U. S. NUCLEAR REGULATORY COMMISSION

REGION I

Docket Nos:	50-272, 50-311, 50-354
License Nos:	DPR-70, DPR-75, NPF-57
Report Nos:	50-272/96-14, 50-311/96-14, 50-354/96-08
Licensee:	Public Service Electric and Gas Company
Facilities:	Salem and Hope Creek Nuclear Generating Stations
Location:	Hancocks Bridge, New Jersey
Dates:	August 15 - September 3, 1996
Inspectors:	G. C. Smith, Senior Security Specialist E. B. King, Physical Security Inspector D. F. Limroth, Senior Reactor Engineer
Approved by:	R. R. Keimig, Chief Emergency Preparedness and Safeguards Branch Division of Reactor Safety

DETAILS

S2 Status of Security Facilities and Equipment

S2.1 Protected Area Detection Aids

a. Inspection Scope

The inspectors conducted a physical inspection of the protected area (PA) intrusion detection systems (IDSs) on August 21, 1996.

b. Observations and Findings

The inspectors observed that the IDSs were installed and maintained as described in the NRC-approved security plan (the Plan).

c. Conclusion

No deficiency or weakness was identified.

S2.2 Alarm Stations and Communications

a. Inspection Scope

The inspectors observed central alarm station (CAS) operations and interviewed CAS operators to assess the effectiveness of the alarm station operations and the familiarity of the operators with the operations.

b. Observations and Findings

The inspectors observed that the CAS was being maintained and operated as committed to in the Plan. Inspector interviews with operators found them to be knowledgeable of their duties and responsibilities. The inspectors also found that the operators were not required to engage in activities that would interfere with assessment and response functions.

c. Conclusion

No deficiency or weakness was identified.

S2.3 Testing, Maintenance and Compensatory Measures

a. Inspection Scope

The inspectors reviewed commitments related to the testing of intrusion detection systems delineated in the licensee's NRC-approved security plan and implemented through security procedures. Additionally, the inspectors reviewed the results of five such tests in order to determine the acceptability of test results.

b. Observations and Findings

On April 3, 1996, at 8:51 a.m., security force members commenced testing of Salem perimeter intrusion detection system (IDS) zone 16. When a series of undefined tamper alarms that interfered with the intrusion alarms occurred, testing was terminated and corrective maintenance was initiated to investigate the cause of the tamper alarms. At about noon, with no maintenance having been performed, the personnel involved in the testing and maintenance departed the zone. Concurrently, the security force member who had been posted as a compensatory measure for the zone, which was anticipated to be in an alarm condition during the test, was also released from the compensatory post.

At 1:45 p.m., a technician commenced maintenance on the system consisting of opening, trouble-shooting, and tightening termination in a sensor status concentrator and in transmitter and receiver boxes for the zone. Following completion of the maintenance, the zone was challenged by three "walk" intrusions, following which, at 3:31 p.m., the personnel involved in the testing and maintenance and the security force member assigned as a compensatory measure departed the area. Security Procedure SP 12 (Revision 9), Security System Testing and Maintenance, requires, in part, that three "crawl" tests be performed following maintenance.

On June 5, 1996, at 2:38 p.m., following use of the "crane gate" for the transition of a vehicle, the security force members controlling access through the gate and satisfying compensatory posting requirements (since the zone would be in an alarm condition) were released after the IDS zone had been tested with a "walk test." The two security force members proceeded on their security rounds. Approximately 18 minutes later, the zone was properly tested in accordance with security procedures by means of three "crawl tests." Records indicate that the security force members who had functioned as compensatory measures actually left the immediate area during the 18 minute period in question; however, records do not reflect whether the field operations supervisor was in the vicinity of the zone (and therefore physically in a position to function as a compensatory measure) or not. The field operations supervisor was not available for interview regarding the details of the event in question.

Security Procedure 8, Vehicle Access Control, Revision 8, requires, in part: "10. Use of Crane Gate...Security Shift Supervisor/designee...Direct that the zone be crawl tested after the vehicle passes and prior to securing the patrol." This procedure further states, "SFM 1: Remain posted at the gate until the zone passes the crawl test."

c. Conclusions

The securing of the compensatory post on April 3, 1996 when undefined tamper alarms should have raised the question of the operability of the zone's IDS is considered a weakness.

