ENCLOSURE 2

U.S. NUCLEAR REGULATORY COMMISSION
REGION IV

Docket Nos.:	50-361; 50-362
License Nos.:	NPF-10; NPF-15
Report No.:	50-361/98-12; 50-362/98-12
Licensee:	Southern California Edison Co.
Facility:	San Onofre Nuclear Generating Station, Units 2 and 3
Location:	5000 S. Pacific Coast Hwy. San Clemente, California
Dates:	July 13-17, 1998
Inspector(s):	A. Bruce Earnest, Physical Security Specialist Plant Support Branch
Approved By:	Blaine Murray, Chief Plant Support Branch

ATTACHMENTS:

Attachment 1	Supplemental Information
Attachment 2	Facsimile from Licensee, dated September 24, 1998

EXECUTIVE SUMMARY

San Onofre Nuclear Generating Station, Units 2 and 3
NRC Inspection Report 50-361/98-12; 50-362/98-12

This routine, announced inspection focused on the licensee's physical security program. The areas inspected included access authorization/fitness-for-duty, personnel access control, compensatory measures, assessment aids, onsite review of event reports, and followup of previously identified items.

Plant Support

- A noncited violation of 10 CFR Part 26 and security procedures was identified for failing to complete a fitness-for-duty drug screen prior to granting access to an individual who was not fit-for-duty (Section S1.1).

- A noncited violation of the physical security plan and security procedures was identified for failure to control personnel access control to a vital area (Section S1.2).

- A violation of the physical security plan and security procedures was identified for failing to adequately compensate for three separate failures of the security computer system (Section S2.1).

- A noncited violation of the physical security plan was identified for two instances of inattentive security officers manning the guard towers (Section S2.2).

- A violation of 10 CFR 50.9 was identified involving the submittal of inaccurate information to the NRC (Section S8.1).

Report Details

IV. Plant Support

S1 Conduct of Security and Safeguards Activities

S1.1 Access Authorization/Fitness-for-Duty

a. Inspection Scope

Portions of the access authorization program were reviewed in order to determine compliance with 10 CFR 73.56 and the physical security plan. Portions of the fitness-for-duty program were reviewed in order to determine compliance with 10 CFR Part 26.

b. Observations and Findings

10 CFR 26.24(a)(1) requires that personnel will be initially tested within 60 days prior to granting unescorted access. 10 CFR 26.10(a) requires fitness-for-duty programs to provide reasonable assurance that personnel are not under the influence of any substance which in any way affects their ability to safely and competently perform their duties.

The requirements of 10 CFR 73.56 are implemented, in part, by the licensee's General Procedure SO123-XV-7, Revision 8. Paragraph 6.3.1 of the procedure requires that a badge granting unescorted access into the primary access is not to be issued until a satisfactory drug and alcohol screen has been completed within 60 days prior to granting access.

During a review of a licensee reported event (LER 98-003), the inspector noted the following:

- On March 10, 1998, while reviewing a report of pending security badges, the access authorization supervisor determined that a protected area unescorted access badge had been inappropriately issued to a contract worker on March 9, 1998, before drug screening test results were received. The test was administered to the contract worker on March 9, 1998, the same date that unescorted access was granted. The contract employee entered the protected area on March 10, 1998, at 6:44 a.m. After discovering the mistake, the supervisor caused the unescorted access of the individual to be canceled. The contractor was escorted out of the protected area at 9:37 a.m. The contractor employee was inside the protected area for approximately 3 hours. There was no vital area access during the 3-hour time period. Subsequently, on March 16, 1998, the medical review officer declared that the worker's sample collected on March 9, 1998, was positive for methamphetamine.

The failure to submit appropriate fitness-for-duty test information to access authorization personnel, in order for an appropriate evaluation or consideration of that information

prior to granting unescorted access, resulted in the granting of access to an individual that if the drug screen results had been considered, the individual would not have been granted access. The failure to provide accurate drug screen results and present the results for consideration before granting access is a violation of 10 CFR 26.24(a)(1) and Paragraph 6.3.1 of the licensee's General Procedure SO123-XV-7, Revision 8, (50-361/9812-01;-362/9812-01). This nonrepetitive, licensee-identified and corrected violation is being treated as a noncited violation consistent with Section VII.B.1 of the NRC Enforcement Policy.

The above noncited violation is similar to the violation documented in NRC Inspection Report 50-361/95-05; 50-362/95-05. Information provided by the licensee by facsimile (Attachment 2) on September 24, 1998, was considered in dispositioning this recent violation as a noncited violation. This recent violation was not considered a repetitive violation in accordance with the NRC Enforcement Policy.

The root cause of this noncited violation was an erroneous computer data entry that inaccurately stated that the contract employee had been drug and alcohol tested and that there was a negative finding. When drug screening was completed, the initial test at the plant revealed a positive test for methamphetamine, and the confirmatory test results received on March 16, 1998, confirmed the contract worker was unfit for duty.

The corrective actions included the briefing and training of appropriate fitness-for-duty personnel. In addition, the access authorization computer database was modified to not permit the entry of a drug screening result if a drug screening submittal has not first been entered. The access authorization section changed their process by requiring a hard copy of the test results before granting unescorted access.

c. Conclusion

A noncited violation of 10 CFR Part 26 and security procedures was identified for failing to complete a fitness-for-duty drug screen prior to granting access to an individual who was unfit for duty.

S1.2 Access Control - Personnel

a. Inspection Scope

The personnel access control program was inspected to determine compliance with the requirements of 10 CFR 73.55(d)(1), and (7), and the physical security plan.

b. Observations and Findings

10 CFR 73.55(d)(7)(i)(B) requires that the licensee positively control all points of personnel access to vital areas and limit such access to vital areas under nonemergency conditions to individuals who require access in order to perform their duties.

Paragraph 5.1.4 of the physical security plan, Revision 58, states, in part, "The SONGS VA access authorization system, which is described in written station procedures, has been designed to limit access to individuals who require entry to particular areas in order to perform their job duties." Further, it states that, "Positive identification of VA access authorization is accomplished by means of card-key badges."

Paragraph 6.7.1.2 of Security Procedure SO123-IV-5.1, Revision 7, requires that all family tour escorts have their vital area access removed prior to the tour starting. Paragraph 6.4.2.3 of licensee Security Procedure SO123-XXIII-4, Revision 2, states that all vital areas will be off limits to visitors and employees (escorts) participating in the Family Tour Program.

The licensee identified in the safeguards event log that on May 10, 1998, three personnel (escort and two family members) were incorrectly granted access to a vital area (diesel generator building) during a family tour. None of the three persons was authorized access to the vital area. The access control system was bypassed by a second employee (not an escort) when the second employee allowed the visitors and their escort to tailgate in and out of the vital area.

The licensee determined the root cause of the violation was personnel error. Both the escort, who did not have vital area access, and the second employee who did, forgot rule and procedural requirements in their attempt to provide an informative tour to family members. Corrective actions included retraining of the two employees involved, re-emphasis of the procedural requirements to the plant population at large, and a change to the General Employee Training emphasizing escorting and vital area access. The failure to control vital area access constitutes a violation of the requirements of 10 CFR 73.55(d)(7)(i)(B), paragraph 5.1.4, of the physical security plan, and paragraph 6.7.1.2 of Security Procedure SO123-IV-5.1 (50-361/9812-02; -362/9812-02). This nonrepetitive, licensee-identified and corrected violation is being treated as a noncited violation consistent with Section VII.B.1 of the NRC Enforcement Policy.

c. Conclusion

A noncited violation of the physical security plan and security procedures was identified for failure to control personnel access to a vital area.

S2 Status of Security Facilities and Equipment

S2.1 Compensatory Measures

a. Inspection Scope

The compensatory measures program was inspected to determine compliance with the requirements of 10 CFR 73.55(a), (g)(1), and the physical security plan. The areas inspected included the deployment of compensatory measures and the effectiveness of those measures.

b. Observations and Findings

10 CFR 73.55 (g)(1) states, in part, "All alarms, communications equipment, physical barriers, and other security related devices or equipment shall be maintained in operable condition. The licensee shall develop and employ compensatory measures including equipment, additional security personnel, and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment and structures."

