APPENDIX B

U.S. NUCLEAR REGULATORY COMMISSION
REGION IV

Inspection Report: 50-445/92-50
50-446/92-50

Operating License: NPF-87

Construction Permit: CPPR-127

Licensee: TU Electric
Skyway Tower
400 North Olive Street, L.B. 81
Dallas, Texas 75201

Facility Name: Comanche Peak Steam Electric Station, Units 1 & 2

Inspection At: Comanche Peak Site, Glen Rose, Texas

Inspection Conducted: October 22 through December 18, 1992

Team Leader: Mark A. Satorius 1/12/93
Mark A. Satorius, Team Leader, Date
Division of Reactor Projects, Region IV

Team Members: A. B. Earnest, Physical Security Specialist,
Facilities Inspection Programs Section, Region IV

T. W. Dexter, Senior Physical Security Specialist,
Facilities Inspection Programs Section, Region IV

Approved: [signature] 1/15/93
J. P. Jaudon, Deputy Division Director Date
Division of Radiation Safety and
Safeguards, Region IV

Inspection Summary

Areas Inspected: Reactive, announced inspection of the licensee's physical security program as it related to an alleged assault on an armed security officer within the protected area of the station on October 21, 1992. The areas inspected included plant operations response to the event, safeguards contingency plan implementation, security organization, communications, physical security plan and implementing procedures, management effectiveness, and the licensee's fitness-for-duty and access authorization programs.

9301260151 930120
PDR ADOCK 05000445
Q PDR

Results:

- One violation of the Physical Security Plan was identified in the area of behavioral observation training (Section 4.1).
- A noncited violation involving the loss of control of a weapon inside the protected area was identified (Section 4.3).
- The security shift on duty during the contingency event responded well and followed their contingency procedures (Sections 2.1.2 and 2.1.3).
- There was good cooperation and support between the operations staff and the security staff during the contingency event (Section 2.1.3).
- There were adequate numbers of security officers on duty to meet plan and contingency procedure commitments (Section 2.1.1).
- While some minor communications issues were identified by the licensee, overall the communications were good (Section 3).
- The team was concerned that the contingency procedures were heavily weighted toward the outsider threat (Section 2.1.3).
- There was information to suggest a high degree of frustration and low morale among the security officers (Section 5.2).
- The behavioral observation training was heavily weighted in the area of drug and alcohol abuse aberrant behavior without similar emphasis on aberrant behavior caused by other factors (Section 4.1).
- There appeared to be a lack of management effectiveness in the area of behavior observation referral (Section 4.2).

Summary of Inspection Findings:

- Violation 445/9250-04; 446/9250-04 was opened (Section 4.1).
- A noncited violation was identified (Section 4.3).
- Inspection Followup Item 445/9250-01; 446/9250-01 was opened (Section 2.1.4).
- Inspection Followup Item 445/9250-02; 446/9250-02 was opened (Section 3).
- Inspection Followup Item 445/9250-03; 446/9250-03 was opened (Section 4.1).
- Inspection Followup Item 445/9250-05; 446/9250-05 was opened (Section 4.2).

Attachment:

- Attachment - Persons Contacted and Exit Meeting

DETAILS

1 ONSITE RESPONSE TO EVENTS (93702)

1.1 Special Inspection Team Dispatched

On October 22, 1992, Region IV dispatched a team of inspectors to the Comanche Peak Steam Electric Station in response to a security event that had occurred on October 21, 1992. The event was centered around the licensee's discovery of an unconscious security officer who had been the subject of an apparent assault inside the protected area of the station. That event resulted in the loss of control of the security officer's weapon for a short period of time, declaration of a notification of unusual event, and setting the highest security condition of readiness, Security Condition (SECON) Red.

Following this initial, reactive inspection visit from October 22-23, 1992, the team returned to the station several more times during the following weeks. The team returned on October 28, 1992, for 3 days; November 13, 1992, for 1 day; December 14, 1992, for 2 days; and December 18, 1992, for 1 day. These continuation inspection visits were conducted to followup on issues that were identified during the initial portions of the inspection, to receive updates of the licensee's efforts to complete the investigation, and to conduct independent verification, in so much as the team was qualified, of the licensee's investigation results. In addition, the team received regular reports from the licensee by teleconference which provided status of the licensee's investigation.

