these additional systems is unrealistic unless full compliance is not expected for 10 years or more. Resource constraints cannot support such an expanded scope with compliance expected in a shorter time-frame. In some cases, especially where older technologies are used, there will be technological constraints preventing compliance. Upgrading those older facilities to newer technologies in order to become compliant simply collides with resource constraints.

**2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?**

Yes

No

Comments

An annual availability of 99.5% for communications between secure perimeters such as the control center and a remotely located control room seems reasonable. However, if this requirement includes communications to substation and plant sites, then the requirement should be the cumulative availability summed over all sites. For example, communications to a very rural/remotely located substation may be down for more than 43.8 hours during a year, but the cumulative availability to all substation and plant sites would be less than 43.8 hours annually (assuming these other sites do not have similar extended communications outages).

**3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?**

Yes

No

Comments

Availability is a separate issue from security. While minimum availability requirements seem appropriate in principle, different systems (EMS vs SCADA vs Plant DCS vs ICCP vs Substation Automation vs etc., etc., etc.) may require different availability requirements. And for each system, the criteria for determining when that system is available may vary from entity to entity. Entity A may be able to function "acceptably" only when 10% or less of its user workstations are down, but Entity B may be able to operate acceptably with 25% of its user workstations down.

One possible exception would be the availability of communications to the regional security coordinator. The security of the region is dependent on the availability of such communications, so requiring minimal availability based on well defined criteria would be appropriate.

It must also be pointed out that availability is increased by redundancy. Redundancy also has a mitigating effect on security. That is that if a redundant asset is rendered unusable, the backup equipment will operate, offsetting the overall need for expanded security measures.

**4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:**

**a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers**

Yes

No

Comments

It is not clear that encryption provides the necessary security to the data being transmitted.

**b. SCADA master station to RTU communications using peer-to-peer communications protocols**

Yes

No

Comments

It is not clear that encryption provides the necessary security to the data being transmitted. Also, encryption is not practical for older RTU protocols still predominant in the industry.

**c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)**

Yes

No

Comments

It is not clear that encryption provides the necessary security to the data being transmitted.

**d. Data collection servers communications to substation IEDs**

Yes

No

Comments

It is not clear that encryption provides the necessary security to the data being transmitted.

**e. If the above were included, how long would each take to complete?**

Comments

It is difficult to estimate time to implement since the scope is not well defined regarding which communications would require encryption. It is estimated that at least 10-15 years would be required if all of the above must be encrypted such that critical functions still operate correctly while still meeting real-time response requirements. Data is transmitted via any number of public networks. These networks may include data protocols that are proprietary to a certain service provider.

**5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?**

Yes

No

Comments

Redundancy of critical cyber assets should not be confused with highly available functions. Redundancy is probably the most popular means to achieve high availability. As mentioned earlier, redundancy provides inherent security in some cases. Requirements should exist to restore critical functionality rather than to require redundancy.

**6. Please enter any other comments you have regarding this SAR in the space below.**

Comments

As mentioned previously, the scope of this SAR greatly expands the definition of critical cyber assets, far beyond the requirements in the Urgent Action Request. If these expanded definitions remain unchanged, electric utilities will not be able to fully comply with them for at least 10 years.

The detailed description of the SAR contains a lot of justification that should not be in this section of the SAR. In addition, the requirements intended by the SAR should be spelled out and they are not. The risks and amount of damage that can be done by penetrating each cyber asset should be a factor in the level of security that is required. Physical protection at individual substations may not be feasible given the level of risk that is involved. If a hacker can only attack a local site, less damage can be done. A one-size fits all approach to critical cyber assets is not feasible or desired. The SAR should recognize this and provide for such distinctions.

Our concern is that the standard uses a one-size fits all approach to critical cyber assets, no matter what the risk is to the interconnected system. Utilities must take steps to protect cyber assets, but the same levels of security are required in a substation as at the Control Center. In addition, the SAR does not spell out (other than a reference to the urgent action standard) what the security requirements will be.

In paragraph 3, requiring third-party providers of services (e.g. OASIS, System Suppliers, etc.) to comply with this standard may be beyond the control of the utilities contracting those services, imposing an administrative burden on, presumably, a regulatory body charged with verifying compliance.

Finally, the last sentence in the last paragraph is unreasonable. Requiring that all data utilizing shared public network resources...be encrypted not only is technically unfeasible but will also impose undue financial hardship

#### Detailed Description portion:

We are concerned that the underlying premise of the document is too broad. The sentence stating that standards are required to “provide a level of assurance that even a single compromise of a critical cyber asset does not compromise system security, and thus, grid failure” seems overly ambitious and impractical. If the intent of the SAR is to create a perfect world, this effort will result in failure at enormous cost.

At the end of this section, the proposed SAR references a requirement for encryption of data under certain circumstances. However, we have some concerns that the state of development of encryption technology today would not be sufficient to accomplish that measure within the requirements of real time operations. Inclusion of that requirement may well force companies to use inadequate technology and result in serious degradations of operating systems.

#### Definitions

The SAR proposes to include substations and generation facilities within its definition of critical cyber assets. This is a significant expansion of the emergency action standard. Moreover, we believe that such an expansion will undermine industry efforts in this area as it will require tremendous resources to manage minimal risk and detract from our efforts to improve security in key operating systems.

#### Other Comments:

The proposed SAR references building off the comments provided as part of the Emergency Action SAR. The most controversial portion of that document (as measured by the number of questions and comments) involved questions about implementing background investigation requirements for existing employees. That issue alone had the potential to defeat the Emergency Action SAR.

This document is silent on that issue. Given the above history and the nature of the SAR process, we believe that this document should state what the intentions are in this area and how it will be addressed as part of the process. Failure to address this issue properly will risk the defeat of a permanent standard when it is finally issued.