Paragraph 3.2.3 of the physical security plan states, in part, "Upon identification of a failure to comply with this plan or its implementing procedures, security management will implement prompt corrective action to mitigate the consequences of system failure, to achieve equivalent protection, and to prevent recurrence." Further, paragraph 3.2.4 states, in part, "SCE has established a management system that provides for the development, revision, implementation, and enforcement of security procedures. New procedures and revisions to current procedures are subject to the approval of the Manager, Site Security. All procedures are reviewed and updated annually in accordance with standard station policy."

Paragraph 6.6.3 of the physical security plan states, in part, "An armed security officer/unarmed security personnel equipped with a radio observes the affected segment pending restoration of intrusion detection capability." Further, paragraph 6.6.4 (VA Alarm Failure) states, in part, "In the event of a VA alarm system outage, the following compensatory measures will be taken: All VA card-key access portals are designed to fail locked and are inspected by an armed security officer or unarmed security personnel. Any portals found unlocked are secured with either a security padlock or a manned logging station is established. Armed security officers/unarmed security personnel equipped with access lists control access to such portals until the system is repaired and tested." At the bottom of the page, which contained the above requirements, the physical security plan states, in part, "These measures will provide an equivalent level of intrusion detection protection pending prompt repair of the failed system."

Threat Event TS M4-D contained in the safeguards contingency plan requires the security organization to deploy the security force to compensate for failed computer channels. Further, under the data required section, it references preplanned scenarios for predesignated security post assignments and patrol routes contained in the shift commanders post order binder to compensate for the range of security computer failures.

During NRC Inspection 50-361/97-24; 50-362/97-24, the inspector determined that the licensee had not established a specific procedure for the employment of compensatory measures resulting from a security computer failure. Pending further review by the NRC, the issue was characterized as an unresolved item in NRC Inspection Report 50-361/97-24; 50-362/97-24. The subsequent review determined that during

three events that occurred on May 20, July 29, and October 30, 1997, both security computers failed; adequate compensatory measures were not instituted in that security officers were not posted to control most of the vital area portals; and the measures instituted did not ensure an equivalent level of protection. The failure to provide adequate compensatory measures is a violation of the requirements of paragraphs 3.2.3 and 6.6.3 of the physical security plan (50-361/9812-03; -362/9812-03).

Corrective actions by the licensee included changes to the compensatory measures procedure to include security computer failures. The inspector reviewed changes to Security Procedure SO123-IV-6.8, Revision 2, which describes the addition of compensatory measures for a degraded security computer. The procedure was greatly enhanced by the changes. Information directing compensatory measures was more detailed, comprehensive, and user friendly. On July 15, 1998, the inspector observed a drill in which the security shift on duty simulated the loss of the security computers. All of the compensatory measures posts were manned within 5 minutes. The inspector walked down the posts with shift security supervision. The officers at each post were questioned about the area that they were compensating, and the responses indicated a very well trained shift. The compensatory measures plan for posting was well thought out and adequately ensured that all detection system losses were compensated. The inspector concluded that the corrective actions implemented should prevent recurrence of a similar violation.

c. Conclusion

A violation of the physical security plan and security procedures was identified for failing to adequately compensate for three separate failures of the security computer system.

S2.2 Assessment Aids/Inattentive Security Officers

a. Inspection Scope

The assessment aids program was inspected to determine compliance with 10 CFR 73.55 (h)(4) and (6) and the physical security plan.

b. Observations and Findings

10 CFR 73.55(h)(6) requires a capability of observing the protected area isolation zones. Paragraph 6.2.1 of the physical security plan requires the guard tower officers to assess all alarms and activities in the isolation zones.

During a review of the safeguards event logs, the inspector determined that the licensee had identified that guard tower security officers were discovered asleep in the guard towers on March 14 and April 12, 1998, and unable to assess the alarms and activities in the isolation zones. The inspector reviewed documentation of corrective action that included notifying all security officers of the necessity of staying awake on post and

disciplinary action for the officers involved. The corrective action was apparently effective. Even with a higher awareness among supervisors, there has not been an identified recurrence since the last incident in April 1998. The inability of security officers to assess alarms and activities in the isolation zones is a violation of paragraph 6.2.1 of the physical security plan (50-361/9812-05; -362/9812-05). This nonrepetitive, licensee-identified and corrected violation is being treated as a noncited violation consistent with Section VII.B.1 of the NRC Enforcement Policy.

c. Conclusion

A noncited violation of the physical security plan was identified for two instances of inattentive security officers manning the guard towers.

S8 Miscellaneous Security and Safeguards Issues (81700-02.08)

S8.1 Inaccurate Information Submitted to the NRC

a. Inspection Scope

Through inspection activities and interviews, the accuracy of information provided by the licensee during an enforcement conference and in a letter from the licensee to the NRC dated February 3, 1998, was reviewed to confirm compliance with the requirements of 10 CFR 50.9.

b. Observations and Findings

10 CFR 50.9(a) states, in part, "Information provided to the Commission by an applicant for a license or by a licensee or information required by statute or by the Commission's regulations, orders, or license conditions to be maintained by the applicant or the licensee shall be complete and accurate in all material respects."

During a predecisional enforcement conference in Region IV on January 20, 1998, and in a letter dated February 3, 1998, the licensee submitted information that indicated compensatory measures utilized during security computer failures on May 20, July 29, and October 30, 1998, were adequate in that responding security officers had all received patrol cards and that they had been trained on the use of the cards. Inspection activities by NRC staff during an initial inspection provided information that was different from that provided by the licensee. Subsequent review by NRC confirmed that the above submittals were inaccurate. The licensee reached the same conclusion subsequent to being notified by the inspection staff. A licensee letter to the NRC dated February 24, 1998, concluded that the information submitted was inaccurate and corrected the information. The failure to submit complete and accurate information to the NRC constitutes a violation of 10 CFR 50.9 (50-361/9812-04; -362/9812-04).

c. Conclusion

A violation of 10 CFR 50.9 was identified by NRC in which the licensee submitted inaccurate information to NRC.

S8.2 Onsite Review of Event Reports (92700)

S8.2.1 (Closed) LER 50-361/98-02;-362/98-02: Diesel Fuel Oil Filtration

The LER described events when a diesel fuel oil filtration trailer was brought into the protected area. There was some doubt on the part of the licensee as to whether correct escort and compensatory measures requirements were appropriately implemented. A review of the incident by NRC did not reveal any noncompliance. However, the licensee did clarify procedural requirements to prevent further confusion regarding escort and compensatory requirements during diesel fuel oil filtration operations.

S8.2.2 (Closed) LER 50-361/95-02;-362/95-02: Loss of Safeguards Information in the U.S. Mail

The licensee did not mishandle or improperly mail the safeguards information lost. NRC guidance allows the use of the U.S. mail to transmit safeguards information. The licensee attempted to trace the mailed information numerous times with post office officials to no avail.

S8.2.3 (Closed) LER 50-361/96-02;-362/96-02: Missed Surveillance

The licensee failed to perform a testing surveillance on an infrared detection zone as per the plan requirements. It was licensee-identified, of minor nature and, except for the requirements of license condition 2.G which has since been changed, would have been logged in the safeguards event log. The missed surveillance was of minor significance and did not affect the health and safety of the plant personnel or the public.

S8.2.4 (Closed) LER 50-361/96-03;-362/96-03: Security Alarm Not Posted

During a 1996 review of security records, the licensee discovered that on December 20, 1992, a segment of the protected area detection aids was not posted upon discovery that the zone had exceeded the false and nuisance alarm rate. It was licensee identified, of minor nature and, except for the requirements of license Condition 2.G, which has since been changed, would have been logged in the safeguards event log.