1.2 Background

At 3:43 a.m., on October 21, 1992, the licensee's security shift supervisor directed the security force into an increased state of readiness by entering SECON Yellow. This action resulted from Central Alarm Station operators being unable to contact an armed security officer within the protected area by either radio transmission or gaitronics announcement. The security shift supervisor immediately directed that a search be initiated and ordered the officer's key card be deactivated; this precluded its use in accessing vital areas. In addition, the control room shift supervisor in the Unit 1 control room was notified and requested to provide operators to assist in the search. At 4:34 a.m., as a contingency initiative, the control room shift supervisor requested and received armed security officers stationed in the control room and at the alternate shutdown panel.

At 4:44 a.m., the missing security officer was found by one of the searching security officers in the turbine building on a fire protection valve room roof. The officer was bound, gagged, appeared to be unconscious, and had apparently sustained some type of injury. In addition, the officer's weapon was missing. The security shift supervisor immediately declared a SECON Red, the highest state of security force readiness, because the officer appeared to have been assaulted, and the weapon was missing.

At 4:50 a.m., the officer's missing weapon, belt, holster, and ammunition was located approximately 25 feet from where the officer had been found. The weapon was secured along with the ammunition and taken to the Central Alarm Station. At 4:52 a.m., the control room shift supervisor declared a Notification of Unusual Event based on the licensee's emergency plan manual.

The injured security officer was transported out of the protected area and an ambulance left the site at 5:03 a.m. enroute to a local hospital with the injured officer. By 5:12 a.m., the licensee had made all notifications required by 10 CFR 50.72.

At 5:24 a.m., after recovering the weapon, conferring with the control room shift supervisor and security force supervisors, the security shift supervisor reduced the SECON level to Yellow. The local law enforcement officials, members of the staff of the Somervell County Sheriff's Department, were notified at 5:06 a.m. and arrived on site at 6:14 a.m.

By 8:00 a.m., the licensee had accounted for everyone who had been on site during the incident, by either key carding personnel offsite or sequestering personnel in preparation for questioning.

At 8:47 a.m., the emergency coordinator terminated the Notification of Unusual Event followed at 9:00 a.m. by the termination of the SECON Yellow condition by security management.

The Somervell County Sheriff's Department immediately began their investigation of the event with jurisdiction being established as a result of an apparent felony assault having been committed against the security officer.

On October 22, 1992, the NRC team arrived on site to begin their inspection. That same date, the allegedly assaulted security officer was released from the hospital. The security officer's injuries consisted of several superficial cuts to the body and bruises on the face.

Subsequent attempts by members of the Somervell County Sheriff's Department to obtain a formal complaint from the allegedly assaulted security officer were unsuccessful. Because of the security officer's refusal to consider pressing charges against any person or persons identified by the investigation, the local law enforcement agency terminated their investigation on October 28, 1992. State and federal investigative agencies were contacted by the licensee in order to determine if those groups would be able to establish jurisdiction and continue the investigation. These efforts were not successful; therefore, the licensee's corporate security investigators assumed the investigation on October 28, 1992.

1.3 Licensee's Investigation and Results

The licensee's corporate security department assembled a comprehensive investigatory team that included criminal investigators, serologists, fingerprint authorities, crime scene forensic specialists, handwriting experts, and psychological interview professionals. This group collectively possessed many years of police and investigative experience. The licensee

also retained the services of two forensic laboratories to process the physical evidence that had been collected by the Somervell County Sheriff's Department and the licensee's staff. In addition, the licensee instituted a quality control system of independent verification by contracting with a renowned forensic pathologist to review all evidence, statements, and conclusions after the licensee's investigation was completed.

The licensee's investigative team assembled a large amount of physical and testimonial evidence prior to arriving at their conclusions. The physical evidence was forwarded to the pathology laboratories retained by the licensee, where it was analyzed for use by the licensee's investigative team. The licensee's investigating team conducted interviews and collected statements from approximately 100 licensee staff members; in addition, the NRC inspection team interviewed approximately 35 licensee employees, to verify independently the licensee's conclusions and to followup on regulatory issues. The NRC team was thoroughly briefed of all findings on a real time basis, either when on site during one of the four onsite periods or via teleconference call.

