U.S. NUCLEAR REGULATORY COMMISSION

REGION III

Docket Nos:	50-295; 50-304
License Nos:	DPR-39; DPR-48
Report Nos:	50-295/98002(DRS); 50-304/98002(DRS)
Licensee	Commonwealth Edison Company
Facility:	Zion Station, Units 1 and 2
Location:	105 Shiloh Boulevard Zion, IL 60099
Dates:	January 12 through February 19, 1998
Inspectors:	J. Belanger, Senior Physical Security Inspector G. Pirtle, Physical Security Inspector
Approved by:	J. R. Creed, Chief, Plant Support Branch 1 Division of Reactor Safety

EXECUTIVE SUMMARY

Zion Generating Station, Units 1 and 2
NRC Inspection Reports 50-295/98002; 50-304/98002

The initial purpose of the inspection was to review some security and fitness-for-duty concerns received by Region III and to review aspects of the licensee's physical security program related to staff knowledge and performance, training and qualification, and security organization and administration. The inspection was expanded to include a review of heightened security measures initiated following the January 15, 1998, plant closure announcement. Additionally, the inspectors reviewed the details/root cause and immediate corrective action related to a reported security event involving the discovery of unattended safeguards information found in an uncontrolled area. Previously identified open items were also reviewed.

Plant Support

- An unresolved item was identified relating to the circumstances surrounding the protection of safeguards information. It appears that the information was not secured properly, that some individuals may not have been trained appropriately and that the self-assessment program may have been too narrowly focused. This item will remain unresolved pending further NRC review. (Section S8.1.a)

- A security officer requesting unescorted access apparently falsified his criminal history questionnaire. (Section S1.1)

- Security measures implemented on January 15, 1998, to address the announcement that Zion Station would close, were well-planned and effectively implemented in a timely manner. (Section S1.2)

Report Details

IV. Plant Support

S1 Conduct of Security and Safeguards Activities

S1.1 Falsification of Criminal History Information by Security Officer

a. Inspection Scope (81700)

On December 15, 1997, the licensee received the results of a fingerprint check from the Federal Bureau of Investigation which showed two arrests that were not included in criminal history section of a Personal History Questionnaire submitted by a security officer in support of his request for unescorted access authorization. The inspectors reviewed the licensee's access authorization program in relation to management's review of the evaluation criteria identified in NUMARC 89-01, in making a determination of trustworthiness or reliability.

b. Observations and Findings

On August 25, 1997, a named security officer completed a Personnel History Questionnaire (PSQ) in support of his request for unescorted access at the Zion Nuclear Plant. The applicant identified several arrests in the criminal history portion of the PSQ. The licensee granted temporary unescorted access authorization on an interim basis not to exceed 180 continuous days. This authorization was contingent upon satisfactory completion of the required conditions which included the evidence that a request for a criminal history check of the individual by the FBI was submitted to the NRC.

On December 15, 1997, the licensee received the results of the criminal history record check from the Federal Bureau of Investigation which showed two additional arrests that were not identified in his PHQ. A member of the licensee's access authorization staff immediately identified the discrepancy and contacted the individual who denied that the arrests were his. On January 13, 1998, the licensee notified the individual by certified mail that his unescorted access was placed on temporary hold until he resolved the issue. The individual, by letter dated February 8, 1998, admitted that the arrests were his. The licensee terminated the individual's unescorted access based on a review of the evaluation criteria for unescorted access authorization detailed in NUMARC 89-01 and Corporate Nuclear Security Guideline No. 502, Revision 4 dated February 1997 which address "Willful omission or falsification of material information submitted in support of employment or request for unescorted access". The licensee stated that if the individual had not lied when questioned about the discrepancy, they would likely have granted unescorted access based on the nature of the arrests and the age of the applicant at the time of the arrests. They felt that the issue developed into one of trustworthiness and reliability when the individual lied about the arrests.

c. Conclusions

A security officer omitted some criminal history information when applying for unescorted access and initially lied when confronted about the discrepancy. The licensee appropriately considered the information obtained during the background investigation in making a determination of trustworthiness or reliability.