S8.2.5 (Closed) LER 50-361/97-02;-362/97-02 and LER 50-361/97-02-01;-362/97-02-01: Failure to Protect Safeguards Information

This issue was previously dispositioned as a Severity Level III violation (EA 97-585).

S8.2.6 (Closed) LER 50-361/97-03;-362/97-03: Security Computer System Out of Service

The licensee was previously issued a violation in Inspection Report 50-361/97-24; 50-362/97-24 for failing to report these computer failures. This LER documented the corrective actions for the earlier noncompliance, as well as reported two additional failures. The inspector confirmed during the current inspection that interim corrective actions were in place, and that they were effective in preventing computer failures. Software corrections were ongoing.

S8.2.7 (Closed) LER 50-361/97-04;-362/97-04: Unlocked Weapons Containers

The licensee was previously issued a violation for failing to report instances of unlocked weapons containers. The violation was cited in Inspection Report 50-361/97-24; 50-362/97-24.

S8.2.8 (Closed) LER 50-361/98-01;-362/98-01: Security Computer Failure

The licensee was in the process of making significant changes to the reportability procedure when the computer failed. They did not take into account that adequate compensatory measures were in place before the attempted reboot of the computer. With adequate compensatory measures in place prior to the reboot, this event becomes of minor significance and would not have required an LER to be submitted.

S8.2.9 (Closed) LER 50-361/98-03;-362/98-03: Inadequate Access Authorization/Fitness-for-duty.

This item is identified as a noncited violation in this report. Refer to Section S1.1 for details.

S8.2.10 (Closed) LER 50-361/98-04;-362/98-04: Safeguards Information

The licensee identified several safeguards information documents that were not adequately protected. The discovery of these documents was part of the corrective actions for a previously identified Severity Level III violation (EA 97-585).

S8.3 Followup-Plant Support (92904)

S8.3.1 (Closed) VIO 50-361/9724-01;-362/9724-01: Inadequate Emergency Power Supply

The licensee failed to install a detection zone battery resulting in noncompliance when a power failure occurred. The licensee installed a battery and tested the zone. The inspector reviewed records to confirm that the corrective action was completed.

S8.3.2 (Closed) URI 50-361/9724-02;-362/9724-02: Inadequate Compensatory Measures

The unresolved item is closed and a new item opened as a violation in this report. Refer to Section S2.1 for details.

S8.3.3 (Closed) VIO 50-361/9724-03;-362/9724-03: Failure to Report

The licensee failed to report an incident in which a safeguards contingency cabinet containing weapons and ammunition was left unsecured inside a vital area. The root cause of the violation appeared to be unclear guidance in the reportability procedure. During this inspection, the inspector reviewed changes to the procedure. The change to the procedure appears to be an effective corrective action.

S8.3.4 (Closed) VIO 50-361/9724-05;-362/9724-05: Failure to Secure Contingency Weapons

On two separate occasions, security contingency weapons cabinets were left unsecured. The licensee changed the locks in order to prevent the keys from being removed until the locks are secured. There has been no recurrence of the violation. The corrective action appears to be effective.

S8.3.5 (Closed) URI 50-361/9724-04;-362/9724-04: Failure to Protect Safeguards Information

This Item was previously dispositioned as a Severity Level III violation (EA 97-585).

S8.3.6 (Open) VIO 50-361/E 97-585; -362/E 97-585: Failure to Protect Safeguards Information

The violation was issued as a Severity Level III violation. The violation will be left open because the corrective action is not complete. Some minor documents are still being discovered as part of the corrective action (See Section S8.2.10). This item will be reviewed further in a future inspection.

S8.3.7 (Closed) URI 50-361/9803-07;-362/9803-07: Diesel Fuel Oil Filtration

Refer to Section S8.2.1 for details.

V. Management Meetings

X1 Exit Meeting Summary

The inspector presented the preliminary inspection results to members of licensee management at the conclusion of the inspection on July 17, 1998. Final exit briefings were conducted telephonically on August 21 and October 7, 1998. The licensee acknowledged the findings presented during the August 21 phone call; however, they disagreed that the characterization of the access authorization issue constituted a potential Severity Level III violation. Upon further review, it was communicated to the licensee during the October 7, 1998, phone call that the access authorization issue was a noncited violation.

ATTACHMENT 1

PARTIAL LIST OF PERSONS CONTACTED

Licensee

R. Krieger, Vice President, Nuclear Generation
F. Barvara, Instrumentation and Calibration Engineer
S. Blue, Supervisor, Fitness-for-Duty
G. Broussard, Security Operations Supervisor
L. Camacho, Administrative Supervisor
S. Chun, Security System Engineer
G. Cook, Supervisor Compliance
T. Cook, Security Shift Commander
M. Flannery, Supervisor, Central Processing Facility
T. Frey, Compliance Coordinator
G. Gibson, Manager, Compliance
K. Gross, Central Document Management Supervisor
D. Herbst, Manager, Quality
R. Jones, Supervisor, Security Systems
J. Matthews, Supervisor, Security Business and Personnel
H. Newton, Manager, Support Services
G. Plumlee, Supervisor, Security Compliance
M. Ramsey, Root Cause Engineer
R. Reiss, Supervisor, Security Self Assessment
D. Rolph, Administration Supervisor
A. Scherer, Manager, Nuclear Regulatory Affairs
K. Slagle, Manager, Nuclear Oversight
R. Todd, Supervisor, Security Equipment and Training
J. Wallace, Security Manager
L. Youde, Industrial Engineering
M. Zar, Quality Assurance Engineer

NRC

J. Sloan, Senior Resident Inspector

INSPECTION PROCEDURES USED

IP 81700	Physical Security Program for Power Reactors
IP 92904	Followup
IP 92700	Onsite Review of Event Reports

ITEMS OPENED AND CLOSED

Opened

50-361;-362/9812-01	NCV	Inadequate Access Authorization/Fitness-for-Duty
50-361;-362/9812-02	NCV	Inadequate Access Control - Personnel
50-361;-362/9812-03	VIO	Inadequate Compensatory Measures
50-361;-362/9812-04	VIO	Inaccurate Information Submitted to the NRC
50-361;-362/9812-05	NCV	Inadequate Assessment Aids/Inattentive Security Officers

Closed

50-361;-362/9812-01	NCV	Inadequate Access Authorization/Fitness-for-Duty
50-361;-362/9812-02	NCV	Inadequate Access Control - Personnel
50-361;-362/9812-03	VIO	Inadequate Compensatory Measures
50-361;-362/9812-05	NCV	Inadequate Assessment Aids/Inattentive Security Officers
50-361;-362/9724-01	VIO	Inadequate Emergency Power Supply
50-361;-362/9724-02	URI	Inadequate Compensatory Measures
50-361;-362/9724-03	VIO	Failure to Report
50-361;-362/9724-04	URI	Failure to Protect Safeguards Information
50-361;-362/9724-05	VIO	Failure to Secure Contingency Weapons
50-361;-362/9803-07	URI	Diesel Fuel Oil Filtration
50-361;-362/98-02	LER	Diesel Fuel Oil Filtration
50-361;-362/95-02	LER	Loss of Safeguards Information in US Mail
50-361;-362/96-02	LER	Missed Surveillance
50-361;-362/96-03	LER	Security Alarm Not Posted
50-361;-362/97-02	LER	Failure to Protect Safeguards Information
50-361;-362/97-02-01	LER	Failure to Protect Safeguards Information
50-361;-362/97-03	LER	Security Computer System Out of Service
50-361;-362/97-04	LER	Unlocked Weapons Containers
50-361;-362/98-01	LER	Security Computer Failure
50-361;-362/98-03	LER	Inadequate Access Authorization/Fitness-for-Duty
50-361;-362/98-04	LER	Safeguards Information

LIST OF DOCUMENTS REVIEWED

Security Procedure SO123-IV-6.8, Revision 2, "Protected Area and Vital Area Barrier Patrols"

Security Procedure SO123-IV-11.2, Revision 4, "Reporting Safeguards Events"

Security Procedure SO123-XV-7, Revision 8, "Drug and Alcohol Testing Program for Protected Area Access and Assignment to Emergency Operations Facility Duties"