The NRC team received a final, in-depth briefing on December 14, 1992, by the licensee's investigative team. At that briefing, the licensee's investigative team shared the criminal evidence and numerous investigative documents and findings with the NRC team. In addition, the licensee's investigative findings were independently verified by the forensic pathologist retained for quality control purposes.

Although the team was not able to independently verify all the findings of the licensee's investigation, the team concluded that based on their findings and their review of the licensee's investigation the evidence indicated the incident on October 21, 1992, did not involve collaboration by another individual or individuals.

2 ONSITE RESPONSE TO THE INCIDENT

In addition to maintaining an up-to-date status of the licensee's investigation, the team inspected portions of the licensee's organization to determine regulatory compliance prior to and after the incident.

2.1 Security Force Response

The team reviewed security force procedures for adequacy and appropriate implementation. In addition, the security force organization was reviewed to determine that the required staffing levels were maintained in accordance with the Physical Security Plan.

2.1.1 Staffing Levels (81022)

The licensee's security organization was inspected to determine the licensee's compliance with the requirements of 10 CFR 73.55(a), (b)(1), (2), and (h), and the requirements of the Physical Security Plan.

The team reviewed licensee logs and staffing documents to determine if adequate security personnel were assigned to the shift during the incident on

October 21, 1992, to meet the contingency plan requirements. The normal shift complement consisted of approximately 45 uniformed personnel. That number was comprised of both armed and unarmed security officers. Although the shift's supervisor, a lieutenant, was not on site during the incident, one of the two assigned sergeants was acting as the security shift supervisor. The team determined that the security shift on duty during the incident contained sufficient armed security officers to meet their Physical Security Plan requirements.

2.1.2 Physical Security Plan and Implementing Procedures (81018)

The Physical Security Plan and the implementing procedures were inspected to determine the licensee's compliance with the requirements of 10 CFR 50.54(p) and 73.55(b)(3).

The team reviewed implementing procedures for adequacy and determined that the licensee had an effective management system for the development and administration of procedures, determined that changes to the procedures did not reduce the effectiveness of the licensee's security program, and that the security procedures in place at the time of the incident were adequate to ensure that station security was maintained.

2.1.3 Contingency Plan Implementation

The team conducted numerous interviews with security staff personnel in addition to reviewing logs and Central Alarm Station documents in order to determine if the actual response by the security force during the incident was adequate.

The shift security sergeants and Central Alarm Station operators were knowledgeable of the procedural requirements during the security incident involving a missing security officer. The sergeant in charge of the shift promptly and efficiently initiated the SECON Yellow condition when the security officer was first determined to be missing. After the missing security officer was found without accounting for the weapon, the sergeant properly initiated a SECON Red condition as per the procedural and Physical Security Plan requirements.

The team identified a weakness in the method of the security force's implementation of requirements under SECON Red conditions following the alleged assault of a security officer. The Physical Security Plan requires that upon declaration of SECON Red, all vital areas were locked down and a physical search of the areas conducted for a possible inside threat and signs of possible sabotage. The inspectors determined from interviews of security force members that although the vital areas were locked down, they were not searched during the implementation of SECON Red.

The search for possible sabotage was not conducted because security force supervisors did not consider that the potential assailant represented a possible inside intruder threat with the capability of conducting station sabotage. This belief was because security and other licensee supervisors were convinced that the incident was the result of an attack by a specific

licensee employee. Their belief was based upon an earlier, personal confrontation between the injured security officer and that employee.

Although the vital area's were searched as part of the SECON Yellow condition for the missing security officer, no search was conducted after the SECON Red condition was initiated for signs of sabotage or a potential inside threat until October 24, 1992, and then only after NRC prompting. After a review of the licensee's Physical Security Plan, the team determined that the plan did not provide clear response requirements for potential insider threats during SECON Red, when compared to the external threat response requirements.

