U.S. NUCLEAR REGULATORY COMMISSION

REGION III

Docket No:	50-305
License No:	DPR-43
Report No:	50-305/98003(DRS)
Licensee:	Wisconsin Public Service Corporation
Facility:	Kewaunee Nuclear Power Plant
Location:	RR#1, Box 99 Kewaunee, WI 54216
Dates:	January 28 through February 3, 1998
Inspectors:	T. J. Madeda, Physical Security Inspector J. R. Creed, Chief, Plant Support Branch 1
Approved by:	John A. Grobe, Director Division of Reactor Safety

EXECUTIVE SUMMARY

Kewaunee Nuclear Power Plant
NRC Inspection Report 50-305/98003

The purpose of the inspection was to evaluate an incident that involved the inadequate protection of Safeguards Information at the Kewaunee Nuclear Power Plant that was identified and reported on January 20, 1998. Safeguards Information stored outside of the protected area, while unattended, was not properly locked in a security storage container. The event was reported to the NRC as required by 10 CFR Part 73.71. Inspection activities were conducted between January 28 and February 3, 1998. The inspectors concluded that the failure to properly secure the protected information was not indicative of a programmatic weakness.

The following is a summary of the inspection findings and conclusions.

- One violation was identified regarding the failure to properly secure SGI stored outside the protected area in a controlled access area. The SGI was maintained in a cabinet secured with an inadequate locking device for approximately four years. The SGI consisted of sensitive information that identified the licensee's target sets and some response plans. This information, if compromised, might be of assistance to an adversary.

- The area where the SGI was stored was essentially maintained as a controlled access area. The boundaries of the area were of substantial construction and access was usually controlled by personnel recognition or locked doors. The SGI was stored in a cabinet that was improperly locked.

- Two security personnel, trained to maintain control over SGI, failed to recognize that the information was SGI. The failure was attributed to a misunderstanding by the two individuals of what was considered to be SGI.

Report Details

IV. Plant Support

S8 Miscellaneous Security and Safeguards Issues

S8.1 Failure to Protect Safeguards Information

a. Inspection Scope (IP 81810)

The inspectors reviewed, discussed, and evaluated the circumstances regarding a licensee-identified event that concerned the inadequate protection of three security manuals that contained Safeguards Information (SGI). The SGI was stored outside the protected area but within a controlled access area. Inspection activities included review of records and documents, interviews and observations.

b. Observations and Findings

On the morning of January 20, 1998, the security contractor project manager, while looking for some documents, opened a locked file cabinet secured with a key-type padlock and discovered a binder that was labeled as containing Safeguards Information (SGI). The cabinet was located in a security training office on the second floor of the security access building. The second floor of this building is located outside the protected area. The manager immediately recognized that the cabinet was not an approved SGI storage container and took control of the SGI stamped binder and the cabinet. Further search of the cabinet resulted in the identification of two additional binders that were also labeled/stamped as containing SGI. No additional protected information was found in the cabinet or other cabinets in the office. The licensee reviewed the information in the three binders and concluded that some of the information was SGI. The SGI consisted of current, specific vital area target sets which were identified by name and elevation location. Other information in the binders included out-of-date defensive strategies and scenarios. The licensee did not consider that information to be SGI because it was not specifically accurate. The licensee determined that the SGI had been stored in the manner described for approximately four years. The licensee reported the event in accordance with 10 CFR 73.71.

The licensee's finding demonstrated that the cabinet referenced above was not secured in accordance with NRC requirements. The file cabinet's locking device was not in accordance with 10 CFR 73.21(d) and 10 CFR 73.2 requirements which stipulate that SGI maintained outside the protected area in a controlled area must be stored in a cabinet equipped with a combination GSA-approved padlock. The failure to adequately protect Safeguards Information is a violation of NRC requirements (VIO 50-305/98003-01(DRS)).

When identified by the licensee, the SGI was removed from the cabinet and properly secured. The licensee's security director conducted an examination and determined that no evidence of tampering or compromise was discovered. No further examples of

inadequately secured SGI were found. The responsible individuals were interviewed, counseled, and retrained in their responsibilities to protect SGI. The event was briefed to all SGI custodians. The SGI was evaluated by the licensee to determine the impact on the licensee's current and specific defensive strategies.