Security Procedure SO123-IV-5.1, Revision 7, "Protected and Vital Area Access"

Security Procedure SO123-IV-4.4, Revision 5, "Security Lock and Key Control"

Security Procedure SO123-XV-2.4, Revision 3, "Security Responsibilities of Site Employees"

Security Procedure SO 123-XXIII-4, Revision 2, "Site Access"

Security Procedure SO123-XXIII-4.1, Revision 1, "Authorization and Issuance of Security Photo Identification Badges"

Security Procedure SO123-XV-6, Revision 5, "Fitness-for-Duty (Behavior Observation)"

Nuclear Organization Directive D-006, Revision 1, "Fitness-for-Duty"

Security Event Logs, First, Second, and Third Quarters, 1998

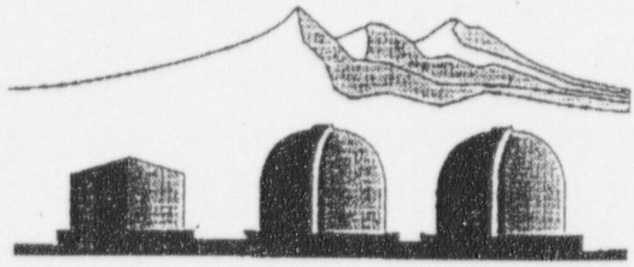
Licensee Action Request Nos. 980301717-01; 980401023-01

Surveillance Reports SOS-036-97 and SOS-037-97

ATTACHMENT 2

ATTACH FACSIMILE AS ATTACHMENT 2.

FAX COVER SHEET



Southern California Edison Company

5000 Pacific Coast Highway
San Clemente, CA 92672

Date:

TO: Bruce Earnest Voice: Fax: (817) 860-8212

FROM: Geoff Cook Voice: (949) 368-7571 Fax: (714) 368-7575

Number of Pages (including cover sheet): 20

NUCLEAR REG AFFAIRS Fax:949-368-7575 Sep 24 '98 11:05 P.01

PROTECTED AREA ACCESS AUTHORIZATION
INCIDENT OF MARCH 9-10, 1998

I. Background

On March 9, 1998, Collection Site Personnel (CSP), while processing pre-access drug screening information, made a data entry error in the T2000 computer program. The error resulted in a contract worker being granted unescorted access to the Protected Area (PA) prior to passing a required pre-access drug screening test.

On March 10, 1998, the individual entered the PA for approximately three hours, when it was discovered that the individual had a presumptive positive result on their pre-access drug screening test. Upon discovery of the error, steps were taken to have the individual escorted out of the PA. On March 16, 1998, SCE's Medical Review Officer (MRO) declared a "positive" drug test result for the contract worker.

It is noted that, since implementing corrective actions for an access authorization violation in 1995, SCE has processed at least 7193 security badges, with this being the only example where an inappropriate individual was granted a security badge. This constitutes a program success rate of 99.9%.

II. SCE Fitness For Duty (FFD) Testing Program (Pre-access)

In order to receive unescorted access to the Protected Area (PA), all individuals are required to pass FFD requirements in accordance with 10CFR26. The FFD testing program for initial site access consists, in part, of a drug screening test and an alcohol breath analysis test. The individual must provide an acceptable urine sample, as determined by measuring quantity, temperature, specific gravity and PH of the sample, and the sample is then analyzed for the presence of specific drugs. The results of the alcohol test are indicated by the alcohol measuring device, and are immediately known to the CSP conducting the test. The drug screening analysis is performed by the onsite prescreen Specialist, normally within a few hours of collecting the sample. ***The CSP collecting the urine sample does not usually perform the drug screening analysis, and did not perform the drug screening analysis on March 9, 1998.***

Behavioral observation is also part of the FFD program. In order to receive a security badge, all personnel must complete a FFD training course, which includes supervisory level training for identifying aberrant behavior associated with the use of drugs or alcohol. Additionally, if any unusual or aberrant behavior is observed during the pre-access testing process, CSPs are instructed to document the behavior in the Permanent Record Log Book maintained at the Drug Screening Facility.

III. Chronology of Events (See Attached Timeline)

March 9, 1998, Morning

The contract worker entered the Central Processing Facility (CPF) on the morning of March 9, 1998, and began the process for obtaining an unescorted access badge. Between the time the individual entered the CPF until approximately 1030 hours, the individual completed the required Site Access and Fitness For Duty courses, with passing test scores. At 1153 hours, the individual was logged in at the Drug Screening Facility. The CSP obtained a valid urine specimen (i.e., the specimen's quantity, temperature, specific gravity, and PH level were within acceptable limits), and the individual passed an alcohol breath analysis test. The individual exited the Drug Screening Facility at approximately 1300 hours on March 9, 1998.

March 9, 1998, 1300 - 1530 Hours

Sometime between 1300 and approximately 1500 hours, a CSP entered the individual's drug and alcohol screening information in the T2000 computer program, which is the software program used at SONGS for processing security badges for unescorted access. The T2000 FFD program contains two parts; a "Submittal" screen and a "Results" screen. The "Submittal" screen is completed after the individual has provided an acceptable urine sample (i.e., quantity, temperature, specific gravity and PH are within limits) and passed the alcohol test, and the "Results" screen is completed after the individual has passed the pre-access urine drug test. Both screens must be completed for a badge to be issued by CPF.

The attached Figure 1 shows a printout of the FFD program computer screen. ***The "Submittal" and "Results" screens are visually identical.*** In order to enter information on the "Submittal" screen, the CSP uses the mouse to click on the "Submittal" button. In order to enter information on the "Results" screen, the CSP uses the mouse to click on the "Results" button. Both screens require the CSP to enter the following information fields for the individual being tested: social security number, date, test type, and results. The test type identifies if it is a random or initial (pre-access) drug test, or other type. On the "Submittal" screen, a "P" is entered in the results field when an acceptable urine sample is attained. On the "Results" screen, a "P" is entered in the results field when passing results are obtained for the drug/alcohol test (i.e., test results are negative for drug usage). ***Unacceptable urine samples and presumptive positive drug test results are NOT entered in T2000.***

> (Note: The process described here for processing individuals in T2000 was the process in place on March 9, 1998. As part of the corrective actions for LER 98-003, the process was enhanced to prevent recurrence of the type of incident that occurred on March 9; e.g., the codes used for the "Submittal" screen result field are now different than the codes used for the "Result" screen result field.)

While entering the individual's drug screening information, the CSP ***inadvertently and unknowingly*** used the mouse to click on the "Results" screen when she intended to click on the

"Submittal" screen. The computer screen "buttons" for the two screens are located right next to each other, and the two computer screens are visually identical. The CSP then ***unknowingly*** completed the "Results" screen for the individual, rather than the "Submittal" screen. Consequently, by entering a "P" in the results field of the "Results" screen, the CSP ***unintentionally and unknowingly*** entered a "passing" drug test result for the individual

At 1509:03 hours on the same day (after the initial data entry error had been made), a second CSP verified the "Submittal" screen information. The purpose of this verification was to verify that all individuals, who had been entered in the Permanent Record Log Book as having provided valid chemical test samples (i.e., urine quantity, temperature, specific gravity and PH were within acceptance limits, and negative alcohol breath test), were also entered on the T2000 "Submittal" screen. On March 9, 1998, there were 30 individuals tested at the Mesa Site Collection Facility. To complete the verification, the CSP accessed a review data screen for submittal entries only. Starting with the first entry in the Permanent Record Log Book, the CSP found the corresponding social security number on the group "Submittal" screen, and then verified the individual's social security number, date and test type. During this verification, the second CSP identified a Permanent Record Log Book entry, with a valid chemical test specimen, that was not entered on the T2000 "Submittal" screen. This entry was for the individual who earlier had been ***inadvertently*** entered on the "Result" screen rather than the "Submittal" screen. Since the log book indicated that a valid chemical test sample had been attained, the second CSP created a "Submittal" screen entry for this individual. Consequently, the individual completed "Submittal" and "Result" screens, taken together, now satisfied the FFD requirements for receiving unescorted access to the PA.

