



T. Moser, Chairman
STARS Integrated Regulatory Affairs Group
P.O. Box 620, Fulton, Missouri 65251

2007 SEP 13 11:29:08

Ref: 72FR37058

RECEIVED

STARS-07013

September 10, 2007

Chief
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
ATTN: Rulemaking, Directives, and Editing Branch, Office of Administration

7/6/07
72FR37058

8

**STRATEGIC TEAMING AND RESOURCE SHARING (STARS)
COMMENTS ON DRAFT REGULATORY GUIDE DG-5019
72FR37058 (July 6, 2007)**

The Strategic Teaming and Resource Sharing (STARS)¹ alliance would like to take advantage of this opportunity to comment on the Draft Regulatory Guide (DG) 5019 Reporting of Safeguards Events. Comments are provided in the enclosure to this letter.

The STARS alliance appreciates the opportunity to comment on the Draft Regulatory Guide. If there are any questions regarding these comments, please contact me at 573-676-4775, or tmoser@ameren.com, or Ted Koser at 361-972-8963, or tckoser@stpegs.com.

Sincerely,

T. Moser, Chairman
STARS Integrated Regulatory Affairs Group

SONSI Review Complete

E-RFDS = ADM-03

¹ STARS is an alliance of six plants (eleven nuclear units) operated by Luminant Power, AmerenUE, Wolf Creek Nuclear Operating Corporation, Pacific Gas and Electric Company, STP Nuclear Operating Company and Arizona Public Service Company.

add = J. Ridgely (JNR)

Template = ADM-013

add = B. Schnetzler (b965)

The STARS Alliance respectfully submits the following comments on Draft Guide 5019 with the reference indicated first followed by the specific comment.

General Comment

In some instances the guideline refers to the compensation time in the NRC-approved security plan requirements and other places refers to specific time frames (e.g. 10 minutes, 1 hour etc.). In most cases the appropriate compensation time in the Reg Guide should be based on the requirements in the NRC-approved security plan.

STARS comment number 1

2.4 Examples of Security Events to be Reported Within 1 Hour

(3)

- *confirmed cyber attacks on or failures of computer systems that may adversely impact safety, security, and emergency preparedness*

Comment

Suggest rewording as follows since stations should only need to report if there any failures of these systems related to a threat not an equipment failure in itself.

- *confirmed cyber attacks on or failures of computer systems that **are a result of a confirmed cyber attack that** may adversely impact safety, security, and emergency preparedness*

STARS comment number 2

(4)

- *discovery of a criminal act involving individuals granted unescorted access, which in the judgment of the licensee, could afford an opportunity to adversely effect plant safety or represents a threat.*

Comment

Incorporate examples provided in RG 5.62 for clarification. See following mark-up

- *discovery of a criminal act involving individuals granted unescorted access, which in the judgment of the licensee, could afford an opportunity to adversely effect plant safety or represents a threat. **(e.g., felonious***

acts, discovery of a conspiracy to bomb-the facility or disturb its vital components, vandalism of vital equipment, reasonable suspicion of illegal sale, use, possession, or introduction of a controlled substance onsite).

STARS comment number 3

(4)

- *improper control of access control area or media (e.g., key-cards, passwords, cipher codes) that results in the use of the media during the time it is not controlled (e.g., tailgating into an area to which the individual would not have been authorized)*

Comment

The intent of this example is unclear. The example indicates tailgating would be considered a 1 hour reportable event. Generic Letter 91-03, "Reporting of Safeguards Events", indicates that tailgating would be logged if there was no malevolent intent. Suggest a specific example or delete.

STARS comment number 4

(4)

- *incomplete or inaccurate preauthorization screening that would have resulted in the denial or suspension of unescorted access authorization had the screening been complete and accurate (this involves either the authorization or the granting of unescorted access)*

Comment

Clarification in parentheses is unclear. Suggest mark-up as follows

- **authorization of or the granting of unescorted access due to** *incomplete or inaccurate preauthorization screening that would have resulted in the denial or suspension of unescorted access authorization had the screening been complete and accurate (~~this involves either the authorization or the granting of unescorted access~~)*

STARS comment number 5

(5)

- *failure to adequately compensate for an event or identified failure, degradation , or vulnerability that could allow undetected or unauthorized access (licensees need not report within 1 hour if the failure involves a very short period of time, i.e., 10 minutes or less, those events should be logged)*

Comment

This example uses as a "short period of time" one that is more restrictive than requirements in NEI 03-12, "Security Plan Template". This proposed time period would cause unneeded changes to our Security plans and programs.

