

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 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.

SAR Commenter Information (For Individual Commenters)

Name	Stuart Brindley
Organization	IMO (Ontario)
Industry Segment #	2
(Telephone	905) 855-6108
E-mail	stuart.brindley@theIMO.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

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

- 1st 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.