S1.2 Conduct of Security and Safeguards Activities

a. Inspection Scope (IP 81700 and 81020):

On January 15, 1998, the security force implemented a "heightened security awareness" posture in conjunction with the licensee's public announcement that the Zion station would be closed. The short term (less than two weeks) increased measures included additional patrols, implementation of a 12-hour shift for the security force, strengthened security measures within the owner-controlled area, and increased oversight of security activities by plant and corporate licensee and contractor managers. The inspectors reviewed the implementation of those measures.

b. Observations and Findings

The additional heightened-awareness security posts were well-planned and appropriate for the existing status of the plant at the time of implementation. Effective coordination and communication occurred between the site and corporate security representatives (licensee and contractor) and the security force members. Implementation of 12-hour shifts was completed within 12 hours after initiation of the heightened-awareness posture. This increased the effective on duty size of the security force. Post orders for additional security posts were completed upon initiation of the 12-hour shifts. The post orders reviewed were adequate to identify the security actions and activities appropriate for the particular post. All security personnel checked on post had appropriate post orders and were knowledgeable of the security requirements for the post.

c. Conclusions

The heightened-awareness security measures were well-planned, implemented in a timely manner, and closely coordinated and monitored by licensee and contractor security management personnel.

S2 Status of Security Facilities and Equipment

a. Inspection Scope (81700):

The inspectors reviewed the condition of security equipment and facilities required by the security plan. The equipment observed included, but was not limited to, search equipment, intrusion and alarm assessment equipment within both alarm stations, and equipment within the Main Access Facility.

b. Observation and Findings

Equipment observed within the alarm stations and the Main Access Facility functioned as designed. Maintenance support for security equipment seemed timely and adequate. Monthly trending data for September 1997 through November 1997 showed that closed circuit television (CCTV), perimeter alarm zones, and door alarm availability was 99% or higher.

c. Conclusions

Equipment observed functioned as designed.

S3 Security and Safeguards Procedures and Documentation

a. Inspection Scope (IP 81700):

The inspectors reviewed selected procedures pertaining to the areas inspected, to include special post orders for the heightened-awareness posture assumed on January 15, 1998. Inspectors also reviewed appropriate logs, records, and other documents pertaining to security performance .

b. Observation and Findings

Procedures and post orders reviewed were well-written and in sufficient depth to address the tasks appropriate to the security posts. Reviewed documentation maintained by security officers observed on post was complete and accurate.

c. Conclusions

Procedures and post orders reviewed were adequate. No deficiencies were noted in logs, records, or other documents reviewed.

S4 Security and Safeguards Staff Knowledge and Performance

a. Inspection Scope (IP 81700 and 81022):

The inspectors toured various security posts, including both alarm stations and the Main Access Facility and each special security post manned during the heightened-awareness security posture. Security personnel performance of duties were observed to determine whether the security officers were knowledgeable of post requirements. Security event logs pertaining to security force performance were also reviewed.

b. Observation and Findings

Security officers observed on post and interviewed on post were knowledgeable of the appropriate security requirements. Personnel on post who were response force members were aware of response equipment cabinet locations and location of their

posts and were properly equipped with radio communications. Security officers evaluated on the heightened-awareness security posts had appropriate post orders and were aware of the security requirements and specified equipment within their patrol zones.

Review of the security human error event trending data for the period between November 1996 and November 1997 showed good performance by the security force.

c. Conclusions

Security force members observed were knowledgeable of post requirements, including the heightened-awareness posts and performed their duties in accordance with their procedures.

S5 Security and Safeguards Staff Training and Qualification

a. Inspection Scope (IP 81700)

The inspectors reviewed the training records of the approximately 20 security force personnel who were hired within the past year.

b. Observations and Findings

Training records reviewed were well-maintained, complete, and accurate. Inspectors' reviews included completion of required critical tasks, weapon qualifications when appropriate, physical examinations, fitness testing when appropriate, and certification of completion of training. No deficiencies were noted during review of training records.

c. Conclusions

Training records reviewed were accurate and complete.

S7 Quality Assurance in Security and Safeguards Activities

a. Inspection Scope

The inspectors reviewed the physical security portion of the latest Licensee Site Quality Verification Audit (No. QAA 22-97-01, dated April 30, 1997) for the site security program; the Burns International Security Services. Inc. (BISSI) audit conducted March 11-15, 1996 (No. UBU 96-04); the Job Description for the Self Assessment Administrator of the BISSI security force (approved June 23, 1997); and security parameters monitored on a monthly basis.

b. Observation and Findings

The licensee's audit report for the security program was of sufficient depth and scope and identified weaknesses that were being addressed by the security staff to include contraband drill performance, and control of safeguards information.

The licensee's audit also noted that the contractor security force (BISSI) planned to fully implement its independent self-assessment program within the near future. Interviews with the BISSI Self Assessment Administrator (SAA) and review of the SAA's job description indicated that the program, when implemented, would further strengthen the self-assessment process. The potential impact on self-assessment efforts of the decision not to operate the Zion plant was being evaluated.