The team identified two weaknesses in the command and control of the security force by security force supervision. As mentioned in the preceding paragraph, station supervisors in the security force and within other station organizations were originally focused on the incident having been initiated by a single licensee employee. As a result of this focus, for a period of time following the recovery of the missing weapon, the two sergeants on shift went to the control room and confronted the suspected licensee employee. The team considered this action a weakness in that during a SECON Red Condition both of the senior security force supervisors had removed themselves from either direct security force supervision in the field or the Central Alarm Station. The team noted that other oncoming shift lieutenants arriving at the station in addition to the experienced Central Alarm Station operators ensured that command and control was maintained and that the security force in the field received adequate direction.

The second command and control weakness identified by the team concerned the volume of incoming calls received at the Central Alarm Station. The sergeant in charge of the shift and the Central Alarm Station operators stated during interviews that it became difficult to maintain command and control over the security force because of the large volume of telephone and radio traffic after the incident began. The constant requests for updates and additional information by onsite and offsite management personnel made it difficult for the sergeant and the Central Alarm Station operators to maintain effective control of the security contingency in progress. Although the increased traffic had the potential to have interfered with the security force contingency actions, the team determined that the direction and oversight from the Central Alarm Station during the incident indicated that the sergeant and the operators displayed a good knowledge of contingency requirements and a very good ability to remain calm and efficient during the stress of the contingency event.

2.1.4 Conclusion

The security shift on duty during the incident contained sufficient armed security officers to meet their Physical Security Plan requirements.

The licensee met all plan and procedural commitments as written and approved. The security shift supervisor adequately dealt with difficult decisions during that process. A weakness was identified with the licensee's Physical Security Plan concerning the lack of guidance in SECON Red to appropriately deal with the insider threat.

The team identified two weaknesses to licensee management, who committed to study the problems identified and, if appropriate, institute corrective action to ensure that only essential radio and telephone traffic would be routed to the Central Alarm Station during contingency events and that the insider threat procedures and training would be strengthened. These two issues will be tracked as Inspection Followup Item (IFI 445/9250-01; 446/9250-01).

2.2 Operations Force Response

The team reviewed control room logs, shift security records, and interviewed operations and security personnel to determine the appropriateness of the operations response to the incident.

2.2.1 Shift Operations Force Response

The control room shift supervisor first became aware the security officer was missing at 3:43 a.m. when the Central Alarm Station operators at the direction of the security shift supervisor deactivated the missing officer's key card. Just prior to the officer being located, the control room shift supervisor requested, after conferring with the security shift supervisor, an armed security officer be stationed in the control room and at the alternate shutdown panel. This initiative was a compensatory posting not required by SECON Yellow but motivated by the various unknowns associated with the missing security officer.

At 4:52 a.m., the control room shift supervisor declared a Notification of Unusual Event based on Emergency Plan Manual Procedure EPP-201, Revision 8, "Assessment of Emergency Action Levels, Emergency Classification and Plan Activation." The control room shift supervisor originally assumed the duties of Emergency Coordinator and made all notifications required by 10 CFR 50.72 by 5:12 a.m. The Emergency Coordinator duties were later transferred to another senior reactor operator in the Technical Support Center, after the Technical Support Center had been established.

The licensee's management team in the Technical Support Center acted as facilitators during the event. At that time in the event, it was perceived by the licensee that the security officer had been assaulted by an attacker, and based on the security force response to the event during SECON Red, the alleged assailant would either be still located inside the protected area or would have key carded out of the protected area. The greatest challenge to the licensee involved the manner of dispositioning all personnel that were inside the protected areas during the alleged assault such that any possible attacker would be removed from the protected area and any threat to the security of the station terminated.

The licensee generated a list from the security computer of personnel that were in the protected area during the alleged assault. By comparing this list of personnel with the computer generated protected area egress records, the licensee was able to determined what individuals in the protected area during the alleged assault were still in the protected area. The licensee then decided to key card out all these individuals; an action that would ensure any alleged assailant was removed from site.

As an additional initiative, licensee management decided to remain in the Notification of Unusual Event in order to maintain the additional staffing in the Technical Support Center and onsite as a compensatory measure for unforeseen events. In addition, licensee management directed that the security force remain in SECON Yellow until all individuals in the protected area during the alleged assault were offsite.

By 8:00 a.m., the licensee had accounted for everyone who had been onsite during the incident by either key carding personnel offsite or sequestering them in preparation for questioning.

