



Entergy Operations, Inc.
17265 River Road
Killona, LA 70066
Tel 504 739 6379

Everett P. Perkins, Jr.
Director, Nuclear Safety Assurance
Waterford 3

W3F1-2000-0088
A4.05
PR

July 7, 2000

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

Subject: Waterford 3 SES
Docket No. 50-382
License No. NPF-38
Reporting of Security Incident Report

Gentlemen:

Attached is Security Incident Report (SIR) 00-S03-00 for Waterford Steam Electric Station Unit 3. This report provides details of a safeguard system vulnerability related to the security computer software function for upgrading access to vital areas for Emergency Response Organization personnel during emergencies. This condition is being reported pursuant to 10CFR73.71, Appendix G (I)(c) as a vulnerability in our system that could have allowed unauthorized or undetected access to vital areas for which compensatory measures were not employed. All of the commitments contained in this submittal are identified on the attached Commitment Identification/Voluntary Enhancement Form.

Very truly yours,

E.P. Perkins, Jr.
Director,
Nuclear Safety Assurance

EPP/LBB/rtk
Attachment 1

Commitment Identification/Voluntary Enhancement Form

IE74

Reporting of Security Incident Report
W3F1-2000-0088
Page 2
July 7, 2000

cc: E.W. Merschoff, (NRC Region IV)
N. Kalyanam, (NRC-NRR)
A.L. Garibaldi
P. Lewis - INPO Records Center
J. Smith
N.S. Reynolds
NRC Resident Inspectors Office
Louisiana DEQ/Surveillance Division

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 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. If an information collection does not display a currently valid OMB control number, the NRC may not conduct or sponsor, and a person is not required to respond to, the information collection.

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)
Waterford Steam Electric Station, Unit 3

DOCKET NUMBER (2)
05000-382

PAGE (3)
1 of 6

TITLE (4)
Safeguard System Vulnerability due to Security Computer Software Function for Upgrading Access

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
06	08	00	00	S03	00	07	07	00	N/A	N/A
									N/A	N/A

OPERATING MODE (9)	POWER LEVEL (10)	THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR § (Check one or more) (11)								
1	100	20.2201(b)	20.2203(a)(2)(v)	50.73(a)(2)(i)	50.73(a)(2)(viii)					
		20.2203(a)(2)(i)	20.2203(a)(3)(i)	50.73(a)(2)(ii)	50.73(a)(2)(x)					
		20.405(a)(1)(ii)	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 Lisa B. Borel, Sr. Licensing Engineer	TELEPHONE NUMBER (Include Area Code) (504) 739-6403
--	---

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 15 single-spaced typewritten lines) (16)

On June 8, 2000 it was discovered that an Emergency Mode software flag was incorrectly enabled in the Security System database, which allowed unfettered access to the Vital Area for multiple personnel. The software flag is associated with emergency responder plant access and should be disabled in non-emergency/non-drill conditions. On June 9, 2000 this was determined to be a vulnerability in a safeguard system that could allow unauthorized or undetected access to a vital area for which compensatory measures have not been employed and is being reported pursuant to 10CFR73, Appendix G, I(c). A one-hour notification was issued per the same requirement. The root cause was determined to be inadequate design verification and testing by the software vendor for this unique feature in their software system. The emergency responder software flags were reset and an investigation determined that no personnel received access to vital areas inappropriately. Compensatory measures were put in place to control access during drills and emergencies until long term corrective actions to remove this function from the computer system are completed. There is no safety significance associated with this event. This event had no adverse affects on the health and safety of the public and is not considered a Safety System Functional Failure (SSFF).

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET (2)	LER NUMBER (6)			PAGE (3)
Waterford Steam Electric Station, Unit 3	05000-382	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	2 OF 6
		00	S03	00	

TEXT (If more space is required, use additional copies of NRC Form 366A) (17)

REPORTABLE OCCURRENCE

On June 9, 2000, it was determined that Waterford 3 contained a vulnerability in a safeguard system that could allow unauthorized or undetected access to a vital area for which compensatory measures have not been employed. This is a violation of 10 CFR Part 73, Appendix G, Paragraph I(c). It was discovered that an Emergency Mode software flag was incorrectly enabled in the Security Computer database, which allowed unfettered access to the Vital Area for multiple personnel. The software flag is associated with emergency responder plant access and should be disabled in non-emergency/non-drill conditions. This provided an opportunity for personnel with only Protected Area access to gain access to the Vital Area via the emergency accountability process. This condition was present in both the primary and backup security computers. On June 9, 2000, a one-hour report of this event was issued per the same paragraph.