The failure to test the IDS zone following maintenance in accordance with Security Procedure 12 on April 3, 1996, and the failure of the Security Shift Supervisor/designee to cause the zone to be tested in accordance with Security Procedure 8 on June 5, 1996, compounded by the security force members' failure to remain at their post until the zone had been tested in accordance with Security Procedure 8, constitute an apparent violation, i.e., failure to follow procedures.

S2.4 Access Control of Personnel

a. Inspection Scope

The inspectors reviewed the licensee's program for access control of persons granted access to the Protected and Vital Areas. The inspectors reviewed the security plan and implementing procedures, interviewed personnel implementing the access control program and observed implementation of the program.

b. Observations and Findings

Control of Terminated Personnel

The inspectors reviewed the access control process and found that individuals are granted access to the protected area and to specific vital areas (VA) of the plants based on specific needs. However, the inspectors' review of the process to inactivate access authorizations for persons that no longer require access to those areas disclosed several deficiencies. In June, 1996, seven employees were terminated; however, their access to the plants was not terminated until July, 1996, when the 31 day VA revalidation lists were returned to the Access Control Department. In July, 1995, five employees were terminated; however, their access to the plants was not terminated until August, 1995, when the 31 day VA revalidation lists were returned to the Access Control Department. The inspectors' review further disclosed that the terminated employees had access to the plants for periods ranging from 5 to 30 days after their employment had been terminated.

The PSE&G Security Procedure 4, "Personnel Access, Revision 3," dated November 1, 1994, in Section 4.13, states, in part, "when a person granted unescorted access terminates employment or no longer requires access to the PA, the cognizant department shall notify the screening supervisor within two work days. The Screening Supervisor ensures the administrative actions required to inactivate the security photo badge and personnel access clearance are accomplished." The failure to inactivate the badge and clearance access authorization for those persons that no longer require access within two work days is an apparent violation.

Control of Access Badges and Key Cards

On August 14, 1996, an NRC resident inspector observed that the locking mechanism on the door to one of the bullet resistant photo badge issue areas that was not occupied by security force personnel (SFP) at the time had been taped over rendering the lock inoperative. The notified PSE&G management of the situation and immediate action was taken to remove the tape and restore the lock to an operable condition. Security management also implemented actions to determine if the inoperative lock, which compromised the positive control of the photo badges, had resulted in an unauthorized entry into the PA or VAs. This event was reviewed further during this inspection, and the inspectors determined that, at the time the lock was inoperative, no compensatory measures were in place. After being notified of the event, security personnel conducted sweeps to verify that all personnel in the VAs were authorized. This was done by comparing the picture on the photo badge of personnel in the VAs to the person in possession of the badge. No unauthorized personnel were identified. Security personnel also conducted photo badge key card transaction histories for all badges located in the compromised badge issue area for the period the lock had been inoperable (approximately 8 hours). The card-transaction histories were then compared against other documentation to verify that the photo badge key card had only been used by the person to whom it was issued. The reconciliation of the transaction histories was completed on September 3, 1996, and no discrepancies were identified.

The NRC-approved security plan states, in part, in Section 5.6, "vital area access control is positively controlled by the photo badge key card system which permits access into specific areas to persons designated on the current access list contained in the system computers. Positive access control is accomplished by SFP prior to issuance of the photo badge/card key." The failure to provide positive control of the photo badge key cards by SFP is an apparent violation.