The drug screening analysis is performed by an onsite prescreen Specialist some time after the sample has been collected. The Specialist separates the "Presumptive Positive" tests (i.e., presence of drugs has been detected) from the "Negative" tests (i.e., no drugs detected). The paperwork for each "Negative" test result has a yellow top sheet that is stamped to indicate the test was passed. The paperwork for each "Presumptive Positive" test result has a white top sheet with no stamp. The Specialist enters the "Presumptive Positive" test results on a "Send Out List" which is provided to the CSPs to ensure that the samples are sent to the offsite laboratory for confirmatory analysis, and also notifies the FFD Supervisor that a presumptive positive result was obtained. As the screening tests are completed, the Specialist provides the paperwork to the CSPs. The CSPs maintain the "Presumptive Positive" test results in a single folder, and all "Negative" test results are entered on the T2000 "Results" screen. ***"Presumptive Positive" test results are NOT entered in T2000, and not specifically reviewed by the CSPs.***

On March 9, 1998, two aliquots from the suspect individual were analyzed by the prescreen Specialist and determined to contain methamphetamine. The Specialist concluded that the individual was "Presumptive Positive," and subsequently entered the test result on the "Send Out List," and also notified the FFD Supervisor. The paperwork for the individual was processed as a "Presumptive Positive," and provided to the CSPs. One of the CSPs placed the paperwork for

the "Presumptive Positive" test in the appropriate folder. *The "Presumptive Positive" test result was not entered in T2000.*

The CSPs also perform a verification of the entries on the T2000 "Results" screen. In this case, the CSP performing the verification accessed a group "Results" screen that included all individuals tested on March 9, 1998, that had "Negative" test results. Using the completed paperwork for the "Negative" test results, the CSP verified that there was a corresponding entry on the T2000 "Results" screen. The purpose of this verification was to ensure that there was a T2000 "Results" screen entry for all individuals with paperwork showing a passing drug test. *Using the completed paperwork for the "Negative" test results, this verification would identify if there was a missing T2000 "Results" entry, but would not be expected to identify if there was an additional "Results" entry, as was the case on March 9, 1998.*

March 9, 1998, 2018 Hours

Since T2000 now had completed "Submittal" and "Result" screens for this individual, CPF personnel concluded that FFD requirements had been satisfied, as displayed in T2000, which allowed for the issuance of a security badge. The security badge was activated in the computer in the Central Alarm Station at 2018 for Protected Area access only. (NOTE: T2000 will not allow the issuance of a security badge without a "Submittal" and "Result" completed within the previous 60 days. Since both were completed on March 9, 1998, this requirement was met.)

March 10, 1998, Morning

Security logs show that the individual picked up his badge and entered the PA at 0644:33. There is no evidence that the individual was accompanied when he entered the PA. He apparently proceeded directly to his assigned assembly area for an 0700 pre-job briefing. Several SCE and contract workers accompanied the individual at the pre-job brief and while he was working in the PA. Although it appears that the individual was accompanied the majority of the time, *there is insufficient evidence to indicate that the individual was accompanied 100% of the time.*

At approximately 0930, the CPF Supervisor was reviewing a pending security badge report. During the review, he identified critical path workers that had drug screen submittals pending, but did not have results. Based on this information, he met with the CSPs and identified that there was a discrepancy in the number of pending badges (badges awaiting drug test results due to presumptive positive results). The Supervisor identified the improperly issued badge, and immediately directed the Screening Supervisor to contact Security to have the badge deactivated. The Screening Supervisor then called the SCE supervisor of the individual who had received the badge, and instructed him to have the individual escorted out of the PA and have him return to CPF.

The individual was escorted to the exit turnstile, and exited the PA at 0937:02. The individual's badge was deactivated at 0942. *The individual was in the PA for approximately 2 hours and 53 minutes with a security badge.* The individual subsequently reentered the PA with an escort

badge and escort.

March 10 - 13, 1998
The individual completed his work under an escort badge while accompanied by an escort and departed the site.

March 16, 1998
The MRO declared a "Positive" test result after reviewing the report from the Health and Human Services certified laboratory that performed the confirmatory drug test analysis. SCE made the required one hour notification to the NRC Operations Center, in accordance with 10CFR73.71(b)(1).

April 8, 1998
SCE submitted the required Licensee Event Report in accordance with 10CFR73.71(d).