INITIAL CONDITIONS

At the time this condition was identified, Waterford 3 was operating in Mode 1 at approximately 100% power. No structures, systems or components were out of service that contributed to this event.

EVENT DESCRIPTION

On June 8, 2000 during an investigation of a tailgating event, it was discovered that an Emergency Mode software flag was incorrectly enabled in the Security Computer database, which allowed access to the Vital Area for multiple personnel. The software flag is associated with emergency responder plant access and should be disabled in non-emergency/non-drill conditions. A design feature of the security computer is that the Accountability Card Readers grant unfettered access to the Vital Area when in Emergency Mode. During times when the Accountability Card Readers are activated (Emergency Plan drills and actual events), the badges that are swiped at the Accountability Card Readers cause the Emergency Responder Access Flag to be set, allowing access to all areas (both Vital Area and Protected Area). During the security computer upgrade completed in December 1998,

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET (2)	LER NUMBER (6)			PAGE (3)
Waterford Steam Electric Station, Unit 3	05000-382	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	3 OF 6
		00	S03	00	

TEXT (If more space is required, use additional copies of NRC Form 366A) (17)

this emergency response access function was scoped into the Design Technical Specification for the software program for the purpose of providing Entergy with an effective way of handling the function of upgrading access to vital areas during emergencies without requiring significant manual input from Security. Historically, Waterford 3 had multiple access levels (>50), resulting in a lengthy process to manually change access levels during emergencies. Since the accountability card readers are activated during drills, the upgrade in access levels functioned during drills as well as during actual emergencies. This feature is unique to Waterford 3 only from the aspect that the computer performs this emergency response function – the security computer system vendor has not installed this feature at other sites. This emergency function was first activated for a drill on December 8, 1998. The Emergency Responder Access Flag is set in both the primary and backup security computers when Emergency Mode is entered. On exit from Emergency Mode, the flag is cleared only in the primary computer and remains active on the backup computer. This includes periods during which system transfer establishes the backup computer as the primary (active) system. At the time of discovery, the Emergency Responder Access Flag was found to be active on both the primary and backup computers for multiple personnel. It is believed that the access flags on the primary computer were enabled when on April 24, 2000, the primary computer stalled and did not automatically transfer to the backup. This required a manual transfer which causes a database synchronization between the primary and backup computers. This database synchronization caused the access flags in the primary computer to also be enabled. The Accountability Card Reader located in the Maintenance Support Building is capable of granting unfettered access to the Vital Area to personnel who are normally only authorized access to the Protected Area. Note that the only Accountability Card Reader not in a Vital Area is the one located in the Maintenance Support Building. This creates the potential of granting unfettered Vital Area access to personnel not associated with the Emergency Response Organization and to personnel associated with the Emergency Response Organization who normally have only Protected Area access, and having that access remain after securing from the drill or actual event. Upon discovery of the emergency access flags on both the primary and backup computers being enabled, they were

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Waterford Steam Electric Station, Unit 3	05000-382	00	S03	00	4 OF 6

TEXT (If more space is required, use additional copies of NRC Form 366A) (17)

immediately reset back to normal (i.e. disabled). The personnel whose flags had been enabled were investigated. It was determined that in no case was an employee granted Vital Area access that did not already have Vital Area access granted through normal procedures.

CAUSAL FACTORS

The causal factors associated with this event include the following:

Manufacturer Fabrication/Construction Less Than Adequate – The software vendor (Harmon Control and Information Systems, Inc.) designed the software such that it set the Emergency Responder Access Flag on both computers but failed to reset the flag on the backup computer. The vendor’s testing of the computer code for the Emergency Responder Access Flag function was not adequately design verified or tested. Because the standard software system functionality is common to other nuclear plants, and the backup computer mirrors the primary, a full check of backup computer functions was not done during the software acceptance testing. The Emergency Responder Access Flag is the single unique software function not provided by the computer vendor to other sites, and not mirrored on the backup computer.