Control of Search Train

On August 19, 1996, a contractor en route to the plant protected area caused the metal detector in the personnel search train to alarm. The contractor was directed through a second metal detector that also alarmed. After failing to clear the second metal detector, the contractor was allegedly told by SFP to stand aside and await a pat-down (hands-on) search to determine the cause of the alarm. However, the contractor went to the badge issue area, was issued a photo badge/key card and entered the PA. When the security supervisor in the area was notified of the event, he initiated actions to identify the individual, but did not initiate the actions specified in the licensee's NRC-approved Security Contingency Plan for a potential threat to the plant. The individual was identified by the officers performing the search function using the file copies of the photo badge photographs about 50 minutes later. After identification of the individual, his supervisor was notified of the problem and the contractor was returned to the process facility and searched again with negative results about 30 minutes later. Additionally, the individual's locker, work area, and route to and from his work location were searched with negative results. However, the control room was not notified of the potential security threat

so that the appropriate emergency action level could be evaluated to determine the proper response, the contractor's badge/key card was not deactivated by SFP, which would have precluded him entering any VAs, nor was he paged on the plant paging system, once he was identified to expedite locating him.

The NRC-approved security plan states, in part, in Section 4.2.1.4, "searches at the guardhouses are performed by locally alarming portal or hand held metal and explosive detectors. When there is reasonable cause to suspect that a person is attempting to introduce firearms, explosives, incendiary devices or other unauthorized material into the protected area, the person is given a physical pat-down search." The failure to conduct a physical pat-down search of the contractor after he caused the portal metal detectors to alarm, which should have resulted in reasonable cause to suspect that person was attempting to introduce unauthorized material into the protected area, is an apparent violation.

The NRC-approved Security Contingency Plan states, in part, in Section 8.1.3.2, "it will be assumed that a security threat exists until it is known otherwise." Section 8.1.4 of the Contingency Plan defines "Intruder: A person present in a protected or vital area without authorization." Section 8.2.2.6 of the Contingency Plan states "Discovery of Intruders or Attack" notify SNSS (Senior Nuclear Shift Supervisor) of implementation of Contingency Event 6 (Discovery of Intruders...). Provide concise situation report. Request SNSS to classify the event per Event Classification Guide Section 16." The failure to notify the SNSS of the event so that it could be classified per the Event Classification Guide is an apparent violation.

c. Conclusion

Three apparent violations were identified in access control of personnel. The inspectors concluded that the apparent violations indicate a lack of knowledge or understanding of fundamental nuclear plant security principles, serious complacency, or both, on the part of the SFPs.

S5 Security and Safeguards Staff Training and Qualification

a. Inspection Scope

On August 19, 1996, the inspectors selected at random and reviewed the training, physical, and firearms qualification/requalification records of three security monitors, three armed security officers, three alarm station operators and three new security supervisors.

b. Observations and Findings

The inspectors found that training for the security monitors, armed security officers, and alarm station operators had been conducted in accordance with the NRC-approved security training and qualification (T&Q) plan and that it was properly documented. However, the inspectors also found during their review of training records and shift activity logs, that two of the three contractor security supervisors

were performing independent Field Operations Supervisory duties prior to qualifying satisfactorily on all of the required critical security tasks necessary for the performance of their related security duties.

The Salem-Hope Creek (Artificial Island) T&Q Plan, Section 3.3, states, in part, "the qualification matrix identifies the courses of instruction by job classification, which each person shall pass in order to qualify for performance of related security duties." Section 3.8, titled Supervisory Training, states that supervisors are required to qualify in all security force tasks. Critical Security Task #5, titled Conduct Patrols, states, in part, in Element 05-A, that the examinee will demonstrate knowledge of the site by responding correctly to the location of several protected and vital area alarms.

The inspectors found that the supervisors were signed off as qualified and given a 90 day period to complete Element 05-A satisfactorily. However, during the 90 day period, the supervisors were assigned independent Field Operations Supervisor duties, to include contingency response coordination. Contingency response coordination is an extremely important function and requires extensive knowledge of the protected and vital area alarm locations. These supervisors were assigned those duties without demonstrating requisite knowledge. The failure to qualify the supervisors in accordance with the requirement of the NRC-approved T&Q Plan is an apparent violation.

The inspectors also found noteworthy degradations in two past good practices. Based on a review of security training lesson plans, they noted that the lesson plans were not being kept current. This was apparent by numerous annotations in the margins. Additionally, continuing self-assessments of security performance by the training staff had been discontinued. The training supervisor stated that the lesson plans would be updated in the near future.

c. Conclusion

The inspectors concluded that the training of SFP conformed to the licensee's NRC-approved Training and Qualification Plan, except for the two new supervisors. However, based on the problems identified in personnel access control and testing, the effectiveness of the training appears to have decreased.