Several performance indicators were monitored on a monthly basis to include: security human error events, loggable security events, door ajar alarms, security force turnover, several aspects of maintenance support for security equipment, and security drills. Problem areas were being addressed when identified.

c. Conclusions

Self-assessment efforts were varied and effective in identifying problem areas.

S8 Miscellaneous Security and Safeguards Activities

S8.1 Inadequate Control of Safeguards Information

a. Inspection Scope (81810)

On January 14, 1998, at approximately 4:40 p.m., the inspectors learned that the licensee had discovered eleven rolls of uncontrolled safeguards drawings in design engineering outside the protected area. The inspectors reviewed the security organization's response to this event including the reporting of the event under 10 CFR 73.71, the licensee's evaluation of the significance of the information, corrective actions, and the use of Zion Administrative Procedure 11000-03, Revision 3 dated April 30, 1997, "Safeguards Information"

b. Observations and Findings

On January 14, 1998, a clerk from Central Files attempted to locate some safeguards drawings that were in the process of being updated. The clerk's documentation showed that these drawings had been in the update process for an extended period of time. The clerk went to see the Senior Electrical Designer in Design Engineering who was responsible for handling Drawing Change Requests (DCR). This person is the normal recipient of all electrical drawings that are updated by an off-site vendor and then shipped back to the site. The clerk asked this individual if he knew the location of the drawings in question. The individual pointed to two opened brown paper shipping bags containing 46 safeguards drawings laying in the corner of his office cubicle. He noted

that the drawings were there for six months. This office cubicle was located in an open office area on the second floor of an uncontrolled building outside the protected area. The clerk asked the engineer whether he knew they were safeguards information and if he knew how to handle them. The engineer responded affirmatively to both questions and told the clerk that he should simply PIF (Problem Identification Form) him for not following the procedure.

At approximately 12:00 p.m., the Central Files clerk contacted the security department's Self-Assessment Administrator (SAA) who, with the clerk, inventoried the drawings using a list supplied by the clerk and the transmittal sheets that accompanied the drawings. No discrepancies were identified and all documents were accounted for.

The SAA reviewed the occurrence with the engineer. In this conversation, the engineer reiterated that he knew how to handle safeguards documents, and, due to an incident concerning uncontrolled safeguards within Design Engineering late last year, he had recently been reminded how to handle Safeguards. Although the engineer had not been trained specifically in the site procedure pertaining to safeguards information (Zion Administrative Procedure 1100-03, Revision 3), he had also received training on the handling of safeguards through Nuclear General Employee Training (NGET). (Page 15 of the Study Guide for NGET, Revision 18, dated February 1997, stated that safeguards information must be stored in a GSA-approved locked security storage container when unattended.) The SAA reviewed the proper procedure for handling safeguards information with the engineer and took custody of the drawings. At approximately 3:30 p.m., the documents were moved to the Secondary Alarm Station within the Protected Area for protection against unauthorized disclosure.

Initially, the licensee classified the event as a twenty-four hour loggable event; however, further evaluation by the site security staff resulted in reclassification of the event to a one-hour reportable event because of the potential significance of the information on the drawings. (Note: On February 9, 1998, an engineer from the licensee's Operational Analysis Department (OAD), familiar with security systems, independently evaluated the drawings at the vendor's site and concluded that, although appropriately considered Safeguards Information, the information would not significantly assist an individual upon intent committing an act of radiological sabotage.)

While conducting event followup review activities, on January 22, 1998, Design Engineering personnel found uncontrolled prints of the drawings related to the January 14, 1998, event. These prints were in a folder on the floor of the same cubicle belonging to the engineer involved in the January 14, 1998, event. These drawings had been delivered by a vendor courier approximately May 1997; however, the courier did not recall to whom the documents were given. The engineer was not aware that these copies were in his cubicle. Design engineering personnel took possession of these drawings, inventoried them, and shipped them back to the vendor but failed to immediately notify the Station Security Administrator, contrary to the NGET instructions.

