U.S. NUCLEAR REGULATORY COMMISSION

REGION III

Reports No. 50-263/90023(DRSS); 50-282/90018(DRSS); 50-306/90019(DRSS)

Docket Nos. 50-263; 50-282; 50-306 License No. DPR-22; DPR-43; DPR-60

Licensee: Northern States Power Company
414 Nicollet Mall
Minneapolis, MN 55401

Inspection At: Corporate Headquarters, Minneapolis, Minnesota

Inspection Dates: November 8, 1990 onsite
November 9 through 26, 1990 in NRC Region 1.1 office

Inspector: Terry J. Madeda 11/30/90
T. J. Madeda Date
Physical Security Inspector

Approved by: for Gary S. Pirtle 11/30/90
James R. Creed, Chief Date
Safeguards Section

Inspection Summary

Inspection on November 8-26, 1990 (Report Nos. 50-263/90023(DRSS); 50-282/90018(DRSS); 50-306/90019(DRSS))
Areas Inspected: Included a review and discussion of circumstances involving a licensee identified incident of inadequate storage of Safeguards Information at the licensee's corporate office.
Results: Based on the results of this inspection, one potential violation was identified regarding failure to adequately secure some significant Safeguards Information.

DETAILS

1. Key Persons Contacted

In addition to the key members of the licensee's staff listed below, the inspector interviewed other licensee employees and members of the security organization. The asterisk (*) denotes those present at the corporate office Exit Interview conducted on November 8, 1990.

*G. Ortler, Manager, Nuclear Human Resources
*L. Waldinger, Manager, Production Training
*G. Miserendino, Manager, Corporate Security
*C. Bowman, Supervisor, Corporate Screening Services
*J. Kreger, Security Consultant
*B. Anderson, Security Consultant
*R. Cleveland, Fitness-For-Duty Coordinator
*D. Schroeder, Security Screening Consultant
D. Brose, Security Consultant

2. Entrance and Exit Interviews (IP 30703):

a. At the beginning of the inspection, the Corporate Manager of Security and other staff members were informed of the purpose of the visit and the functional areas to be examined.

b. The inspector met with the licensee representatives denoted in Section 1 at the conclusion of the onsite inspection on November 8, 1990. A general description of the scope of the inspection was provided. Briefly listed below are the findings discussed during the exit interview. The details of each finding discussed are referenced, as noted, in this report. Included below is a statement provided by or describing licensee management's response to each finding.

The inspector described a potential escalated violation involving a failure to adequately secure Safeguards Information. The inspector noted that the licensee identified that the security storage cabinet within the corporate headquarters which contained significant Safeguards Information was left unlocked, open, and unattended. The licensee initiated corrective action, as described in Section 4 of the Report Details, to prevent recurrence.

Licensee management agreed with the facts presented by the inspector regarding the unsecured container. They emphasized that the event was identified by the licensee, promptly reported to the NRC, and that corrective action was immediately implemented.

c. On November 28, 1990, the Corporate Manager of Security was contacted to clarify some issues related to our review and, during the telephone contacts, we arranged to hold an enforcement conference in Region III at 11:00 a.m. on December 6, 1990.

3. Program Areas Inspected (MC0610):

Listed below are the areas which were examined by the inspector within the scope of these inspecti. activities. These areas were reviewed and evaluated as deemed necessary by the inspector to meet the specified "Inspection Requirements" (Section 02) of the applicable NRC Inspection Procedure (IP) and appropriate NRC regulations. Only those areas in which findings were identified are discussed in subsequent report sections. Sampling reviews included interviews, o[illegible]tions and document reviews. The depth and scope of activities were [illegible]ted as deemed appropriate and necessary for the program area being inspec[illegible].

Number	Program Area and Inspection Requirements Reviewed
81810	Protection of Safeguards Information: (01) General; (02) Access to Safeguards Information; (05) Storage; (07) Reproduction;

4. Protection of Safeguards Information (IP 81810): One potential violation was identified and is described below:

On November 5, 1990, a member of the licensee's Corporate Security Department, upon reporting to work at approximately 7:00 a.m., found a Safeguards Information security container unlocked and the area unattended. The licensee later determined that the security container was in this condition from approximately 5:00 p.m., November 2, 1990, to approximately 7:00 a.m., November 5, 1990 (a period of 62 hours). This is a potential violation of 10 CFR 73.21(d)(2) which requires unattended Safeguards Information to be stored in a locked security storage container.