At 8:47 a.m., the emergency coordinator terminated the Notification of Unusual Event followed at 9 a.m. by the termination of the SECON Yellow condition by security management.

As a further initiative in conjunction with the security force's vital area walkdowns, the licensee conducted monthly system line-up checks on the following safety-related systems:

- Boration Flowpath
- Residual Heat Removal
- Emergency Diesel Generators
- Safety Chill Water
- Station Service Water
- Component Cooling Water

2.2.2 Post Incident Response

Following the licensee's successful accounting of all personnel in the protected area at the time of the incident, the licensee determined that it would be necessary to deny access to a number of their employees. This determination was based on the need to ensure that any suspected party to the alleged assault would not gain entry into the protected area.

In order to complete this requirement, the licensee reviewed the roster of personnel that were in the protected area at the time of the incident. The licensee eliminated the great majority of the personnel who had been on site as the potential assailant. This determination was based on the known location of the alleged victim and the chronology of the alleged victim's movements. The licensee identified 13 individuals that could be considered by proximity to have been able to have perpetrated the alleged assault. The access of these individuals was suspended. The licensee continuously evaluated this group of employees denied access as their investigation continued. A number of persons were removed from the group, and three were later added. On December 14, 1992, there were still seven site personnel with suspended access pending disciplinary review by the licensee.

The Team evaluated the licensee's action regarding the initial suspension of licensee employee access into the protected area and the subsequent employee return. The team concluded that the licensee's rationale for suspending and

restoring access was sound and that the security of the station was maintained throughout the investigation.

Immediately following the incident, the licensee took several interim actions to maintain personnel safety and station safeguards. These actions included: the assignment to backshift of additional security foot patrols, additional security foot patrols assigned within the protected area, increasing the frequency of routine security radio checks, and the implementation of a buddy system for workers located in isolated areas of the station. At the time of their implementation, these actions appeared to the Team to be prudent based on the limited information concerning the alleged assault and necessity to maintain station security and employee safety.

2.2.3 Conclusion

The team considered the licensee's operations response to the event good. The licensee's emergency plan was followed, all required notifications were made in a timely manner, and a number of positive initiatives were taken by the licensee to resolve personnel accountability in the protected area and ensure safety-related systems were properly aligned.

Although not specifically required by procedures, the team considered the decision to provide a compensatory security officer posting to the control room and the auxiliary shutdown panel to be an excellent initiative.

3 COMMUNICATIONS (81088)

During interviews, several security force personnel that were on shift during the incident indicated that radio deadspots within the plant and inoperative gaitronics equipment had the potential to hinder the successful implementation of the security contingency plan requirements.

The team reviewed the open action requests for the station gaitronics system and interviewed the licensee's system engineer with the responsibility for the system. The team determined that there were 255 gaitronics stations available at the plant. At the time of the incident, 9 of these 255 stations were logged as inoperable; however, the speakers were operable such that plant announcements were capable of being transmitted. In addition to the 9 inoperable stations, an additional 22 of the 255 stations had documented deficiencies, many minor. The team concluded that the gaitronics system was in relatively good state of repair and not a factor in reducing the implementation of the contingency plan requirements.

The team requested information from the licensee relative to the locations on the station where radio use is prohibited because of the possibility of the signal interfering with the reactor protection system and creating the potential for causing a plant trip or other plant transient. In addition, the licensee conducted a complete walk-down of the plant in order to locate any additional radio deadspots that had not been previously identified.

The inability of hand-held radios to communicate with the Central Alarm Station from deep within areas of stations has been common knowledge for years

within the nuclear industry. Some licensee's have resolved the problem by installing a special coaxial wire antennae throughout these radio deadspot areas which was the approach that the licensee had taken to improve communications in their identified deadspots. During their walkdown, however, the licensee did discover two previously unknown radio deadspots. The licensee has informed security personnel of their location, taken interim compensatory action to preclude the deadspots negative effect, and planned corrective action to permanently correct the deadspots in the future. These issues will be tracked for future followup as Inspection Followup Item (IFI 445/9250-02; 446/9250-02).

Conclusion

The plant radio and gaitronics communications systems were adequate to meet contingency plan requirements. The identified deadspots and small number of gaitronics devices requiring corrective action did not affect the successful resolution of the contingency event on October 21, 1992.