The licensee's investigation developed information that the involved engineer received the original mylar drawings in April 1997. The vendor's courier, who delivered the

drawings, could not recall whether he specifically told the engineer that the packages contained safeguards information; however, a transmittal letter from the vendor dated April 18, 1997, addressed specifically to this engineer stated that the drawings were safeguards. The engineer, in a signed statement taken during the licensee's initial investigation of the event, indicated that he did not open the packages until July or August of 1997. He further indicated that when he opened the packages, he noted that they were original drawings marked as Safeguards Information and that since he only reviewed prints, he contacted another (named) engineer who identified the Safeguards Information drawings requiring engineering review. The inspector noted that the second engineer was trained in ZAP 1100-03 in addition to having received safeguards training in NGET and understood safeguards information protection requirements. ZAP 1100-03, section G.5 required that any person who receives or acquires safeguards information shall ensure that it is protected against unauthorized disclosure. Section G.7.b required that safeguards information located in uncontrolled areas be stored in a GSA-approved security container. In addition to not properly securing the documents in a GSA- approved security container when unattended, the engineer who had been trained in ZAP 1100-03 did not notify the Design Engineering Department's Safeguards Information Custodian. Consequently the documents were not included in the latter individual's inventory. ZAP 1100-03 required that the Safeguards Information Custodian maintain an inventory of major safeguards information items including drawings. The involved engineer's supervisor became aware of the existence of these drawings which were apparently stored in his office periodically between July 1997 and January 1998. The supervisor was trained in the protection of safeguards information through NGET, but he was not trained in ZAP 1100-03.

The licensee's investigation of this event identified interface deficiencies between the vendor's safeguards program and ComEd's program. Neither party was cognizant of the identity of the other party's safeguards custodians. ComEd's program did not require that the onsite safeguards custodians be identified to the offsite vendors. However, the vendor's procedure (Sargent & Lundy General Office Procedure GOP 3-7, Revision 6 dated August 15, 1994) required the Project Manager to obtain from the client a list of client personnel who are authorized to discuss, transmit, or receive safeguards information and distribute the list to project personnel. The vendor did not implement this aspect of their procedure. This failure caused the delivery of safeguards information to a member of the licensee's organization other than the Safeguards Information Custodian who was not trained in ZAP 1100-03.

The licensee's Site Quality Verification Department had audited the safeguards information program; however, the audits addressed the site implementation of the program and did not include the vendors who provided the information. The audits apparently only provided documents that were logged in the Safeguards Information protection system. The audit report (QAA 22-97-02) dated April 30, 1997, identified that refresher training for individuals handling safeguards information was not being conducted on an annual basis (Level III finding).

Corrective actions taken by the licensee for this event included:

Immediate Actions

- When discovered, plant security personnel immediately took possession and properly stored the uncontrolled safeguards information.

- Immediate non-documented verbal counseling was given to the involved individuals at the time of discovery.

- The Design Engineering Supervisor discussed this incident at the January 14, 1998 department meeting.

- The Station Security Administrator initiated a sweep of the station for safeguards documents. An informational package was distributed instructing all department heads to review with their personnel how to look for and to control safeguards documentation. As a result of this effort, a second instance of improperly protected drawings in the same engineer's office.

- On January 30, 1998, by phone and a follow-up letter on February 6, 1998, the licensee instructed its vendors to send all safeguards documents to the Security Department until further notice.

Other Corrective Actions

- The quality assurance group will audit the safeguards programs belonging to vendors that handle licensee safeguards documents.

- The licensee will provide a list to all off-site safeguards vendors identifying those onsite individuals authorized to receive and handle safeguards information and likewise will obtain a list of vendor personnel authorized to receive safeguards information. This list will be updated every six months. This is an interim measure until evaluation of the results of the next item.

- Quality Assurance will research the issue at all six stations to assure compliance and a common methodology for handling safeguards information.

In addition to the Station's onsite review of the PIF (PIF # Z1998-00195), the Station Security Administrator requested a corporate security investigation of this incident. The licensee will provide a report of this investigation to the NRC for review. This matter is considered unresolved pending further review and evaluation by the NRC. [URI 50-295/98002-01(DRS); 50-304/98002-01(DRS)].

c. Conclusions

Unattended Safeguards Information in the owner-controlled area was not properly protected. Training in the site administrative procedure pertaining to safeguards information protection program was not administered to some individuals who handled safeguards information program. The licensee's quality assurance program did not

include reviews of vendors who provided safeguards information to the utility. Communication between the licensee and its vendor on the transmission of documents between the two facilities was poor. This is an unresolved item pending additional review and evaluation by the NRC.

S8.2 (Closed) Inspection Follow-up Item (295/304-95023-12(DRS)): This item related to the gap in CBOP coverage that would trigger the "ascertaining activities" requirement of Regulatory Guide 5.66. NUMARC 91-03 specified this period to be "greater than 30-day period" while the most recent guidance as stated in NEI 95-01 specified "greater than 60 days". The licensee's practice was to pull a security badge after 365 days of non-usage for permanent and contractor/vendor employees. The licensee stated that they would adopt the greater-than-60 day standard in NEI 95-01 if NRC accepted this position.

