Consumers Energy

A CMS Energy Company

Palisades Nuclear Plant
27780 Blue Star Memorial Highway
Covert, MI 49043

Tel: 616 764 2296
Fax: 616 764 2425

Thomas J. Palmisano
Site Vice President

March 17, 1998

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

DOCKET 50-255 - LICENSE DPR-20 - PALISADES PLANT
LICENSEE EVENT REPORT 98-004 - DISCOVERY OF CARD READER VULNERABILITY AND INSUFFICIENT COMPENSATORY MEASURES TAKEN

Licensee Event Report 98-004 is attached. This event is reportable to the NRC in accordance with 10 CFR 73.71(b)(1) because a vulnerability was discovered in the card reader system and insufficient compensatory measures were taken.

SUMMARY OF COMMITMENTS

This letter contains two new commitments and no revisions to existing commitments. The commitments are:

1. Revise Security Implementing Procedure #8 to specifically indicate that keycards shall not be ordered with five digit identification numbers of 00001 through 00099.

2. Add the Palisades Security Reporting Matrix, which includes compensatory actions, to the appropriate Security Implementing Procedure.

200011

Thomas J. Palmisano
Site Vice President

CC Administrator, Region III, USNRC
Project Manager, NRR, USNRC
NRC Resident Inspector - Palisades

Attachment

1/1
IE74

NRC FORM 366 (4/95) U.S. NUCLEAR REGULATORY COMMISSION

APPROVED BY OMB NO. 3150-0104
EXPIRES 4/30/98

ESTIMATED BURDEN PER RESPONSE TO COMPLY WITH THIS MANDATORY INFORMATION COLLECTION REQUEST: 50.0 HRS. REPORTED LESSONS LEARNED ARE INCORPORATED INTO THE LICENSING PROCESS AND FED BACK TO INDUSTRY. FORWARD COMMENTS REGARDING BURDEN ESTIMATE TO THE INFORMATION AND RECORDS MANAGEMENT BRANCH (T-6 F33), U.S. NUCLEAR REGULATORY COMMISSION, WASHINGTON, DC 20555-0001, AND TO THE PAPERWORK REDUCTION PROJECT (3150-0104), OFFICE OF MANAGEMENT AND BUDGET, WASHINGTON, DC 20503

LICENSEE EVENT REPORT (LER)

(See reverse for required number of digits/characters for each block)

FACILITY NAME (1)	DOCKET NUMBER (2)	Page (3)
CONSUMERS ENERGY COMPANY PALISADES NUCLEAR PLANT	05000255	1 of 5

TITLE Discovery of Card Reader Vulnerability and Incorrect Compensatory Measures Taken

EVENT DATE (5)			LER NUMBER (6)			REPORT DATE (7)			OTHER FACILITIES INVOLVED (8)	
MONTH	DAY	YEAR	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	MONTH	DAY	YEAR	FACILITY NAME	DOCKET NUMBER 05000
02	16	98	98	004	00	03	17	98	FACILITY NAME	DOCKET NUMBER

OPERATING MODE (9)	N
POWER LEVEL (10)	100

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR§: (Check one or more) (11)

	20.2201(b)		20.2203(a)(2)(v)		50.73(a)(2)(I)		50.73(a)(2)(iii)
	20.2203(a)(1)		20.2203(a)(3)(I)		50.73(a)(2)(ii)		50.73(a)(2)(x)
	20.2203(a)(2)(I)		20.2203(a)(3)(ii)		50.73(a)(2)(iii)	x	73.71
	20.2203(a)(2)(ii)		20.2203(a)(4)		50.73(a)(2)(iv)		OTHER
	20.2203(a)(2)(iii)		50.36(c)(1)		50.73(a)(2)(v)		Specify in Abstract below or in NRC Form 366A
	20.2203(a)(2)(iv)		50.36(c)(2)		50.73(a)(2)(vii)		

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER (Include Area Code)
Barbara E. Dotson, General Technical Analyst	(616) 764-2265

COMPLETE ONE LINE FOR EACH COMPONENT FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS	CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS

SUPPLEMENTAL REPORT EXPECTED (14)				EXPECTED SUBMISSION DATE (15)	MONTH	DAY	YEAR
	YES If yes, COMPLETE EXPECTED COMPLETION DATE	x	NO				

ABSTRACT (Limit to 1400 spaces, i.e., approximately 15 single-spaced typewritten lines) (16)

On February 16, 1998, with the plant operating at 100% power, a Consumers Energy employee notified security that an escorted visitor had inserted her keycard into an exiting turnstile card reader upside down, and received a green light, activating the turnstile. Security and Maintenance personnel responded to the event by performing system testing, and found that access was allowed to a number of both protected and vital area doors when specific key cards were inserted upside down in specific card readers. Compensatory measures were instituted during the event, but were later determined to be insufficient, based on the scope and nature of the system failure. Additional compensatory measures were then instituted, which met the procedural requirements.

An Incident Response Team was formed on February 17, 1998, to evaluate the event, and to determine the course of action for resolution of issues associated with the event.

The card reader system was returned to service on February 21, 1998, upon completion of corrective actions and extensive system testing.

EVENT DESCRIPTION

On February 16, 1998, the plant was operating at 100% power. A Consumers Energy employee notified security that the visitor she was escorting had inserted her keycard into the exiting turnstile card reader upside down and received a turnstile activation signal. Security tested the keycard in the card reader and verified that it did activate the turnstile card reader. The keycard status shown on the card reader system printer for the transaction indicated the keycard would allow access to some plant vital areas. As a result, testing was performed on other card readers using the same keycard, and in addition, using a security employee's badge. Both badges were inserted upside down. It was determined that both badges, when inserted incorrectly, allowed access to a number of plant doors to both protected areas and vital areas.