4 FITNESS-FOR-DUTY AND ACCESS AUTHORIZATION

The team inspected selected portions of the licensee's fitness-for-duty and access authorization programs to determine the licensee's conformance to the requirements of 10 CFR Part 26 and 10 CFR 73.56, with an emphasis on the manner the programs were able to support the licensee's efforts before and after the incident.

4.1 Behavioral Observation Training

The licensee's behavioral observation program was inspected to determine the licensee's conformance to 10 CFR 26.22 (a)(4) and (c), 10 CFR 73.56 (b)(2)(iii), and the requirements of their plans and procedures.

The team reviewed the licensee's behavioral observation training program. Included in the evaluation was a review of training lesson plans, personnel procedures, and attendance records. The team determined that the licensee had a training program in place to train its managers and supervisors in behavioral observation. In addition to the document review, the team conducted numerous interviews in order to determine the effectiveness of the licensee's behavioral observation training.

The team identified a weakness in the training in that the training received by licensee employees was significantly focused in the area of aberrant behavior resulting from drug and alcohol abuse with little emphasis on aberrant behavior resulting from personality disorders or interpersonal conflicts. This finding may be generic in the nuclear industry as a result of NRC requirements based on the fitness-for-duty rule, 10 CFR Part 26. The licensee acknowledged this finding and stated that they have taken steps to ensure the program more effectively trains in the personality and interpersonal conflicts portions of aberrant behavior determinations. The disparity in focus of the behavioral observation training program will be tracked to determine the manner that the licensee dispositions the issue as an Inspection Followup Item (IFI 445/9250-03; 446/9250-03).

During the review of the behavior observation training program, the team determined that some numbers of licensee and contractor supervisors had never received initial training in behavior observation. In addition, some supervisors had not received the required annual recurring requalification training. Further review by the team determined that the actual number of supervisors who had not received any behavior observation training was 20. An additional 21 supervisors were identified that had not received the annual recurring training.

10 CFR 26.22(a)(4) and 73.56(b)(2)(i) require that licensee's train supervisory personnel in behavior observation techniques for detecting degradations of performance, physical impairments, and changes in employee behavior which, if left unattended, could lead to individual acts detrimental to public health and safety.

Licensee Procedure STA-910, paragraph 6.1.1, states that all TU and contractor employee supervisors shall receive initial and annual recurring training in behavioral observation.

In addition, Technical Specification, Section 6.8.1.c, requires, in part, that written procedures shall be established, implemented, and maintained covering the activities referenced in Security Plan implementation. Licensee Procedure STA-910, paragraph 6.1.1, states that all TU and contractor employee supervisors shall receive initial and annual recurring training in behavioral observation.

The licensee's failure to train initially and to conduct annual retraining of supervisors constitutes a violation of 10 CFR 26.22(a)(4) and 73.56(b)(2)(i) and Technical Specification, Section 6.8.1.c (445/9250-04; 446/9250-04).

The team noted that the licensee took immediate corrective action and ensured that all supervisors at the level of general foreman or senior were formally trained in behavior observation prior to the supervisor's return into the protected area and prior to supervising workers.

In addition to the weakness identified concerning the areas of training focus mentioned earlier in this section, the team identified another weakness in the behavioral observation training program. This weakness involved the level of supervisors receiving behavior observation training. Unit 2 supervisors were trained to the general foreman level, while Unit 1 supervisors were trained to the foreman level, a position subordinate to the general foreman. The weakness associated with this method of training was apparent when the relative number of workers supervised by an individual was compared between the two units. Within Unit 1, the average number of workers per supervisor was approximately seven. In Unit 2, the number was approximately 12, with some examples of over 50 workers assigned to a single supervisor. The team questioned the licensee on the effectiveness of a supervisor that was expected to observe and determine potential behavior problems when supervising over 50 workers. The licensee concurred with the observed weakness and took action to increase the level of supervisor training in behavior observation down to the foreman level. This training was completed prior to the end of the inspection.

