CATEGORY 1

REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR:9904290137 DOC.DATE: 99/04/23 NOTARIZED: NO DOCKET #
FACIL:50-269 Oconee Nuclear Station, Unit 1, Duke Power Co. 05000269
AUTH.NAME AUTHOR AFFILIATION
KING,T.W. Duke Power Co.
MCCOLLUM,W.R. Duke Power Co.
RECIP.NAME RECIPIENT AFFILIATION

SUBJECT: LER 99-S01-00:on 990304,potential vulnerability of plant security computer sys,was determined.Caused by inadequate sys knowledge,verbal & written communications.Patrol search of protected & vital areas conducted.With 990423 ltr.

DISTRIBUTION CODE: IE74T COPIES RECEIVED:LTR 1 ENCL 1 SIZE: 9
TITLE: Safeguards Phys Sec Event Pt. 73.71 (Public Available)

NOTES:

	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL
	LABARGE,D	1	0			
INTERNAL:	AEOD/SPD/RRAB	1	1	FILE CENTER	1	1
	NMSS/FCSS/FCOB	1	1	NUDOCS FULLTEXT	1	1
	RGN2 01	1	1			
EXTERNAL:	NRC PDR	1	1			

NOTE TO ALL "RIDS" RECIPIENTS:
PLEASE HELP US TO REDUCE WASTE. TO HAVE YOUR NAME OR ORGANIZATION REMOVED FROM DISTRIBUTION L
OR REDUCE THE NUMBER OF COPIES RECEIVED BY YOU OR YOUR ORGANIZATION, CONTACT THE DOCUMENT CON
DESK (DCD) ON EXTENSION 415-2083

FULL TEXT CONVERSION REQUIRED
TOTAL NUMBER OF COPIES REQUIRED: LTTR 7 ENCL 6

CATEGORY 1 DOCUMENT

Duke Energy

Duke Energy Corporation
Oconee Nuclear Site
P.O. Box 1439
Seneca, SC 29679
(864) 885-4000

April 23, 1999

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555

Subject: Oconee Nuclear Station
Docket Nos. 50-269, -270, -287
Licensee Event Report 269/1998-S02, Revision 0
Problem Investigation Process No.: 4-098-5678

Gentlemen:

Pursuant to 10 CFR 73.71 Sections (b) (1) and (d) and Appendix G (I)(b), attached is Licensee Event Report 269/1999-S01, concerning the potential vulnerability of the Plant Security Computer System.

This report is being submitted in accordance with 10 CFR 73.71 appendix G (I) (b). This event is considered to be of no significance with respect to the health and safety of the public.

Very truly yours,

W. R. McCollum, Jr.

Attachment

cc: Mr. Luis A. Reyes
Administrator, Region II
U.S. Nuclear Regulatory Commission
61 Forsyth Street, S. W., Suite 23T85
Atlanta, GA 30303

Mr. D. E. LaBarge
U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Washington, D.C. 20555

INPO Records Center
700 Galleria Parkway, NW
Atlanta, GA 30339-5957

Mr. M. A. Scott
NRC Resident Inspector
Oconee Nuclear Station

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

APPROVED OMD NO. 3150-0104
EXPIRES: 04/30/98
ESTIMATED BURDEN PER RESPONSE TO COMPLY WITH THIS INFORMATION COLLECTION REQUEST: 50.0 HRS. FORWARD COMMENTS REGARDING BURDEN ESTIMATE TO THE INFORMATION AND RECORDS MANAGEMENT BRANCH (MNBB 7714), 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)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Oconee Nuclear Station, Unit 1	05000 269	1 of 7

TITLE (4)
Potential vulnerability of the Plant Security Computer System

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(S)
										Unit 2	05000 270
03	04	99	1999	-	S01	- 0	04	23	99	Unit 3	05000 287

OPERATING MODE (9)	N	THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR (Check one or more of the following) (11)					
POWER LEVEL (10)	099	20.402(b)	20.405(c)	50.73(a)(2)(iv)	X	73.71(b)	
		20.405(a)(1)(i)	50.36(c)(1)	50.73(a)(2)(v)		73.71(c)	
		20.405(a)(1)(ii)	50.36(c)(2)	50.73(a)(2)(vii)		OTHER (Specify in Abstract below and in Text, NRC Form 366A)	
		20.405(a)(1)(iii)	50.73(a)(2)(i)	50.73(a)(2)(viii)(A)			
		20.405(a)(1)(iv)	50.73(a)(2)(ii)	50.73(a)(2)(viii)(B)			
		20.405(a)(1)(v)	50.73(a)(2)(iii)	50.73(a)(2)(x)			

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER
Terry W. King, Security Manager	AREA CODE (864) 885-3019