S6 Security Organization and Administration

S6.1 Management Support

a. Inspection Scope

The inspectors reviewed implementation of the security program to determine the level of management support.

b. Observations and Findings

Management support for the physical security program was found to be generally adequate. However, weaknesses in management oversight were identified as evidenced by the problems in the access control, testing, and training and qualification identified in this report.

c. Conclusion

The inspectors concluded that in certain areas of the security program management oversight had been ineffective or lacking.

S7 Quality Assurance in Security and Safeguards Activities

S7.1 Audits

a. Inspection Scope

The inspectors reviewed the licensee's 1995 Quality Assurance (QA) audit of the security program conducted from May 6-17, 1996.

b. Observations and Findings

The audit was documented in Audit Report 96-031, dated June 20, 1996. Weaknesses identified in the audit report that required further management attention were in the areas of VA documentation, preventive maintenance for security equipment, CCTV improvements and a potential weakness for allowing contraband into the PA during a drill. At the time of the inspection, security management had taken immediate short- term corrective actions to correct the specific problems but had not completed long-term programmatic corrective actions.

c. Conclusion

The inspectors concluded that the audit was comprehensive in scope and depth and included an independent technical specialist on the team. Findings were reported to the appropriate levels of management and the audit program was being properly implemented. The findings were indicative of the mood for additional management oversight of the program; however, the audit failed to identify, and cause to be addressed, the specific issues disclosed in this report.

S8 Miscellaneous Security and Safeguards Issues

Fitness-For-Duty Program

a. Inspection Scope

During this inspection, the inspectors reviewed portions of the licensee's Fitness-for-Duty (FFD) Program.

b. Observations and Findings

The inspectors randomly selected and reviewed records of pre-employment and for-cause alcohol tests, the methodology used for screening and confirmation tests, and the actions taken when a individual tested positive. The inspectors found from the records reviewed that the testing and follow-up programs were being conducted in accordance with 10 CFR Part 26 and the licensee's FFD policies and procedures.

c. Conclusion

No discrepancy or weakness was identified in the FFD program area reviewed.

X1 Exit Meeting Summary

The inspectors and NRC Senior Management met with licensee representatives in the Region I Office in King of Prussia, PA, at the conclusion of the inspection on September 3, 1996. At that time, the purpose and scope of the inspection were reviewed and the findings were presented. The licensee acknowledged the inspection findings. During the exit meeting, the licensee presented short-term corrective actions for the apparent violations and provided information from the Root Cause Team that had been established to investigate the problems. Since neither the licensee's nor its contractor's investigations had been concluded at the time of this meeting, the licensee offered to meet with the NRC to provide the results of those investigations when they are available. The licensee committed to contact NRC Region I prior to making any substantive changes to those short-term corrective actions that provide interim measures to assure security program safety objectives are being met. The handouts provided by the licensee during their presentation are attached to this inspection report as Attachment 1.

During a review of the inspection findings subsequent to the September 3, 1996 exit meeting, two additional apparent violations were identified. They were: failure to test an intrusion detection system in accordance with security procedures; and failure to notify the nuclear shift supervisor of a potential threat to the plant. Details of these apparent violations are contained in paragraphs S2.3 and S2.4, respectively. The licensee was notified of these additional apparent violations in a telephone conversation, on September 25, between Mr. G. Smith, NRC RI and Mr. M. Trum, PSE&G Co.

X2 Review of Updated Final Safety Analysis Report (UFSAR)

A recent discovery of a licensee operating its facility in a manner contrary to the UFSAR description highlighted the need for a special focused review that compares plant practices, procedures, and parameters to the UFSAR description. Since the UFSAR does not specifically include security program requirements, the inspectors compared licensee activities to the NRC-approved physical security plan, which is the applicable document. The inspectors reviewed the licensee's control of Licensee Designated Vehicles (LDVs) in the protected area. The licensee previously had a provision for temporary LDVs in their NRC-approved Security Plan, however, the NRC determined that the provision was inappropriate and notified the licensee in early August of that determination. The inspectors' review disclosed that the licensee took immediate action to discontinue the use

reviewed the revised procedures and interviewed members of the security organization responsible for the control of vehicles onsite. The inspectors' review concluded that the procedures adequately reflected the change and that members of the security organization were knowledgeable of the revised procedures. The inspectors' review also disclosed that the licensee's control of LDV was in accordance with applicable regulatory requirements.