Inspection showed that the licensee adopted the 30-day standard by pulling contractor badges after 30 days of non-usage. The licensee indicated that they are aware of their own employees who take extended leave greater than 30 days through the Human Resources Department. The inspector concluded that the licensee met the intent of the guidance in NUMARC 91-03. This item is closed.

S8.3 (Closed) Inspection Follow-up Item (295/304-97022-08): Compensatory measures not established for a degraded vital area barrier. This item was opened pending the licensee's completed investigation and corrective actions. Duct penetration tests conducted by the electrical maintenance personnel on September 30, 1997, showed that internal dimensions and obstructions precluded entry through the pathway. The inspectors concluded that no violation occurred. This item is closed.

S8.4 (Closed) Inspection Follow-Up Item (295/304/97022-09): Inattentive security officers on three occasions within a four-week period. The item was opened pending a further review of this issue by a regional security specialist. In all three instances, the licensee conducted an investigation which resulted in termination of unescorted access authorization. Although the officers in each instance were determined to be inattentive, no violations of the security plan occurred because the specific postings were not determined by the inspector to be plan requirements. The licensee's investigations found no common factors relating to the three events. To preclude recurrence, the licensee's security contractor initiated an onsite program ("Stand Up & Call") at each of the six licensee's nuclear sites. This program addresses individual attention-to-duty responsibilities, actions to preclude inattentiveness, and supervisors' role and responsibilities in ensuring individuals who perform duties on their shift are fit for duty and remain that way the entire shift. This issue is closed.

V. Management Meetings

X1 Exit Meeting Summary

The inspectors conducted an interim exit meeting with members of the licensee management on January 23, 1998, and also conducted a telephone exit on February 19, 1998, to inform licensee management that the issue relating to the protection of safeguards information is considered an unresolved issue pending further NRC. The licensee acknowledged the findings presented.

PARTIAL LIST OF PERSONS CONTACTED

Licensee

B. Finlay, Acting Station Security Administrator
K. Glasure, Security Force Manager (Burns Security)
R. Godlev, Regulatory Assurance
F. Gogliotti, Design Engineering Supervisor
J. Kiser, Self Assessment Administrator (Burns Security)
R. Lane, Nuclear Generation Group Security Director
K. Leech, Acting Station Security Administrator
J. May, Design Engineering Safeguards Informatin Custodian
R. Morley, Nuclear Security Administrator
J. Papaleo, FFD Program Coordinator
D. Ringo, Access Authorization Coordinator
R. Starkey, Station Manager
K. Steele, Station Security, In processing
S. Techau, Access Authorization Program Coordinator
M. Weis, Business Manager

NRC

D. Calhoun, Resident Inspector

INSPECTION PROCEDURES USED

IP 81700	Physical Security Program for Power Reactors
IP 81810	Physical Protection Safeguards Information
IP 81502	Fitness for Duty Program
IP 81022	Security Organization

ITEMS OPENED AND CLOSED

OPENED

50-295(304)/98002-01(DRS)	URI	Safeguards Information Protection requirements

CLOSED

50-295(304)/95023-12(DRS)	IFI	Trigger "ascertaining" under CBOP
50-295(304)/97022-08(DRS)	IFI	Compensatory measures for a degraded vital area barrier
50-295(304)/97022-09(DRS)	IFI	Inattentive Security Officers

LIST OF ACRONYMS USED

BISSI	Burns International Security Services, Inc.
CBOP	Continuous Behavioral Observation Program
CFR	Code of Federal Regulations
DRS	Division of Reactor Safety
FFD	Fitness-For-Duty Program
IFI	Inspection Followup Item
NEI	Nuclear Energy Institute
NGET	Nuclear General Employee Training
OAD	Operational Analysis Department
PIF	Problem Identification Form
QAA	Quality Assurance Audit

PARTIAL LIST OF DOCUMENTS REVIEWED

Contractor Security Status Report for January through December 1997

Site Quality Verification Audit Number QAA 22-997-01, Security/FFD/PADS Audit, dated April 30, 1997

Security Post Instructions for Special Posts established during heightened awareness

Monthly Security Report for November 1997

Security Event Log from June through December 1997

Job Description for Self Assessment Administrator, BISSI

Burns International Security Services Quality Assurance Audit Report No. UBU 96-04

Sargent & Lundy Safeguards Drawings associated with Turnovers (T/0s) #0000000048, 077, 078, 082, 083, 084, 085, 227, 229, 300 and 301.)