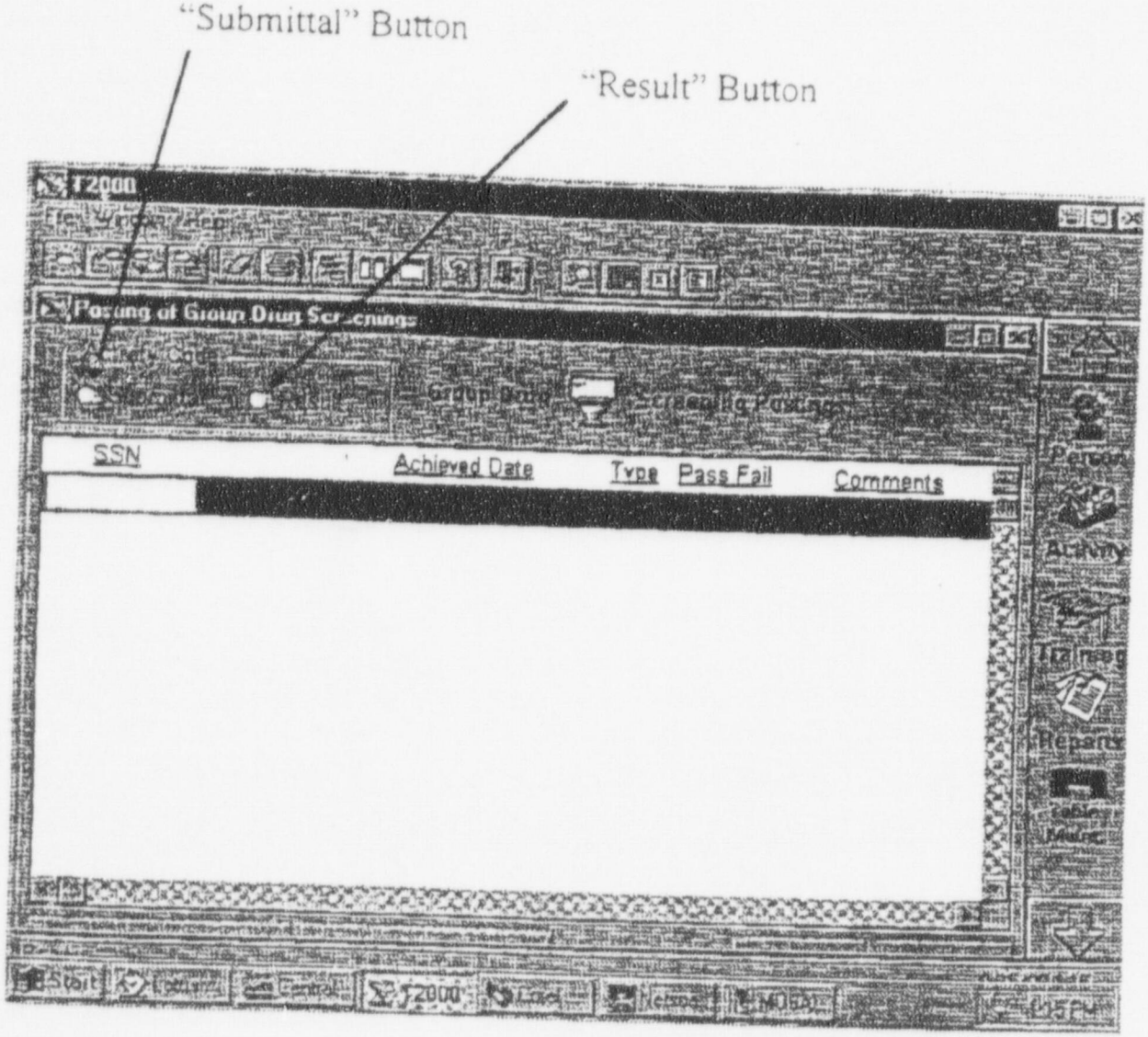
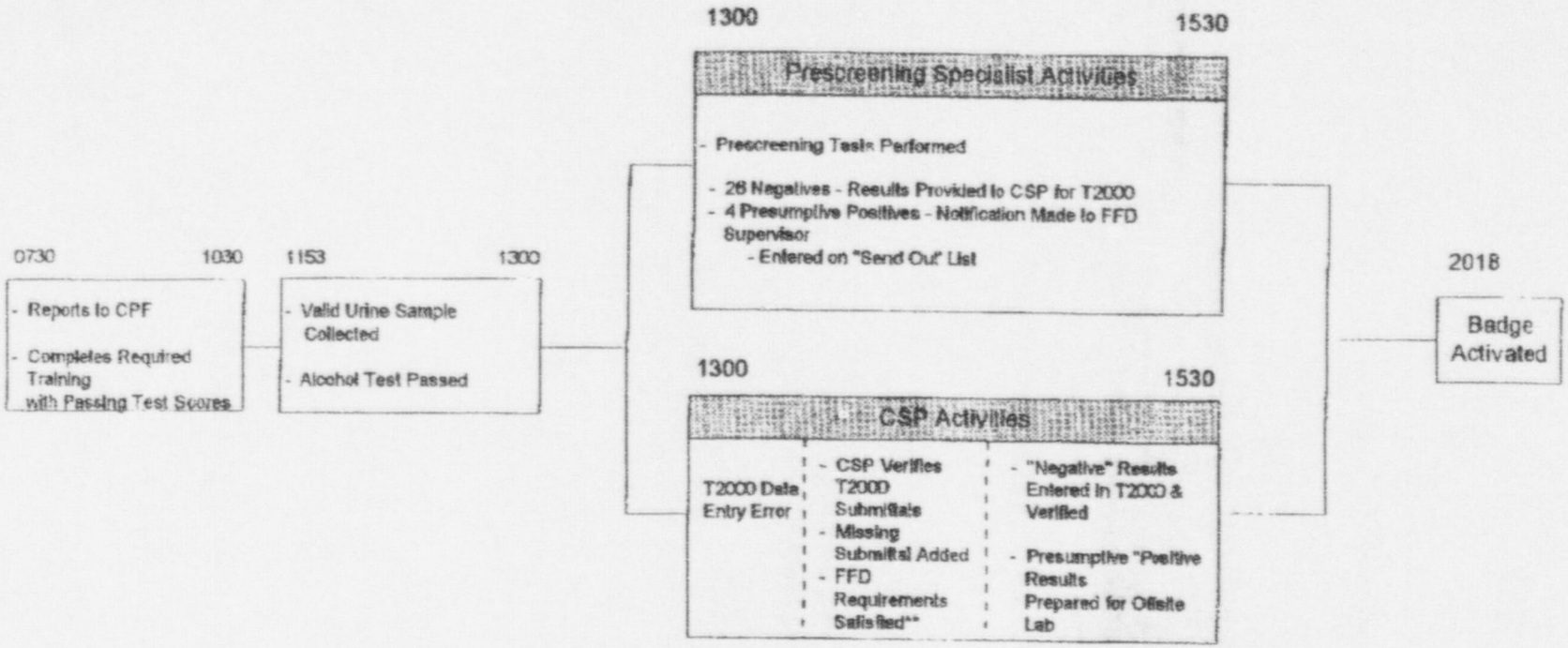


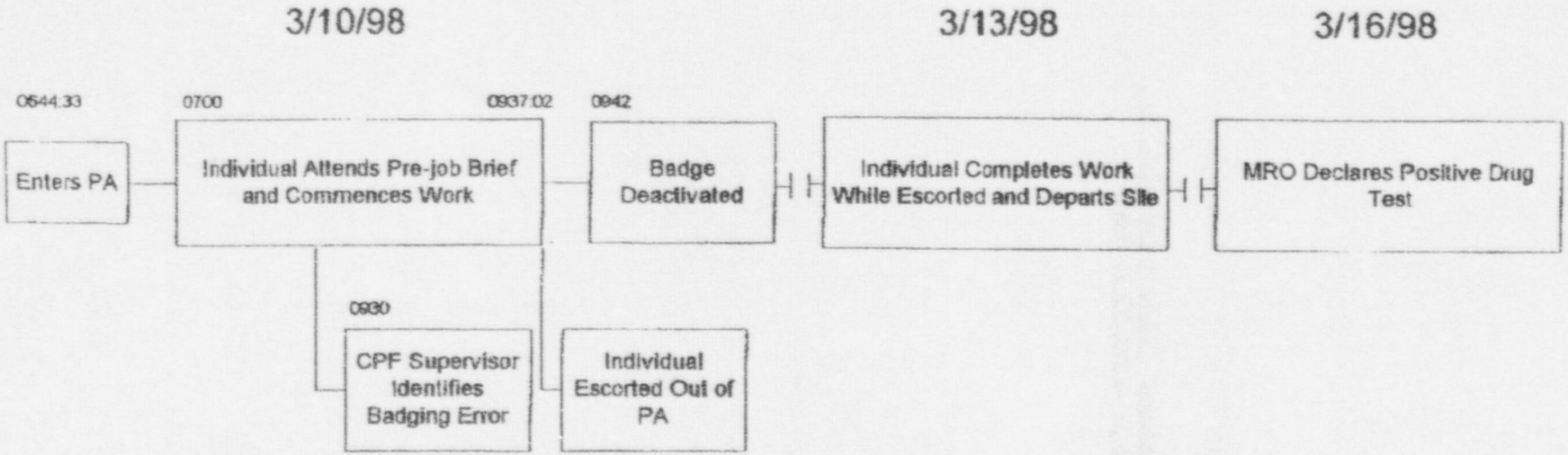
Figure 1 - T2000 FFD Computer Screen

Timeline for Access Authorization Incident

3/9/98



Timeline for Access Authorization Incident



NRA ASSESSMENT OF PROTECTED AREA ACCESS AUTHORIZATION
INCIDENT OF MARCH 9-10, 1998

I. Assessment of Applicable Regulatory Requirements/Guidance

Requirement - 10CFR26 Fitness For Duty Programs

10CFR26.10 General Performance Objectives

Fitness-for-duty programs must:

(a) Provide ***reasonable assurance*** that nuclear power plant personnel,... will perform their tasks in a reliable and trustworthy manner and are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause, which in any way adversely affects their ability to safely and competently perform their duties;

(b) Provide ***reasonable measures*** for the early detection of persons who are not fit to perform activities within the scope of this part;

10CFR26.24 Chemical and alcohol testing

(a) To provide a means to deter and detect substance abuse, the licensee shall implement the following chemical testing programs for persons subject to this part:

(1) ***Testing within 60 days*** prior to the initial granting of unescorted access to protected areas or assignment to activities within the scope of this part.

Note: Although this requirement is germane to the issue, there is no apparent disagreement that SCE has a chemical testing program in place that meets this requirement.

10CFR26.27 Management actions and sanctions to be imposed

(b) Each licensee subject to this part shall, as a minimum, take the following actions. Nothing herein shall prohibit the licensee from taking more stringent action.

(1) Impaired workers, or those whose fitness may be questionable, ***shall be removed from activities*** within the scope of this part, and may be

returned only after determined to be fit to safely and competently perform activities within the scope of this part.