PARTIAL LIST OF PERSONS CONTACTED

Licensee and Contractor

D. Renniek, Security Manager
J. Benjamin, Director, QA/NSR
D. Garchow, Salem General Manager
M. Bezilla, Hope Creek General Manager
L. Storz, Senior Vice President Nuclear Operations
M. Trum, Director, Nuclear Operations Services
D. Powell, Licensing Manager
J. Pollock, Hope Creek QA Manager
G. Grime, Security Consultant
R. Ritzman, Licensing Engineer
M. Ivanick, Security Coordinator
P. Macconi, Operations Services

NRC

W. Kane, Deputy Regional Administrator
J. Wiggins, Director, Division of Reactor Safety
R. Keimig, Chief, Emergency Preparedness and Safeguards Branch
R. Cooper, Director, Division of Reactor Projects
E. King, Security Inspector
L. Nicholson, Reactor Projects Branch Chief
C. Marschall, Senior Resident Inspector, Salem
G. Smith, Senior Security Specialist
S. Morris, Resident Inspector, Hope Creek
J. Kenna, Special Agent
J. Joustra, Senior Enforcement Specialist
R. Summers, Senior Resident Inspector, Hope Creek
D. Limroth, Senior Reactor Inspector

ENCLOSURE 2

Handouts Provided
By Public Service Electric & Gas Company
At the Exit Meeting For
Inspection 50-272/96-14, 50-311/96-14
and 50-354/96-08
Conducted on September 3, 1996

The Power of Commitment

PSE&G

PUBLIC SERVICE ELECTRIC & GAS COMPANY

SECURITY EXIT MEETING
SEPTEMBER 3, 1996

The Power of Commitment

PSEG

APPARENT VIOLATIONS / CONCERNS

- Failure to adequately control badges
- Failure to perform a required patdown
- Failure to adequately qualify supervisors
- Failure to deactivate badges within required time

- Concern - Overall use of procedures

The Power of Commitment

PSE&G

SPECIFIC CORRECTIVE ACTIONS

- Failure to adequately control badges
  - Restored the locks to operability
  - Security informed SNSS's of possible badge compromise
    - Heightened awareness
  - Searched vital and protected areas
  - Established positive identification at Hope Creek and Salem vital areas
  - Conducted badge inventory - all badges accounted for
  - Reported as a loggable event

The Power of Commitment

PSE&G

SPECIFIC CORRECTIVE ACTIONS

- Failure to perform a required patdown
  - Supervisor promptly notified of event
  - Individual identified within 51 minutes of event
  - Individual removed from site within an additional 27 minutes
  - Searched individual's locker, work area, access and egress route
  - Confirmed individual's location during period of time within the Protected Area
  - One Hour report

The Power of Commitment

PSE&G

SPECIFIC CORRECTIVE ACTIONS

- Failure to adequately qualify supervisors
  - Historical finding
  - Supervisors were fully qualified prior to discovery
  - Reviewed qualification of security force members (in progress)
  - Reinforced expectation on qualification cards to training and PSE&G personnel

SPECIFIC CORRECTIVE ACTIONS

- Failure to deactivate badges within required time
  - Active badges were reviewed
  - Badges were deactivated as appropriate
  - Review all active badges weekly
  - Face to face communications with all R/C managers to review procedure and checklist
  - Reported as a loggable event

The Power of Commitment

PSE&G

SHORT TERM CORRECTIVE ACTIONS

- Communications with security force personnel
  - Reinforcement of mission
  - Reviewed recent events
  - Stressed need for procedural adherence
  - Introduced 3-way communications
  - Heightened awareness
- Increased supervisory presence in the workplace
- Reinstate Guard Mount (face to face shift turnover)

