



Tennessee Valley Authority, 1101 Market Street, Chattanooga, Tennessee 37402

Mark O. Medford
Vice President, Nuclear Assurance, Licensing and Fuels

March 19, 1993

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

Gentlemen:

In the Matter of)	Docket Nos. 50-327
Tennessee Valley Authority)	50-328

SEQUOYAH NUCLEAR PLANT (SQN) - NRC INSPECTION REPORT NOS. 50-327,
328/92-37 - REPLY TO NOTICE OF VIOLATION (NOV) 50-327, 328/92-37 AND
PROPOSED IMPOSITION OF A CIVIL PENALTY

The enclosure contains TVA's reply to Stewart D. Ebnetter's letter to me dated February 18, 1993, which transmitted the subject NOV and proposed imposition of a civil penalty. This NOV describes deficiencies in protecting safeguards information (SGI) and, in certain instances, reporting them to NRC. This two-part violation resulted from inattention to detail, failing to follow procedures in controlling SGI, and a difference in interpreting the threshold for logging several safeguards events. Payment of the imposed civil penalty in the amount of \$50,000 was made by electronic fund transfer No. 0315000654.

If you have any questions concerning this submittal, please telephone M. A. Cooper at (615) 843-8924.

Sincerely,

Mark O. Medford

Enclosure
cc: See page 2

IE14
1/1

9303300200 930319
PDR ADOCK 05000327
PDR

U.S. Nuclear Regulatory Commission
Page 2
March 19, 1993

cc (Enclosure):

Mr. D. E. LaBarge, Project Manager
U.S. Nuclear Regulatory Commission
One White Flint North
11555 Rockville Pike
Rockville, Maryland 20852-2739

NRC Resident Inspector
Sequoyah Nuclear Plant
2600 Igra Ferry Road
Soddy-Daisy, Tennessee 37379-3624

Mr. B. A. Wilson, Project Chief
U.S. Nuclear Regulatory Commission
Region II
101 Marietta Street, NW, Suite 2900
Atlanta, Georgia 30323-0199

ENCLOSURE

REPLY TO NOTICE OF VIOLATION
NRC INSPECTION REPORT NOS. 50-327, 328/92-37
STEWART D. EBNETER'S LETTER TO MARK O. MEDFORD
DATED FEBRUARY 18, 1993

Violation 50-327, 328/92-37

"A. Violation Related to the Transfer Offsite of a Security Storage Container which Contained Safeguards Information.

10 CFR 73.21(d)(2) states, in part, 'While unattended, Safeguards Information shall be stored in a locked security storage container.'

10 CFR 73.21(c)(1) states, in part, '[N]o person may have access to Safeguards Information unless the person has an established "need to know" for the information.' Section 73.21(c)(1) also specifies the persons who may have access to such information.

Contrary to the above, on September 18, 1992, it was discovered that a safe containing Safeguards Information (SGI) had been removed from the site, transferred to persons who did not have an established 'need to know,' and later transferred to another individual who also did not have an established 'need to know,' who discarded the SGI in an unauthorized manner.

"B. Violations Related to Failures to Control Safeguards Information While Onsite.

1. 10 CFR 73.21(d)(2) states, in part, 'While unattended, Safeguards Information shall be stored in a locked security storage container.'

Contrary to the above:

- a. Safeguards Information was not secured or attended when containers with Safeguards Information were found unlocked on January 16, April 18, June 29, and October 23, 1991, and August 18, 1992.
- b. Safeguards Information was found in an unsecured, unauthorized container on April 21, 1992, and July 23, 1992.
- c. Safeguards Information was found unattended and unsecured in the alarm station after the station had been dismantled for construction on October 29, 1992.
- d. During a Quality Assurance audit conducted October 26 through December 1, 1992, a security officer at the Essential Raw Cooling Water facility was observed leaving safeguards material unattended.

2. 10 CFR 73.21(e) states, in part, 'Each document or other matter that contains Safeguards Information as defined in paragraph (b) in this section shall be marked "Safeguards Information" in a conspicuous manner...'

Contrary to the above, on September 6, 1991, several safeguards drawings were found not to be properly marked as 'Safeguards Information.'