Applicable NRC Guidance on 10CFR26

Enforcement Policy, Supplement VII - Miscellaneous Matters

C. Severity Level III - Violations involving for example:

6. A failure to complete a suitable inquiry on the basis of 10 CFR Part 26, keep records concerning the denial of access, or respond to inquiries concerning denials of access so that, as a result of the failure, a person previously denied access for fitness-for-duty reasons was improperly granted access;

7. A failure to take the required action for a person confirmed to have been tested positive for illegal drug use or take action for onsite alcohol use; not amounting to a Severity Level II violation;

9. A breakdown in the fitness-for-duty program involving a number of violations of the basic elements of the fitness-for-duty program that collectively reflect a significant lack of attention or carelessness towards meeting the objectives of 10 CFR 26.10;

D. Severity Level IV - Violations involving for example:

4. Violations of the requirements of Part 26 of more than minor significance

Enforcement Manual, Section 7.4, "Enforcement Actions Involving FFD"

7.4.1 Action against the facility licensee

In citing the facility licensee, it is important to note that ***it is not the unfit person that establishes the violation*** but rather the licensee's failures to implement the program, including those of its contractors and vendors, that creates the violation...

Supplement VII of the Enforcement Policy provides examples of violations where the facility licensee failed to meet the requirements of 10 CFR Part 26...

The examples for Severity Level III are significant because they represent

significant individual violations or significant breakdowns in basic elements of a FFD program.... A breakdown in the program categorized at a Severity Level III will normally involve ***more than one significant failure of a single element or single failures of a number of elements***.

NUREG/CR-5227, "Fitness for Duty in the Nuclear Power Industry: A Review of Technical Issues"

Page vii

"...Furthermore, ***drug levels in the urine are not directly correlated to impairment***."

Page 5-1

"...Finally, the correlation between impairment and the level of drug or drug metabolite in the urine varies, and ***it is difficult to determine the appropriate cut-off levels that will identify the impaired persons***."

Page 5-2

"The ***greatest problem with urinalysis is interpretation of the results*** (Sutheimer, Yarborough, Hepler, and Sunshine, 1985). The concentration of a drug or drug metabolite in the urine does not provide information about drugs pharmacologically affecting the person's system nor does it provide information about impairment (Hawks and Chaing, 1986)"

"...Hence, a positive confirmed test result indicates only that an individual has ingested the drug recently. ***A positive result does not provide information about*** the frequency of use, pattern of use, addiction, legitimacy of use, or ***whether the person was under the influence of the drug when the urine was collected*** (Manno, 1986a)."

"Because of the numerous factors that influence the concentration of a drug or drug metabolite in the urine, ***it is impossible to set cut-off levels that relate directly to performance impairment***."

"...Thus ***it is difficult or impossible to make definitive statements linking drug levels in the system to impairment*** (Ambre, personal communication, January 26, 1988)."

Assessment of 10CFR26 Implementation

Example C.6 from the Enforcement Policy, Supplement VII, ***applies to personal background checks*** and is not relevant to the incident at SONGS.

Example C.7 from the Enforcement Policy, Supplement VII, is not relevant to the incident at SONGS since it ***involves confirmed positive test results***; the incident at SONGS involved a pre-access presumptive (not confirmed) positive test. The individual's unescorted access privilege had already been removed when the confirmed positive drug test result was declared by the MRO.

The incident at SONGS does not meet example C.9 of the Enforcement Policy, Supplement VII, since it describes a programmatic breakdown involving a number of violations. The incident at SONGS resulted from a ***random isolated personnel error*** (cognitive).

Example D.4 (Level IV) appears to be the most relevant example in this section of the Enforcement Policy since the incident at SONGS might be considered to be of more than minor significance. In addition, under the terms of EGM 98-006, this would appear to be recategorized as a noncited violation.

Enforcement Manual, Section 7.4, specifically references the Severity Level III examples described in Supplement VII of the Enforcement Policy. ***The incident at SONGS involved a random isolated personnel error***, not a programmatic breakdown, and does not appear to fit the above Severity Level III description. There was not more than one significant failure of a single element, nor single failures of a number of elements. Since March 1, 1995, when corrective actions were implemented for a FFD/Access Authorization violation, through August 31, 1998, SCE processed 7193 security badges, with this being the only example where an inappropriate individual was granted a security badge. This supports the conclusion that the incident at SONGS involved an isolated random personnel error.

NUREG/CR-5227 emphasizes that ***a positive result on a urine drug test does not indicate that the individual was impaired or under the influence of drugs.***

Requirement - 10CFR73 Physical Protection of Plants and Materials

73.56 Personnel access authorization requirements for nuclear power plants.

(a) General

(1) ...By April 27, 1992, the required access authorization program must be incorporated into the site Physical Security Plan as provided for by 10 CFR 50.54(p)(2) and implemented.

[The following is from the applicable section of the Physical Security Plan (PSP), and a plant procedure:

Section 4.4 of the PSP states that badge issuance and control are described in site procedures.

Site Procedure SO123-XV-7, "Drug and Alcohol Testing Program For Protected Area Access and Assignment to Emergency Operations Facility Duties"

Step 6.3 Processing Criteria for Unescorted Access and/or EOF Duties

6.3.1 A badge granting unescorted access into the PA shall not be issued or EOF duties assigned until the Central Processing Facility (CPF) has ***recorded all requirements as satisfied*** including the fulfillment of a drug and alcohol test within 60 days prior to the initial granting of access and initiation of suitable inquiry.]

73.56(b) General performance objective and requirements.

(1) The licensee shall establish and maintain an access authorization program granting individuals unescorted access to protected and vital areas with the ***objective of providing high assurance*** that individuals granted unescorted access are trustworthy and reliable, and do not constitute an ***unreasonable risk*** to the health and safety of the public including a potential to commit radiological sabotage.

(2) Except as provided for in paragraphs (c) and (d) of this section, the unescorted access authorization program must include the following:

(i) A ***background investigation*** designed to identify past actions which are indicative of an individual's future reliability within a protected or vital area of a nuclear power reactor. As a minimum, the background investigation must verify an individual's employment history, education history, credit history, criminal history, military service, and verify an individual's character and reputation.

(ii) A ***psychological assessment*** designed to evaluate the possible impact of any noted psychological characteristics which may have a bearing on trustworthiness and reliability.

(iii) ***Behavioral observation***, conducted by supervisors and management personnel, designed to detect individual behavioral changes which, if left unattended, could lead to acts detrimental to the public health and safety.

(3) The licensee shall base its decision to grant, deny, revoke, or continue an unescorted access authorization on review and evaluation of ***all pertinent information developed***.

Applicable NRC Guidance on 10CFR73/Access Authorization

Enforcement Policy, Supplement III - Safeguards

C. Severity Level III - Violations involving for example:

7. A failure to perform an appropriate evaluation or background investigation so that information relevant to the access determination was ***not obtained or considered*** and as a result a person, who would likely not have been granted access by the licensee, if the required investigation or evaluation had been performed, was granted access;...

Enforcement Manual, Section 8.3.2, "Access Control"

The severity level of an access control violation is determined by: (1) the ease of exploitation of the vulnerability including its predictability and the ease of passage created by that violation, (2) the intent of the intruder, and (3) the combined integrity of both protected area and vital area/material access area barriers...

The intent of the intruder must also be considered. ***Unauthorized intrusions by licensee employees without malicious intent are not by themselves of significant concern...***

Assessment of 10CFR73 Implementation

Although the example in the Enforcement Policy, Supplement III, may appear relevant, the incident at SONGS was caused by a ***random human error*** (data entry keystroke error made by CSP), and therefore, ***unescorted access was not granted based on information "not obtained or considered" by SCE.***

Section 8.3.2 of the Enforcement Manual provides guidance on activities addressed in Supplement III of the Enforcement Policy. The individual granted unescorted access ***did not display any malicious intent*** as evidenced by the fact that the individual completed his assigned work assignment in an acceptable manner. The individual did not have access to vital areas, and the integrity of both protected area and vital area/material access area barriers was not compromised. ***The root cause of the violation was a random isolated personnel error (cognitive). The error was not predictable and could not likely be exploited.***

Neither the regulations nor any of the applicable regulatory guidance documents appear to provide any performance criteria for assessing whether the program implementation meets the applicable acceptance standard of ensuring ***"high assurance."*** The FFD and Access Authorization programs in place on March 9, 1998 (and today), appear to provide "high assurance." This conclusion is supported by the fact that, since implementing corrective actions for an Access Authorization/FFD violation in 1995, 7193 security badges have been processed at SONGS. The incident on March 9, 1998, that was caused by a random human error, is the only example where an inappropriate individual was granted a security badge. ***This represents a success rate of 99.9%, which meets or exceeds the regulatory requirement for providing "high" assurance.***

As a comparison, 10CFR73.55(a) requires that the onsite physical protection system provide ***high assurance*** that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. Regulatory Guide (RG) 5.44, "Perimeter Intrusion Alarm Systems," provides performance testing criteria for determining the acceptability of the Protected Area Intrusion Detection System (IDS), a part of the physical protection system. The RG specifies that the IDS must be able to detect intruders with at least a 90% probability with 95% confidence. Although no similar type of performance criteria was found for measuring the acceptability of the FFD or Access Authorization programs,

the aforementioned program success rate of 99.9% meets or exceeds the regulatory guidance for satisfying a "high assurance" performance standard.