4.2 Behavior Observation Referral

The team reviewed the past disciplinary history of several licensee employees who had exhibited various disciplinary problems. These records indicated that one auxiliary operator had violated security requirements on numerous occasions prior to November 1989. Based on the documentation, his behavior at that time was judged by one security manager to be sufficiently aberrant that security management recommended his access authorization be suspended pending an in-depth psychological evaluation. Following that recommendation, the Manager of Plant Support requested that the auxiliary operator's supervisor investigate and evaluate the status of the auxiliary operator for continued unescorted access. This request was passed to the auxiliary operator's direct supervisor for action. The action taken was to provide the auxiliary operator with a written notice that he was directed to cooperate with the security personnel. In that written notice, the supervisor recorded that the auxiliary operator had stated during the interview that he had no intention of changing his behavior. Since that November 1989 notice, the auxiliary operator continued to be a discipline problem with numerous security infractions that indicated frequent loss of temper, hostility, and an argumentative nature.

The team reviewed files of other licensee employees and determined that there were other examples of repeat disciplinary problems at the station with no indication of any significant disciplinary action or referrals under the behavioral observation program.

The team considered the lack of aggressive and proactive followup on these examples of personnel disciplinary problems to be a weakness in the administration of the licensee's behavior observation program. The resolution of this weakness will be tracked as an Inspection Followup Item (IFI 445/9250-05; 446/9250-05).

4.3 Missing Weapon

As described in Section 1.2, when found, the allegedly assaulted security officer's weapon was missing. The weapon was subsequently discovered after a short search, suspended from a portion of plant piping, approximately 25 feet from where the officer had been found.

Technical Specification, Section 6.8.1.c, requires, in part, that written procedures shall be established, implemented, and maintained covering the activities referenced in Security Plan implementation. Paragraph 5.5 of the licensee's Procedure SEC-106 states, "Those personnel who receive or issue weapons and equipment, are responsible for the proper use, security, and maintenance of the weapons and equipment."

Contrary to the above, on October 21, 1992, the alleged victim of the assault lost control of a .38 caliber revolver for some unknown period of time. The weapon was not physically with the officer, and the officer would not have reasonably been able to regained possession of the weapon in a timely manner. This violation is not being cited because the criteria in paragraph VII.B.(2) of Appendix C to 10 CFR Part 2 of the NRC's "Rules of Practice," were satisfied.

4.4 Potential Introduction of Contraband into the Protected Area

During the hospital treatment of the alleged victim of the incident, a blood sample was taken and analyzed. The results of that sample indicated an alcohol content of an amount that would suggest that the alleged victim probably consumed a significant amount of alcohol during the shift when the incident occurred. This finding would imply that contraband (alcohol) had been introduced into the protected area, either by the alleged victim or another party. Although the hospital tests were indicative of the alleged victim's consumption of alcohol during the shift, because of the nature of the finding and the inability to verify introduction or consumption of alcohol by the alleged victim, this issue will not be pursued further from a regulatory standpoint.

4.5 Conclusion

The licensee was in violation of the requirement to train and retrain annually all supervisors in behavioral observation techniques.

A weakness was identified in the licensee's training program in that the training was heavily weighted in the area of drug and alcohol abuse rather than aberrant behavior caused by other factors.

Another weakness was identified in the area of behavioral observation referral. The team considered that the resolution of behavioral and discipline problems had not received the prompt management oversight necessary to adequately resolve potential personnel performance issues. If this trend of weak resolution of behavior and discipline problems were to continue, issues of a regulatory nature could result.

The alleged victim lost control of the assigned weapon during the incident which was in violation of the licensee's security procedures and Technical Specifications; however, this violation will not be cited.

5 SECURITY MANAGEMENT EFFECTIVENESS (81020)

The licensee's security management effectiveness, as it applied to the security program, access authorization program, and the fitness-for-duty program was inspected to determine the licensee's conformance to the principles of management effectiveness.

5.1 Supervisor Effectiveness

During interviews conducted with the security shift on duty at the time of the alleged assault, the majority of the officers indicated to the team that the security shift supervisor displayed favoritism toward the shift security officer that was the victim of the alleged assault. This favoritism involved dispensing discipline differently between the subject security officer and the remaining members of the shift. In addition, the interviews revealed that this favoritism had reduced the effectiveness of the security shift supervisor because of the disruptive manner in which the subordinate security officer interacted with the security shift supervisor and the remainder of the shift.