The Power of Commitment

PSEG

SHORT TERM CORRECTIVE ACTIONS

- Management mentor
- Security procedure
  - Compliance
  - Revisions
- Root Cause Investigation Team established

Corrective actions have stabilized performance, long term corrective actions under development

The Power of Commitment

PSE&G

ROOT CAUSE TEAM

- Chartered a root cause investigation of the badging incident
- Charter expanded to address additional security issues
- Expectations
  - Determine if security force understand mission and if actions are aligned with mission
  - Evaluate effectiveness of PSE&G and contractor security management, independent oversite and self assessments
  - Identify programmatic, cultural, and generic issues
  - Recommend corrective actions

The Power of Commitment

PSE&G

AREAS OF FOCUS

- Understanding of security mission
- Professionalism of the security force
- PSE&G reinforcement of expectations through daily supervision
- Security team interface
- Adequacy and implementation of security procedures
- Corrective maintenance of security hardware
- Implementation of corrective action process
- Communications

The Power of Commitment

PSE&G

ON-GOING CORRECTIVE ACTIONS

- Completion of Root Cause investigation
- Evaluate Root Cause team recommendations and implement corrective actions as appropriate
- Conduct security awareness training for plant managers, managers, SNSS's, and others

The Power of Commitment

PSE&G

ON-GOING CORRECTIVE ACTIONS

- Provide an update to NRC Management in October
  - Recovery to Excellence Plan
  - Status of actions
  - Performance indicators

We are committed to the return of the security program to excellence

The Power of Commitment

PSE&G

PUBLIC SERVICE ELECTRIC & GAS COMPANY

SECURITY EXIT MEETING
SEPTEMBER 3, 1996

BACKUP

The Power of Commitment

PSE&G

ACCESS CONTROL

- Three part controls:
  - Authorization requirements 10CFR73.56 & 57
    - Background investigation
    - Psychological assessment
    - Behavioral Observation
  - Fitness for Duty provisions 10CFR26
  - Positive access control
    - Metal & explosive detectors
    - X-ray Machines
    - Observation

The Power of Commitment

PSEG

ACCESS CONTROL

- Authorization is based on 10CFR73.56 & 57 requirements
- Access is reaffirmed upon each entry, by use of positive access controls
- A partial failure of the positive access controls occurred in this event - lack of personnel metal detection

The Power of Commitment

PSEG

REPORTING REQUIREMENTS GENERIC LETTER 91-03

- Issued to provide regulatory clarity
- This event can be classified as a: "Partial failure of an otherwise satisfactory access authorization or access control program"
- Extenuating circumstances resulted in a delayed response (Time required to identify the individual)
- Upon finding the individual, a search of the affected areas was conducted
- No malevolent intent was identified
- No deceit was present

Based on the above, this was not an intruder event

The Power of Commitment

PSEG

ON-GOING CORRECTIVE ACTIONS

- Completion of Root Cause investigation
- Evaluate Root Cause team recommendations and implement corrective actions as appropriate
- Provide an update to NRC Management in October
  - Recovery to Excellence Plan
  - Status of actions
  - Performance indicators

We are committed to the return of the security program to excellence

The Power of Commitment

PSE&G

Key Regulatory Terms and Definitions

- Unauthorized person (Fed Register Vol. 52, No. 110): an unescorted individual in an area to which the individual is not granted unescorted access.
- Authorized individual (10 CRF73.2): any individual...who has been designated in writing by a licensee to have...unescorted access to areas where special nuclear materials are used or stored.
- Intrusion (SCP-6): an unauthorized entry into the protected area or vital area.
- Deceit (10CFR73.2): methods used to attempt to gain unauthorized access ... where the attempt involves falsification to present the appearance of authorized access.
- Malevolent (Webster): having, showing, or arising from intense often vicious ill will, spite, or hatred.
- NRC Staff Position (Fed Register Vol. 52, No. 110): "...some unauthorized entries through a required barrier may not involve malevolent intent particularly those involving "tailgating" by individuals into areas to which they are authorized unescorted access."
- Further guidance is provided in Generic Letter 91-03.