Mitigating Factors to be Considered:

There is substantial evidence that the individual who was inappropriately granted unescorted access was not under the influence of drugs, or impaired, on March 9 or March 10:

NUREG/CR-5227, "Fitness for Duty in the Nuclear Power Industry: A Review of Technical Issues," pages, vii, 5-1 and 5-2, note that drug levels in the urine do not provide information about impairment.

The CSP who interacted with the individual on March 9, 1998, are instructed to look for, and document, any unusual behavior. These CSP did not identify any behavior to indicate that the suspect individual was impaired.

The suspect individual completed and received passing test scores for the required Site Access and Fitness For Duty training courses, within hours prior to taking the drug test.

While working in the PA on March 10, the individual was apparently accompanied the majority of the time by other unescorted contract workers and/or SCE employees who had received supervisory level training in recognizing aberrant behavior. All individuals who have been identified as being with the individual while in the PA have stated that they did not observe any unusual or aberrant behavior.

The physician in charge of the laboratory that performed the confirmatory testing indicated (during a telephone call with SCE) that, based on the confirmatory drug test results, and the fact that the individual demonstrated no unusual or aberrant behavior, it was his medical opinion that the individual was not likely impaired on March 9, 1998.

The individual did not have access to any vital areas.

The root cause of the violation was a ***random isolated personnel error*** (cognitive); it was not willful, repetitive, or indicative of a programmatic breakdown. Since implementing corrective actions for a FFD/Access Authorization violation in 1995, SCE processed 7193 security badges, with this being the only badge that was issued to an inappropriate person. This constitutes a program success rate of 99.9%.

II. Regulatory Assessment

A review and assessment of the applicable regulations and regulatory guidance associated with the FFD and Access Authorization programs, and of SCE's procedures for these programs that were in place on March 9, 1998, would lead to the conclusion that ***the incident did not involve a violation of the regulations***. The inappropriate granting of a security badge to a contract worker involved an ***unintentional random human error*** (data entry keystroke error), which in itself, is not a violation of federal regulations. The basis for this conclusion is summarized below.

10CFR26 and 10CFR73.56 provide the regulatory requirements for FFD and Access Authorization programs respectively. 10CFR26.10 requires that the FFD program provide ***reasonable assurance*** that nuclear power plant personnel are not under the influence of illegal substances. 10CFR73.56 requires that the Access Authorization program provide ***high assurance*** that individuals granted unescorted access are trustworthy and reliable, and do not constitute an ***unreasonable*** risk to the health and safety of the public. These regulations also describe the specific elements that must be included in each program. For example, 10CFR26.24 specifies that the FFD program must include chemical testing within 60 days prior to granting any individual unescorted access to the PA, and 10CFR73.56(b)(2) requires that the Access Authorization program include a background investigation, psychological assessment, and behavioral observation.

Neither the regulations nor any of the applicable regulatory guidance documents appear to provide any performance criteria for assessing whether the program implementation meets the applicable acceptance standards of ensuring ***"reasonable assurance"*** and ***"high assurance." Nevertheless, both citations clearly eliminate "perfection" as the regulatory standard.***

The FFD and Access Authorization programs in place on March 9, 1998 (and today), appear to provide both "reasonable assurance" and "high assurance." This conclusion is supported by the fact that, since implementing corrective actions for an Access Authorization/FFD violation in 1995, 7193 security badges have been processed at SONGS. The incident on March 9, 1998, that was caused by a random human error, is the only example where an inappropriate individual was granted a security badge. This represents a success rate of 99.9%. ***A 99.9% program success rate meets or exceeds the regulatory requirement for providing "reasonable" and "high" assurance.***

As a comparison, 10CFR73.55(a) requires that the onsite physical protection system provide ***high assurance*** that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

Regulatory Guide (RG) 5.44, "Perimeter Intrusion Alarm Systems," provides performance testing criteria for determining the acceptability of the Protected Area Intrusion Detection System (IDS), a part of the physical protection system. The RG specifies that the IDS must be able to detect intruders with at least a 90% probability with 95% confidence. Although no similar type of performance was found for measuring the acceptability of FFD or Access Authorization programs, ***the aforementioned program success rate of 99.9% meets or exceeds the regulatory guidance for satisfying a "high assurance" performance standard.***

In addition to the discussion above, the following information is provided to further demonstrate that the incident that occurred on March 9, 1998, did not involve a violation of the regulations:

> With regard to FFD program violations, the Enforcement Manual, Section 7.4.1, notes that ***it is not the unfit person that establishes the violation***, but rather it is the licensee's failure to implement the program. On March 9 and 10, 1998, all aspects of the FFD and Access Authorization programs were reasonably implemented. The error that resulted in issuing the security badge to an inappropriate individual was an unintentional random human error, and a program was in place that met or exceeded (99.9%) the regulatory standards of ***"reasonable assurance"*** and/or ***"high assurance."***.
>
> Further, there is substantial evidence to suggest that the individual inappropriately granted unescorted access was not impaired during pre-access drug testing or while in the PA on March 10, 1998. This evidence includes the following: (1) within hours prior to taking the drug test, the person passed examinations for 2 courses required as part of satisfying badging requirements; (2) personnel who interacted with and accompanied the individual on both days indicated that the individual displayed no unusual or aberrant behavior; and (3) the physician in charge of the HHS certified laboratory that processed the confirmatory urine analysis provided a medical opinion that the individual was not likely impaired on March 9.

Notwithstanding the above discussion, the following is an assessment to demonstrate that, even if it is concluded that a violation occurred, the incident on March 9, 1998, appears to satisfy the criteria in the Enforcement Policy, Section VII.B.1, and in Enforcement Guidance Memorandum 98-006 for a Noncited Violation.

Factors Supporting Noncited Violation (Enforcement Policy and EGM 98-006):

> *The violation was self-identified.*
>
> > The CPF Supervisor, while reviewing a report of pending security badges with the CSP, identified that a security badge had been issued that had pending drug test results.

The violation could not reasonably be expected to have been prevented by the licensee's corrective action for a previous violation or a previous licensee finding that occurred within the past 2 years or the past 2 inspections.

SCE received a Level IV violation in 1995 when three individuals were granted unescorted access before the results of the pre-access drug tests were processed. This violation had a different root cause, and the corrective actions could not reasonably have been expected to prevent the current violation.

It was or will be corrected within a reasonable time...including immediate corrective action and comprehensive corrective action to prevent recurrence.

The individual's badge was terminated, and the individual was escorted out of the PA.

The T2000 computer program has been modified such that the "Submittal" and "Results" screens now utilize different codes for the result field.

The T2000 computer program has been modified such that information can not be entered on a "Result" screen until a "Submittal" screen has been completed.

In addition to the T2000 modifications, a hardcopy form is now provided to badge issuing personnel indicating the results of the FFD pre-access requirements have been verified, prior to badge issuance.

The violation was not willful

The root cause of this violation was a ***random isolated personnel error*** (cognitive).