3. 10 CFR 73.21(c)(1) states, 'Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established "need-to-know" for the information.'

Contrary to the above, on November 19, 1992, an individual was found to have been on the safeguards access list since 1989, who was not a TVA employee, did not have a 'need-to-know,' and should not have had access to Safeguards Information.

4. 10 CFR 73.71(c)(1) states, 'Each licensee subject to the provisions of 73.20, 73.37, 73.50, 73.55, 73.60 ... shall maintain a current log and record the safeguards events described in paragraph II(a) and (b) of Appendix G to this part within 24 hours of discovery by a licensee employee or member of the licensee's contract security organization.'

10 CFR 73, Appendix G, II(b) requires the following to be logged 'Any other threatened, attempted, or committed act not previously defined in Appendix G with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness.'

Contrary to the above, the licensee did not log seven failures to protect safeguards information that were discovered on April 18, June 29, September 6, 1991 and July 23, August 18, November, [sic] 11, 1992, and during the Quality Assurance audit conducted October 26 through December 1, 1992. These events had the potential for reducing the effectiveness of the safeguards system below that committed to in the licensee's physical security plan because the information not protected could have assisted an intruder in unauthorized entry and/or sabotage of the plant.

"This is a Severity Level III problem (Supplement III).

"Cumulative Civil Penalty - \$50,000 (assessed equally among the violations)"

Violation A

Violation A involved the sale of a cabinet containing SGI to a non-TVA organization.

Admission or Denial of the Violation

TVA admits the violation.

Reason for the Violation

The reason for this violation was that an individual failed to follow procedures and properly establish an SGI cabinet that would control and protect the SGI. The container was instead established without the knowledge of Security personnel and without proper SGI storage identification. As such, the container was not on the approved safeguards container list and was not identified or controlled as an SGI container. The apparent owner of the unauthorized cabinet left the employment of TVA without unlocking the cabinet or identifying the contents of the cabinet. Without any physical SGI identification, the cabinet was not recognized as containing SGI and, consequently, was not handled appropriately.

It should be noted that neither the surplus container nor the SGI was located at the Sequoyah Nuclear Plant (SQN) site but was recorded on SQN's reporting logs because SQN SGI material was stored in the container.

Corrective Action Taken and Results Achieved

SGI custodians have been interviewed, and no additional unauthorized cabinets have been identified. An effort was made to determine if any other unauthorized SGI containers were abandoned or sold. The investigative effort determined this event to be an isolated case.

Security SGI procedures have been revised to permit only Security to establish SGI containers, and all SGI containers are to be conspicuously identified. Additionally, only SGI containers will be secured with Sargent and Green (S&G) combination locks. S&G locks can only be procured through TVA Purchasing by Security.

Because of this event, a Quality Improvement Team (QIT) was formed. The findings of the QIT indicated that TVA was generating and storing too much SGI, that the number of SGI custodians was too high, and that there were too many SGI containers. The QIT was functioning before the NRC inspection was conducted. The corrective actions to reduce the volume of SGI, the number of custodians, and the number of SGI containers have been accomplished. Although the overall effectiveness of these actions is indeterminate at this time, no SGI control events (relative to the violation) have been identified since the corrective actions were implemented. The QIT is expected to have its recommendations and evaluations formulated in a final report by September 1993.

Finally, in response to this event, the corporate safeguards custodians have been retrained; and the Facilities Maintenance personnel responsible for moving SGI containers have been sensitized that locked containers are not to be moved until inventories by Security can be conducted.

Date When Full Compliance Will be Achieved

SQN is in full compliance.

Violation B

Violation B, described in this section of the stated violation, involved several instances of failure to properly control and protect SGI. Examples of which included:

1. SGI containers found unlocked and unattended
2. SGI stored in an improper container
3. SGI unsecured in an alarm station after it had been dismantled
4. Documents not properly marked as SGI
5. Former Institute of Nuclear Power Operations (INPO) employee with authorized access to SGI
6. Failure to log incidents involving improper handling of SGI

Admission or Denial of the Violation

TVA admits the violation.