Licensee evaluation of the information concluded that although some of it was SGI, and could be significant, the SGI would not assist a person in actually gaining undetected access or circumventing the physical security system because no information relating to the physical protection systems were identified.

Our evaluation of the event concluded that the SGI contained sensitive plant security information and, had it been compromised, could have assisted an individual in an act of radiological sabotage. However, the SGI was stored in a locked nondescript file cabinet in an office containing five additional cabinets which were similar. The key to the cabinet was likewise unmarked and maintained in a desk in the office. Only two personnel, both security trainers, were aware that the cabinet contained the protected information. Only personnel authorized access to SGI had access to the cabinet. The office in which the cabinet was located was usually locked or normally staffed by one or both of the trainers. On rare occasions the trainers would leave the office for short periods of time during cleaning activities. (Note: Cleaning personnel were screened for protected area unescorted access.) The office was located outside the protected area barrier, on the second floor of the security access building. The first floor of the building was continuously staffed by security personnel who generally monitored building activity. Access to the second floor was controlled during non-routine working hours because the exterior doors to the building were locked. During working hours, the second floor was routinely staffed by security personnel that monitored personnel access. We concluded that the access control functions implemented by the licensee to the building, the second floor office, and the cabinet significantly reduced the possibility of unauthorized personnel gaining access to the cabinet containing the SGI. .

The event occurred because two security trainers responsible for controlling protected information erred in believing that the information was not SGI. Their belief was based on conversations conducted in 1994 between them and licensee tactical response contractors that the licensee's defensive actions had been developed with the assumption that the plans could be compromised. The trainers apparently assumed these statements meant that the information was no longer SGI, dispute the marking. They failed to resolve, what amounted to conflicting information involving the marking and their assumptions. Contributing to this event was the failure by the two trainers to follow procedure guidance regarding the removal of the SGI designation when the information no longer meets the criteria of SGI. (Note: Section 5.8 of Licensee Nuclear Administrative Directive 15.8, "Control Of Safeguards Information," required that documents originally containing SGI shall be removed from the SGI category by the Security Director when the information no longer meets the criteria of SGI.) The individuals had been trained in this specific procedural requirement but in this case forgot to implement it. Had they implemented this procedure, the site security director would have discovered the error, and prevented the information from being improperly stored.

c. Conclusions

One violation was noted. The violation was cited because of the its duration (four years) and that two experienced, appropriately trained personnel failed to implement a portion of the SGI program. The SGI identified information that could assist an individual in an act of radiological sabotage. Unauthorized access to the SGI was limited because of effectively implemented access control measures to the area where the SGI was stored. The event was an isolated incident personnel error and not indicative of a programmatic problem. Effective corrective actions were implemented.

V. Management Meetings

X1 Exit Meeting Summary

The inspectors presented the inspection results to licensee management at the conclusion of the onsite inspection on January 29, 1998. The licensee was preparing additional information to the NRC regarding their review and analysis of the event. That information was provided to Region III on February 2, 1998. Our review was completed on February 3, 1998.

PARTIAL LIST OF PERSONS CONTACTED

Licensee

H. Duquain, QA Auditor
K. Evers, Manager, Plant Support
J. Fletcher, Security Director
G. Harrington, Plant Licensing
C. Schrock, Plant Manager

Security Contractor

A. Deder, Security Operating Supervisor
B. Presl, Project Manager

NRC

B. Clayton, Region III Enforcement/Investigation Officer
J. Creed, Chief, Plant Support Branch 1
J. Lara, Senior Resident Inspector
R. Rosano, Acting Chief, Safeguards Branch, NRR

INSPECTION PROCEDURES USED

IP 81810 Safeguards Information

ITEMS OPENED, CLOSED, DISCUSSED

Opened

50-305/98003-01	VIO	Failure to properly secure Safeguards Information.

DOCUMENTS REVIEWED

Licensee memorandums discussing a SGI incident that was reported on January 20, 1998	January 22, 28, 29 and February 2, 1998
Nuclear Administrative Directive NAD No. 15.3 "Control of Safeguards Information"	August 31, 1993

LIST OF ACRONYMS USED

GSA	General Services Administration
NRR	Office of Nuclear Reactor Regulation
NRC	Nuclear Regulatory Commission
OSRE	Operational Safeguards Response Evaluation
SGI	Safeguards Information