When security confirmed the keycard would open doors it was not programmed to open, compensatory actions were instituted.

The Property Protection Supervisor (PPS) and Burns Security Site Manager were called to the site and began reviewing actions taken. It was determined that compensatory actions in place were insufficient, based on the scope and nature of the system failure. Additional compensatory measures were instituted, which met procedural requirements. Based on the failure to implement appropriate compensatory measures within a ten minute time period, as required by the Palisades Security Reportability Matrix and 10 CFR Part 73, Appendix G, a one-hour NRC notification was made. The card reader system was deactivated and compensatory measures remained in place until the system was restored.

Upon completion of troubleshooting and corrective measures, the system was successfully tested. Review and approval by the Plant Shift Supervisor, allowed the system to be returned to service on February 21, 1998.

ANALYSIS OF EVENT

Maintenance performed troubleshooting and was eventually able to duplicate the system vulnerability on a simulated system mock-up. System testing determined that the scope of the problem was larger than originally identified.

Bleed-through is a phenomena, in the RS-40 Security card reader system, that sometimes occurs when a keycard is inserted into a card reader upside down. The card reader coils which read the magnetic information on the keycard, are able to read the last two digits of the five digit number

programmed to the badge. Investigation found that at card readers where bleed-through was occurring, the card reader would send a five digit number consisting of three or four leading zeroes and one or two digits (000xx or 0000x) to the card reader console when the keycard was inserted upside down. If the five digit number produced by bleed-through matched any five digit number currently programmed in the card reader system memory, with a valid status, the card reader would activate.

Maintenance personnel learned from security personnel that the newest batch of keycards had five digit identification numbers starting with 00001 and continuing through 00099. 38 of these badges had been issued to plant personnel, and the five digit identification numbers had been programmed into the card reader system memory database. New keycards with three or more preceding zeroes had been issued to plant personnel starting on December 29, 1997, and continued until February 17, 1998, when it was determined that they contributed to the cause for the vulnerability. Based on these dates, the window of vulnerability was approximately seven weeks.

When the vulnerability was identified at vital area (VA) doors, compensatory measures were implemented. This occurred at approximately 1726 hours on February 16, 1998. At approximately 1822 hours, it was determined that these compensatory measures were not sufficient based on the Palisades Security Reporting Matrix guidance. It was not until 1841 hours that the correct compensatory measures were implemented at all VA doors then known to be affected. Thus, there was a delay of approximately 75 minutes before correct compensatory measures were instituted on affected VA doors. This delay in initiation of sufficient compensatory measures led to the determination that a one-hour NRC notification was necessary.

SAFETY SIGNIFICANCE

Operation of the plant was not affected by this event, however, this event had the potential to indirectly affect plant safety. When the card readers were deactivated, operators' response to vital plant equipment during a plant transient could have been delayed. Operations has four VA keys assigned to them which can be used at any time to allow entry into all plant vital areas. During this event, the card readers were deactivated by Security for positive control purposes, but could have been reactivated at any time at the direction of the Operations Department.

CAUSE OF THE EVENT

The cause of the card reader system vulnerability was due primarily to card reader bleed-through, as described above.

Causes for the delay in the establishment of sufficient compensatory actions were that the Security Shift Leader (SSL) did not immediately refer to procedures when the event started. Eventually, he referred to the non-safeguards Palisades Security Reportability Matrix which did not contain compensatory actions. This led to misjudgement on how to compensate for the event. In addition, other Security Supervisors had limited knowledge of event conditions due to inadequate communications from the SSL. This prevented the possibility of another Security Supervisor identifying correct compensatory actions. Timely communication of the event to the plant Shift Supervisor was also inadequate. This also prevented an opportunity for the Shift Supervisor to provide input to the SSL about compensatory actions.

Command and control expectations were not met in that the SSL became involved in testing, called in additional personnel and made notifications when he should have been maintaining an oversight and command function. Other Security Supervisors should have performed these responsibilities and the SSL should have focused on the scope of system vulnerabilities, reportability and necessary compensatory actions.

CORRECTIVE ACTIONS COMPLETED

1. Initiated a quarterly surveillance to verify card reader system memory addresses contain correct data.

2. Eliminated keycards programmed with 00001 through 00099, where bleed-through was possible, with the exception of six keycards maintained by Maintenance for future testing activities.

3. Issued programming guidance to personnel responsible for programming and deprogramming of keycard information.

4. Revised the card reader system test to include use of an upside down keycard.

5. Briefed Security Supervisors involved in the event and critiqued the response to the event to develop and reinforce "lessons learned".

6. A detailed communications package discussing the event was given to all Security Shift Leaders for discussion with security personnel. The communications package has also been posted to security bulletin boards. In addition, a required reading package was assembled for review by the entire security force.

7. Removed the non-safeguards Palisades Security Reporting Matrix from on-site security posts to eliminate any confusion in initiation of compensatory actions.

CORRECTIVE ACTIONS TO BE COMPLETED

1. Revise Security Implementing Procedure #8 to specifically indicate that keycards shall not be ordered with five digit identification numbers of 00001 through 00099.

2. Conduct training for the entire Security force on the event lessons learned.

3. Add the Palisades Security Reporting Matrix, which includes compensatory actions, to the appropriate Security Implementing Procedure.

4. Review other Security Department job aids for appropriateness and determine whether they should be incorporated into procedures.