Reason for the Violation

The reason for the failure to properly control and protect SGI in the first four examples was inattention to detail. The personnel involved handled SGI frequently and were aware of the requirements associated with protecting SGI. While each incident was investigated and determined to be an isolated personnel error, a failure in the investigation process to include the extent of condition and previous similar events led to a lack of recognition of a potential adverse trend. It should be noted that individually, each event was of minimal safeguards significance. The principal contributing factors to the failure to control and protect SGI were: (1) too much SGI, (2) too many personnel with SGI authorization, and (3) too many SGI locations.

An INPO employee on an assignment at SQN was granted SGI access and was not removed from the access list after he had completed his assignment at SQN. The cause of this event was reliance on the personnel checkout system to identify personnel that were no longer qualified for access to SGI. The INPO employee failed to follow the proceduralized process and properly check out upon his departure from SQN. The individual was removed from the site access list. However, the site access authorization list was not cross-checked against the list that authorized access to SGI.

The last example in the violation was the failure to properly log events involving improper handling of SGI. The reason for the failure to properly log events was a difference between TVA and NRC in interpreting the threshold for logging SGI events. TVA's reporting standard was developed from its interpretation of the requirements found in 10 CFR 73, the guidance found in NRC Generic Letter 91-03, and the collective interpretation of the Southeast Nuclear Security Association. TVA's reporting process was based on a matrix that classified an event in one of four possible categories, depending on the significance of the SGI and whether the SGI was lost or compromised. Based on this matrix, SGI incidents were recorded in the SQN Site Security log, but only five events were determined to be loggable to NRC in the quarterly report. TVA's reportability determinations were directly related to the overall significance of an event.

The higher threshold precluded identification of an adverse trend since TVA only trended the events that were logged to NRC in the quarterly report. As a result of TVA's reporting threshold, only five events were reported in a two-year period. This small number of events did not indicate an adverse trend in the control of SGI.

Corrective Actions Taken and Results Achieved

To combat the deficiency of inattention to detail, the following corrective actions have been implemented:

1. A letter was issued to the SQN safeguards custodians, and the controlling procedure was revised to require the use of SGI signs and accountability logs.
2. The safeguards custodians were provided upgraded training on SGI control.
3. A security follow-up review verified the use of SGI container signs and accountability logs.

As previously discussed, a QIT was formulated to inspect, investigate, and help improve the control and protection of SGI Valley-wide. This effort was initiated before the NRC security inspection. The team made three recommendations: (1) reduce the volume of SGI, (2) reduce the number of SGI containers, and (3) reduce the number of SGI custodians. The recommendations to reduce the volume of SGI being generated and reduce the number of SGI containers and custodians have been accomplished at SQN.

The SGI access list has been reviewed and cross-checked with the SQN plant access list to ensure that only current personnel are granted access to SGI.

A letter has been issued to the Site Security supervisors requiring all SGI events to be recorded in the 24-hour event log. The safeguards events that were not reported in the previous quarterly reports have been logged in the 24-hour log as a single entry. Every event that has been entered in the 24-hour event log has been appropriately reported to NRC in the quarterly report. TVA has also changed the threshold for the reporting of safeguards events to coincide with NRC expectations.

TVA failed to recognize an adverse trend developing in the control of SGI because each investigation was too narrowly focused. To correct this deficiency in the future, the procedures have been revised to ensure that security event investigations will include: (1) the extent of the condition, (2) a search for previous similar events, (3) one member of the Security Event Team who is trained in root cause analysis methods, and (4) corrective actions of each event that will be formally tracked. Additionally, a trend analysis of security events will be performed to identify adverse trends, and corrective actions will be initiated as appropriate.

Corrective Steps That Will be Taken to Avoid Further Violations

In the future, security events will be reviewed over a broader timeframe, and safeguards events classified as nonreportable will be evaluated and trended in an effort to identify adverse trends. Site Quality will continue to perform oversight reviews of the safeguards program.

The corrective action associated with unauthorized SGI access will include additional management overview to ensure that the access list is periodically updated. The SGI access list will also be cross-checked with the plant access list. The corporate business practice controlling SGI access will be revised to ensure that management controls are established.

Date When Full Compliance Will be Achieved

SGN is in full compliance.

Commitment

The corporate business practice controlling SGI access will be revised to ensure that management controls are established and that the access list is periodically reviewed and updated. This will be accomplished by March 31, 1993.