STARS comment number 6

(5)

- *an uncompensated design flaw or vulnerability in a physical protection system that could have allowed unauthorized access or which could have substantively eliminated or significantly reduced response capabilities*

Comment

Generic letter 91-03 indicates that a design flaw would be logged. The example in the generic letter is PAVA barriers. Compensatory actions are normally established upon discovery. Is this example only referring to vulnerabilities that were discovered but no compensatory actions were taken after discovery? Please provide clarification.

STARS comment number 7

(6)

- *discovery of unaccounted, lost, or stolen keys (but not key-cards or badges) that allow access to controlled areas*

Comment

This example is more appropriate under (5) for vulnerability in a security system that could allow undetected or unauthorized access. Suggest Adding to (5) and removing from item (6).

STARS comment number 8

- (6) *The following are examples of actual or attempted introduction of contraband into an area which the licensee is required to control access:*
- *discovery of unaccounted, lost, or stolen keys (but not key-cards or badges) that allow access to controlled areas*
 - *loss of a security weapon that is not retrieved within 1 hour*

Comment

Neither keys nor security weapons are considered “contraband”. Suggest the example of loss of keys be added to item (5) for vulnerability in a security system that could allow undetected or unauthorized access – see comment 7. Suggest the example be modified to include “unauthorized weapon) as noted in mark-up and add example as noted below.

(6) *The following are examples of actual or attempted introduction of contraband (i.e., **unauthorized/uncontrolled weapons, explosives, or incendiary devices**) into an area which the licensee is required to control access:*

- *~~discovery of unaccounted, lost, or stolen keys (but not key cards or badges) that allow access to controlled areas~~*
- *loss of a security weapon that is not retrieved within 1 hour*
- **Contraband introduced into in a controlled access area (i.e., search failure)**

STARS comment number 9

3.2 Examples of Security Events to be Reported in the Security Log

(1)

- *failure to adequately compensate for an event or identified failure, degradation , or vulnerability that would **not** have allowed undetected or unauthorized access or has existed for only a very short period of time (e.g., posting a compensatory officer in 12 minutes instead of 10 minutes)*

Comment

This example uses as a “short period of time” one that is more restrictive than requirements in NEI 03-12, “Security Plan Template”. This proposed time period would cause unneeded changes to our Security plans and programs.

STARS comment number 10

(2)

- *for power reactors, loss of the partial capability of one alarm station to remotely monitor, assess, or initiate response to alarms if the same capability remains operable in the other alarm station.*

Comment

This example uses ambiguous language, which will allow for “subjective” enforcement actions based upon the interpretation of the inspector (i.e., loss of only 1 sequence monitor that has minimal impact on the

effectiveness of the security system). Suggest removing "partial" from example.

STARS comment number 11

(2)

- *loss of control or protection of unclassified safeguards information when there does not appear to be evidence of theft or compromise, and is recovered within 1 hour*

Comment

The 1 hour limit by itself does not indicate evidence of compromise. The real issue is whether the loss of control could have been exploited. Suggest the following mark-up.

- *loss of control or protection of unclassified safeguards information when there does not appear to be evidence of theft or compromise, **and is recovered within 1 hour (consider location of information, if it has been tampered with, access to the information, amount of time uncontrolled to determine potential compromise)***

STARS comment number 12

(2)

- *discovery of contraband material outside the protected area or inside a designated vehicle barrier or control point that does not constitute a threat or potential threat to the facility*

Comment

This example imposes a new requirement which would require reporting the discovery of contraband in a parking lot. If the contraband does not constitute a threat or potential threat, there should be no requirement to log the event.

STARS comment number 13

(2)

- *the unfavorable termination of personnel whose job duties and responsibilities actively support insider threat mitigation*

Comment

The unfavorable termination of these individuals in and of itself does not indicate vulnerability in the security program. Suggest either removing this

example or providing additional guidance or examples of the types of actions that would prompt logging certain terminations vs. logging all unfavorable terminations.

STARS comment number 14

3.3 Security Events Not Expected to be Reported in the Security Log

Comment

Would licensees be subject to enforcement for conservatively reporting/logging items that fall into this category?