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 SUBMISSION DATE)	X NO				

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

On 3/24/99 at approximately 1710 hours, with Unit 1 at 99% power and Unit 2 and 3 at 100% power, it was determined that a potential vulnerability existed in the Plant Security Computer System. While conducting testing on the test computer system at the Duke Energy General Office in Charlotte, a Duke Energy Information Management employee and a Syseca representative were able to download files to the Oconee Plant Security Computer System. It was determined that one level of the protection barriers for the Plant Security Computer System was not performing its intended function. This resulted in an unplanned reduction in the level of separation of the PSCS from the Duke Intranet. Some levels of protection were still afforded to prevent unauthorized access to the network. A validation of the Plant Security Computer System data was completed on 3/25/99 with no discrepancies discovered. The investigation concluded that there had not been unauthorized access to the PSCS data and that unauthorized entry into the Protected Area did not occur during this event.

Background:

The Plant Security Computer System (PSCS) Replacement Project has been on going for the last 3-4 years at Duke Energy. Installation began at Oconee in 1998. The project is a joint effort between Duke Energy and Syseca Inc. and has been managed centrally at the Duke Energy General Office. The PSCS is an integrated system of computer hardware and software applications that is connected to the Video Badging Network (VBN) system. Security badges for accessing protected and vital areas are issued through the VBN system. The VBN badging workstation at the Oconee Site uploads information to the main VBN server located at the McGuire Nuclear Site (MNS). The information is then downloaded from the McGuire VBN server to the primary controlling PSCS host computer at Oconee. The Oconee PSCS host computer then updates access data to remote control panels (RCPs) associated with controlled access doors (CADs) and entry turnstiles.

Over the last two months a dramatic increase in the number of badge link alarms between the Plant Security Computer System and Video Badging Network system were being observed. The badge link alarm indicates that the software process associated with the PSCS network can not connect to the VBN network. In an effort to troubleshoot these problems, the Duke Power PSCS project team and Syseca recommended that the encryption servers be temporarily disabled between the Oconee PSCS and McGuire VBN server. Syseca believed that the errors being seen were directly related to a timing problem between the encryption servers and the VBN database at McGuire. Disabling the encryption servers at Oconee would allow Syseca to determine if a decrease in link errors were directly related to encryption servers. Prior to disabling the encryption servers from service, Duke Energy network experts in the Information Management Group in Charlotte reviewed the security network to determine if unauthorized access could be gained to the databases. It was determined by the Information Management Group that the encryption servers were not required to prevent unauthorized access to the database due to the network routing design, the unpredictability of the bit streams of data being transmitted, and PSCS database software design.

Due to the configuration management of the Oconee PSCS network routers "ONSSCACAN1" and "ONSSCACAN2", reconfiguration of security filters was necessary to allow the bypassing of the encryption servers. "ONSCACAN1" and "ONSSCACAN2" routers are the "Gateway" in which packets of information are communicated between the VBN system at McGuire and the Oconee PSCS. Security filters screen the incoming information packets to determine which packets of information the filter recognizes as well as actions the filter takes when it recognizes a packet. Oconee filters are applied in layers where each filter specifies a set of addresses from which information packets may or may not flow. Each filter is named and each filter is configured to specify what actions should be taken. Each incoming packet of information is tested against each filter in the list and at the first address match the appropriate action is taken.

During the planning phase to bypass the encryption servers it was identified by Oconee Local Information Technology (LIT) that the "DROP-ALL" filter #8 would have to be disabled in order to bypass the encryption servers. A Process Computer System Modification package "VN-52931 AL1 BI" with technical instructions to bypass the encryption servers to the Oconee Plant Security System was completed with an implementation date of March 4, 1999.

EVENT DESCRIPTION:

The following information is the sequence of events that occurred from the disabling of "DROP-ALL" filter #8 to discovery and re-enabling of filter #8:

3/4/99 11:00	Router "DROP-ALL" filter #8 was disabled by an Oconee Local Information Technology (LIT) employee in preparation for bypassing the Oconee Plant Security Computer System (PSCS) encryption servers.
3/4/99 14:30	The modification (VN-52931 AL1 BI) to disable the encryption servers was initiated by Oconee LIT and the PSCS Project Team.
3/4/99 15:15	The modification to PSCS network configuration was completed and the encryption servers were no longer being utilized.

3/4-22/99		Troubleshooting the problems with the link from the Video Badging Network (VBN) at McGuire to Oconee's PSCS was conducted by the PSCS Project Team and Syseca.
3/22/99	17:00	Oconee PSCS network reconfiguration was completed to place the encryption servers back in service.
3/24/99		While conducting testing on the test computer system in the Duke Energy General Office in Charlotte, a Duke Energy Information Management employee and the vendor representative from Syseca discovered that Oconee files were being copied from the test computer system to the PSCS host. An investigation was conducted by the PSCS Project Team to determine if the files could be accessed from the General Office Test System. It was concluded that with a valid ID and password the Oconee PSCS network could be accessed via the Duke Power Intranet.
3/24/99		Oconee Security and the Oconee LIT group were notified that the Oconee PSCS network could be remotely accessed from the General Office. The Oconee LIT group concluded that the "DROP-ALL" Filter #8 on the Oconee PSCS routers should have prevented access to the Oconee network.
3/24/99	13:00	"DROP-ALL" Filter #8 was enabled. At this time encryption and router protection were in place.