Inadequate Review of Design Change – The emergency responder flag function of the software system was not reviewed to determine the testing requirements for this added function to the vendor’s standard software. No corrective action is deemed necessary for this causal factor. Entergy implemented changes to the design process subsequent to this design change which adequately address the concern.

Control/Display Needed but Absent – The status of the Emergency Responder Access Flag is not available on any operator display and cannot be evaluated by Security personnel. The flag status can only be determined using software development tools. This limited Security’s ability to detect the failure to re-set the flags on the backup computer.

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET (2)	LER NUMBER (6)			PAGE (3)
Waterford Steam Electric Station, Unit 3	05000-382	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	5 OF 6
		00	S03	00	

TEXT (If more space is required, use additional copies of NRC Form 366A) (17)

CORRECTIVE ACTIONS

1. The emergency responder software flags on the primary and backup security computer were reset to the non-Emergency Mode.
2. The personnel whose emergency responder flags were set were investigated. It was determined that in no case was any employee granted Vital Area access who did not normally have Vital Area access.
3. A software change was implemented that allows the CAS/SAS Operators to generate a report listing all personnel with an active Emergency Responder Access Flag.
4. The software vendor was notified of the problem so that they may investigate their software modification process.
5. The software functions of Accountability and Emergency Responder Access Flags will be split apart to enable Accountability without enabling Emergency Responder Access for use during drills. The Emergency Responder Access Flag function was brought about due to the large number of access levels at Waterford 3. Due to a reduction of the number of Access Levels, the Emergency Responder Access Flag function will no longer be required and will be removed from the system. Compensatory measures have been put in place until this permanent corrective action is implemented.
6. The emergency responder access upgrade function of the security computer system software will be temporarily disabled prior to any scheduled emergency drills that may occur before permanent removal of the function from the system.
7. Other enhancements for emergency responder access are being implemented in accordance with the corrective action process.

SAFETY SIGNIFICANCE

The current system design provides the opportunity for personnel with only Protected Area access to gain access to Vital Areas via the emergency response accountability process. Investigation of historical data showed no personnel accessed either the Central Alarm Station or the Control Room

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Waterford Steam Electric Station, Unit 3	05000-382	00	S03	00	6 OF 6

TEXT (If more space is required, use additional copies of NRC Form 366A) (17)

solely due to receiving emergency responder upgraded access. No personnel with protected area only access acquired emergency responder upgraded access via the accountability card readers. Therefore, personnel with only protected area access did not receive access to vital areas inappropriately. This event is not considered a Safety System Functional Failure (SSFF).

SIMILAR EVENTS

A review of Security Incident Reports dating back to 1994 was performed. No previous similar events involving access to vital areas were identified.

ADDITIONAL INFORMATION

Energy Industry Identification System (EIIS) codes are identified in the text within brackets [].

COMMITMENT IDENTIFICATION/VOLUNTARY ENHANCEMENT FORM

Attachment 1 to W3F1-2000-0088
 Security Incident Report 00-S03-00
 July 7, 2000
 Page 1 of 1.

COMMITMENT(S)	ONE-TIME ACTION*	CONTINUING COMPLIANCE*	SCHEDULED COMPLETION DATE (IF REQUIRED)	ASSOCIATED CR OR ER
The security computer software functions of Accountability and Emergency Responder Access Flags will be split and the Emergency Responder Access Flag function will be removed from the system.	X			CR-WF3-2000-0595
A software option was provided to the CAS/SAS Operators to generate a report listing all personnel with an active Emergency Responder Access Flag.		X (until such time as the function is removed from the system)		CR-WF3-2000-0595
The emergency responder access upgrade function of the security computer system software will be temporarily disabled prior to any scheduled emergency drills that may occur before permanent removal of the function from the system.		X (until such time as the function is removed from the system)		CR-WF3-2000-0595