NIAGARA MOHAWK

NINE MILE POINT NUCLEAR STATION / P.O. BOX 32 LYCOMING, NEW YORK 13093 / TELEPHONE (315) 343-2110

May 29, 1987

Mr. Thomas E. Murley
Office of Nuclear Reactor Regulation
United States Nuclear Regulatory Commission
Washington, DC 20555

Re: Nine Mile Point Unit #1 and Unit #2
Docket No. 50-220/50-410
DPR-63/NPF-54

Dear Mr. Murley:

In accordance with 10CFR 73.71(c), enclosed for your information is a copy of a Report of Physical Security Event reported to the NRC Region I office by telephone on May 22, 1987.

This information concerns subject matter which is exempt from disclosure under 2.790(d) of the NRC's Rules of Practice, Part 2, Title 10, Code of Federal Regulations. Accordingly, we request that the attachment not be placed in the Public Document Room and that they be disclosed only in accordance with the provisions of 10CFR 9.12.

Very truly yours,

NIAGARA MOHAWK POWER CORPORATION

Joseph P. Beratta

Joseph P. Beratta
Supervisor, Nuclear Security

JPB/kar

Enclosure

8706040307 XA 4pp.

H/84

IE21
1/1

REPORT OF PHYSICAL SECURITY EVENT

REGION I, USNRC, OFFICE OF INSPECTION AND ENFORCEMENT
631 PARK AVENUE, KING OF PRUSSIA, PA. 19406
PHONE (215) 337-5000

Date of Occurrence: 05/21/87

Time of Occurrence: 1525 hrs

Facility and Location: Nine Mile Point Nuclear Station
Unit 1 & Unit 2, Lycoming, NY 13093

Docket Nos.: 50-220/50-410
License Nos.: DPR-63/NPF-54

Licensee's Occurrence Report No. 87-02

Brief Title (Subject): Security File Restrictive Level Applicator for Access Control

DESCRIPTION OF EVENT: On Thursday, May 21, 1[illegible], at approximately 1525 hours, a guard inadvertently inserted a contractor's Photo-ID Badge into the Unit I Access Control Room (ACR) card reader activating the ACR door. Immediately after verifying that the subject Photo-ID Badge did not have the proper restricted level for accessing the ACR door, the Security Supervisor felt it necessary to randomly select several other Photo-ID badges in an effort to duplicate the same sequence of events. Consequently, several of the Photo-ID Badges activated not only the ACR door but also activated the [redacted] a vital area. A complete chronology of events and actions taken to correct the root causes are contained on attached pages.

RESPONSE BY LICENSEE: Immediately upon realizing the scope of the problem, Security Supervision, in accordance with the Safeguards and Contingency Plan, activated the [redacted]

CONSEQUENCES AT FACILITY: Minimal; keeping in mind that compensatory measures were implemented immediately and the fact that we have [redacted] watchtour in addition to the [redacted] Additionally, a spot check was conducted of Vital Area card readers verifying that no unauthorized entries had been made.

Licensee Employee Reporting: Daniel D. O'Hara, Asst. Nuclear Security Specialist (315) 349-1319

NRC Staff Employee Receiving Phone Call: Mr. Joseph Gritter, H.O.O.

Date of Phone Call: 05/22/87

Time of Phone Call: 1320 hours

SECURITY EVENT REPORT 87-02
Nine Mile Point Unit #1 and Unit #2
50-220/DPR-63
50-410/NPF-54

This report is to inform you of a degradation of the Main Alarm System (MAS) discovered by Security Management on May 21, 1987. The scope of the degradation involved, the security file (s-file) restricted level scheme, which had not been effectively holding for door access control.

[redacted]

At 1525 hours on May 21, 1987, a Unit One Guard returning from the vehicle gate post, inadvertently inserted a contractor's keycard into the Access Control Room (ACR) card reader and it accessed the ACR door. The Guard then advised the Security Supervisor on duty of the sequence of events and immediately verified that the Keycard did not have the proper restricted level for accessing the door.

In an effort to determine if this was an isolated incident, the Security Supervisor randomly selected several other Keycards and found that they, too, accessed the ACR door.

The Security Supervisor felt it necessary to ascertain if the same conditions existed at Vital Areas at both Units. Immediately, a random check of both Units indicated that restricted level access for door control was not holding properly.

Upon realizing the scope of the problem, Security Supervision activated the

[redacted]

In a formal conversation with computer personnel, it was realized that a revision had been made to the disc used in the computer system. The revision had been in place since the previous Thursday; May 14, 1987, at which time the contractor responsible for the computer system corrected a problem with restricted level termination dates. However, it appears that the revision jarred the logic of the restricted level applicator which controls door access.

[redacted]

However, it appeared that the computer system was allowing access to any card containing a restricted level; in essence" a go-no go" type situation.

Immediately, a patch was incorporated to bypass this faulty logic, and a test conducted to confirm proper operation. A spot check of Vital Area Entry transactions was undertaken at both Units for the seven day period, this revealed that no unauthorized entries had been made.

The subject disc was replaced with a corrected revision, tested, and proven effective in holding restricted level access control.

To preclude a recurrence, the [redacted] alarms test procedure has been revised. In addition, any time a software fix has been completed, an additional test will be conducted to include a check of restricted levels.