The Corporate Security Department is located in downtown Minneapolis, Minnesota, and Northern States Power is the sole occupant of the building. Access to the building during non-work hours is gained through entrances which are either controlled by a security guard or a keycard reader, and access is limited to employees, or visitors under employee escort. The building and security department is designed in an "open area" configuration (office partitions). The security container is physically located in an alcove in the security department and cannot be observed from outside of the security department's office area. The corporate security office is not manned during non-business hours.

The licensee's investigation of the incident showed that an informal practice existed for checking that Safeguards Information was adequately secured when unattended. The licensee's previous Corporate Security Manager had established an unwritten policy several years ago that one member of the Corporate Security Staff would be "responsible" for assuring that Safeguards Information security containers were closed and locked at the end of each work day. As a result of this unwritten policy, one member of the Corporate Security Staff is "assigned" each week to check the security container at the end of each day.

The corporate security employee assigned to secure the container on November 2, 1990, stated that he was aware of his responsibility to close and secure the security container. The individual recalled closing the

container, but did not recall checking to assure that the container was locked. During the 62 hour period when the security container was unsecured, approximately 185 company employees entered the building. Apparently, none of these individuals required access to Safeguards Information. At approximately 4:30 p.m. on Sunday, November 4, 1990, a watchman assigned to firewatch duties made his scheduled tour of the building, which included the corporate security office. He later stated that he had observed one drawer of the security container to be slightly open (approximately 1½"). The watchman did not take any additional action to close, lock, or report the finding since his duties only involved firewatch patrols and he had never been instructed to check cabinets. The individual was not able to recognize the significance of the unsecured container. No other individual interviewed by the licensee could recall seeing the security container over the weekend period. Firewatch tours are routinely conducted about once each hour and a half during nonworking and backshift weekend periods.

At 7:00 a.m. on November 5, 1990, the security container was found to be open and unlocked by a member of the Corporate Security Staff upon reporting to work. The Corporate Security Manager was notified and an investigation was immediately initiated. The event was reported by telephone to the NRC at approximately 9:07 a.m. on November 5, 1990. The telephone report was later retracted and the event was logged as stipulated in 10 CFR 73.71.

The licensee's investigation showed that the security container stored copies of the Monticello and Prairie Island Physical Security Plans (PSP); Training and Qualification Plans (T&QP); Safeguards Contingency Plans (SCP); written physical security procedures, and offsite response force commitments. This type of information is considered significant and is required to be protected as Safeguards Information as described in 10 CFR 73.21(b)(1). The security container also stored numerous pieces of correspondence and security audit reports which were also considered by the licensee to be Safeguards Information.

The licensee determined, through inventory results, that all marked documents containing Safeguards Information were located and accounted for. Through interviews with building watchmen and building management personnel, it was determined that no unusual activity in the building or the security department was identified or reported. Interviews of watchmen also concluded that they had not observed use of copying machines by personnel over the weekend period.

Licensee corrective actions consisted of: (1) retraining the Corporate Security Staff in the proper procedure for closing and locking security containers; (2) a corporate procedure was developed and implemented for securing Safeguards Information. The procedure included specific steps to be taken to lock the containers, check that the containers are locked, and document the results; and (3) building security personnel were instructed to identify and report any unlocked security containers observed in the Corporate Security Department during their rounds and to lock such containers if found open; and (4) the responsible individual was formally reprimanded for not properly securing the security container.

The inspector reviewed the investigative results and concluded that the security container was not secured, and that one drawer of the security container was in a slightly open position for approximately 62 hours. Safeguards Information which could significantly assist someone in an act of radiological sabotage was stored within the security container. However, the potential for compromise of the Safeguards Information was low. This conclusion is based on the randomness of the time period the security container was left unlocked. The open security container was easy to identify once it was located since a drawer was open, but, the container was difficult to find since it was located in an alcove in the security department. Also contributing to the difficulty in locating and identifying the security container was the size of the office building (8 floors). Finally, some degree of access control was provided by security guards and key card readers at the outside entrances to the building. Collectively, these factors resulted in the determination that there was a low potential that the information was actually compromised.

This finding represents a potential violation of NRC regulations that require that Safeguards Information be locked in a secured container if left unattended. The failure resulted from human error (failure to lock the container). The licensee has taken adequate initial corrective actions that should prevent recurrence.

On November 26, 1990, the Corporate Security Manager informed NRC Region III that a entry door to the Corporate Security Department had been installed on November 21, 1990, as part of their long term corrective actions. Access through this door is controlled by a card reader. Individuals allowed access are limited to members of the Corporate Security Staff, building patrol officers, and one janitorial person. This action increases the level of protection for the security containers within the security department.