CAUSAL FACTORS:

The evaluation of the facts of this event leads to the conclusion that the root cause was inadequate system knowledge with contributing factors of inadequate verbal communications and inadequate written communications. The knowledge of the router configuration for the PSCS is limited to a few individuals. In preparation for the modification to bypass the encryption servers, there were internal communications in the Oconee Local Information Technology (LIT) Group discussing the necessity to disable the filter. During the

discussion, consequences associated with the disabling of the "DROP-ALL" filter #8 were not adequately communicated to or not fully understood by the individual coordinating the planning process for the Oconee LIT group. Due to a lack of full understanding of the router configuration, the risk factors were not properly identified in preparation for the Process Computer System Modification package. The Technical Instructions did not adequately describe the task requirements for disabling the filter and re-enabling the filter after the encryption servers were bypassed. In addition, the risk factors of disabling the filters were not included in the modification package. The omission of relevant information in the Process Computer System Modification package was not discovered during the approval process due to inadequate knowledge of the router configuration by personnel reviewing the package.

Previous problems with PSCS hardware and software resulted in a failure investigation as part of the Problem Investigation Process (PIP). The investigation of these previous problems also identified documentation and knowledge of the PSCS as a contributing factor. Corrective actions identified had not been fully implemented at the time of this event and therefore could not have prevented this event.

CORRECTIVE ACTIONS:

IMMEDIATE:

1. Patrol/search of the Protected Area and all Vital Areas was conducted for any unauthorized personnel, material or abnormal activity.
2. Maintained heightened awareness of for any unauthorized personnel, material or abnormal activity in the Protected Area and vital areas until the subsequent corrective actions were completed.

SUBSEQUENT:

1. Validation of the Video Badging Network (VBN) data and Oconee Plant Security Computer System (PSCS) data was completed on March 25, 1999.

PLANNED:

1. Conduct assessment of Plant Security Computer System (PSCS) router configuration design.
2. Develop Configuration Management document for PSCS router design.
3. Provide additional technical training for router equipment and system for appropriate personnel.

Planned corrective actions 2 and 3 are considered to be NRC Commitment Items These are the only NRC Commitment items contained in this LER.

SAFETY ANALYSIS:

Prior to March 4, 1999 all data between the Oconee Plant Security Computer System and the McGuire Video Badging Network (VBN) system was encrypted. On March 4 through March 22, 1999, the filter configuration on Oconee routers "ONSSCACAN1" and "ONSSCACAN2" was modified by disabling the "DROP-ALL" Filter #8. When "DROP-ALL" filter #8 is enabled, it blocks all IP traffic destined for the Oconee PSCS network that is not specifically allowed access by the other layer of filters. Even though IP addresses that were previously blocked from the Oconee PSCS network could access the network, some levels of protection were still afforded to prevent unauthorized access. These levels of protection included:

1. The Plant Security Computer System Network is only accessible from the internal Duke computer network.
2. No IP address outside of the Duke Energy network could access the Oconee Security Network.
3. If access were gained from the network within Duke Power, the user would have to supply the appropriate IP Address or a Host Computer Name.
4. If access was gained from the Duke Intranet, and the appropriate IP address or a host name was known, the user would still have to supply a valid user ID and password to log into the system. In addition, the user would have to supply another valid ID and password including the appropriate software to log into the

database that contains the PSCS data. Knowledge of the time frame that the "DROP-ALL" filter was disabled would have been required.

In the event the above levels of protection were infiltrated, a user could have accessed the Oconee Plant Security Computer database. Once inside the database, badging data and security device data could have been altered. Any creation of new access authorization data in the database would have also required access to a composition of additional specialized hardware before a badge could have been fabricated.

A review of the Video Badging Network (VBN) data and Oconee Plant Security Computer System (PSCS) data was completed on March 25, 1999. A comparison of the badging data and security device status was conducted by comparing reports retrieved from the system prior to the disabling of filter #8 on March 4, 1999 and the current system data. The name, social security number, areas of access, badge ID and status of the badge were verified during the review of the badging information. The Security devices verified included microwave units, e-flex cables, controlled access doors, alarm doors and terminal boxes. Any variance between the reports were validated with hard copy files and VBN history reports. No discrepancies were discovered.

There was no safety significance associated with this event. The Licensee investigation concluded that unauthorized entry into the Protected Area did not occur during this event.