There appeared to be a communications barrier or breakdown in that this condition was not communicated to the security management by security force personnel or security management did not routinely and effectively communicate with the security officers in the field.

The team concluded that despite this condition where a security supervisor's effectiveness may have been reduced, the shift remained capable of performing its function of maintaining the security of the station.

5.2 Management Effectiveness

The team conducted extensive interviews with members of all five security shifts and reviewed all the security officer interviews conducted by the licensee during their investigation. The team's intent was to determine the security department's management effectiveness.

The team determined that there was a high level of frustration among the security force such that the attitude of the security officers was becoming a challenge to the ability of security management to maintain morale. The causes of this frustration appeared to be numerous and included the fallout of the incident on October 21, 1992, an impending reduction in force within the security force, changes in compensation benefits, perceptions of a lack of management support and visibility in the field, and the attitude and lack of sensitivity of the contract security management. Based on the team's review, there appeared to be a close corroboration between the results of the inspector's interviews and the information gathered in the investigative team statements. The team recognized that some of the causes of the low morale were intangible and that staff morale was not specifically a regulatory requirement. However, the team was concerned that the low morale might affect the performance of the security force members.

5.3 Conclusion

There was a high level of frustration and low morale prevalent in the security force. While not a regulatory issue at present, it might affect security force performance in the future.

ATTACHMENT

1 PERSONS CONTACTED

1.1 Licensee Personnel

+ D. Andrews, Director, Corporate Security
•# J. Ardizzoni, Supervisor, Security Administration
L. Barnes, Manager, Technical Staff Training
•#*+M. Blevins, Director, Nuclear Overview
• J. Braun, Coordinator, Plant Security
#* K. Britt, Coordinator, Plant Security
#* J. Brown, Coordinator, Fitness-For-Duty Program
•# H. Bruner, Senior Vice President, TU Electric
•#*+W. Cahill, Group Vice President
J. Donahue, Manager, Operations
•#*+N. Harris, Engineer, Regulatory Affairs
T. Hope, Manager, Unit 2 Licensing
#*+ H. Hutchison, Manager, Personnel
•#+ J. Kelly, Vice President, Nuclear Operations
•#*+R. Lancaster, Manager, Plant Support
•#*+J. Rumsey, Manager, Corporate Security
E. Schmitt, Manager, Operations/Engineering Training
•#*+A. Scogins, Manager, Security
• A. Scott, Vice President, Nuclear Operations (Retired)
* R. Smith, Plant Engineering
* K. Tague, Staff Support, Construction
#+ C. Terry, Vice President, TU Electric
#+ R. Walker, Manager, Regulatory Affairs
* D. Woodlan, Manager, Licensing

1.2 Burns Security (Security Contractor to TU Electric)

•#*+D. Hickey, Project Manager, Security
•#* D. New, Assistant Chief, Security
•#* D. Proffitt, Chief, Security

1.3 Independent Attorneys Retained by TU Electric

#+ T. Lillard

1.4 Newman & Holtzinger, P.C.

#+ S. Frantz

1.5 NRC Personnel

*+ J. Jaudon, Deputy Division Director, Division of Radiation Safety and, Safeguards, Region IV
•#*+M. Satorius, Team Leader, Division of Reactor Projects, Region IV
•#*+A. Earnest, Physical Security Specialist, Facilities Inspection Programs Section, Region IV
•#*+T. Dexter, Senior Physical Security Specialist, Facilities Inspection Programs Section, Region IV
• D. Graves, Senior Resident Inspector, Division of Reactor Projects, Region IV
•#*+W. Jones, Senior Resident Inspector, Division of Reactor Projects, Region IV

• Indicates attended the inspection statusing meeting October 23, 1992
# Indicates attended the inspection statusing meeting October 30, 1992
* Indicates attended the inspection statusing meeting November 13, 1992
+ Indicates attended the exit meeting December 18, 1992

In addition to the personnel listed above, the team contacted other personnel during the inspection period.

2 EXIT MEETING

An exit meeting was conducted on December 18, 1992. During this meeting, the team reviewed the scope and findings of this report. The licensee did not identify as proprietary, any information provided to, of reviewed by the team.