



Entergy Operations, Inc.  
P.O. Box 756  
Port Gibson, MS 39150  
Tel 601 437 2800

August 3, 2001

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

Subject: Response to NRC Request for Additional Information for Exemption  
to 10CFR50.71(e)(1) – UFSAR on World Wide Web  
Grand Gulf Nuclear Station  
Docket No. 50-416  
License No. NPF-29

Reference: GNRO-2000/0086 Letter from Grand Gulf to NRC – Request  
for Exemption to 10CFR50.71(e)(1) UFSAR Update By Use of  
a Utility Maintained Website for UFSAR Access

GNRO-2001/00055

Ladies & Gentlemen:

This letter is a response to a request for additional information sent via a NRC letter dated May 30, 2001 in regard to an exemption to 10CFR50.71(e). The attachment provides our responses to the NRC questions. If you have any a questions in regard to our exemption or these questions please contact Michael Larson at 601-437-6685. This letter does not contain any commitments.

Yours truly,

A handwritten signature in black ink, appearing to be "CAB".

CAB/MJL

attachment: 1. Response to RAI questions

cc: (See Next Page)

August 3, 2001  
GNRO-2001/00055  
Page 2 of 2

cc:

Hoeg	T. L.	(GGNS Senior Resident)	(w/a)
Levanway	D. E.	(Wise Carter)	(w/a)
Reynolds	N. S.		(w/a)
Smith	L. J.	(Wise Carter)	(w/a)
Thomas	H. L.		(w/o)

Mr. E. W. Merschoff (w/2) Regional Administrator U.S. Nuclear Regulatory Commission Region IV 611 Ryan Plaza Drive, Suite 400 Arlington, TX 76011	ALL LETTERS
Mr. S. P. Sekerak, NRR/DLPM/PD IV-1 (w/2) <b>ATTN: ADDRESSEE ONLY</b> U.S. Nuclear Regulatory Commission One White Flint North, Mail Stop O7-D1 11555 Rockville Pike Rockville, MD 20852-2378	ALL LETTERS

	<b>NRC QUESTIONS</b>	<b>GGNS RESPONSE</b>
1.	<p>The licensee should address plans for distribution of back up Compact Disk Read-only Memories (CD-ROMs) to the U. S. Nuclear Regulatory Commission (NRC) staff. Should the UFSAR website fail during a plant incident, what provisions can be made for rapid distribution of the back-up CD-ROMs to the NRC and plant staffs?</p>	<p>Should the website fail, we propose to have a second website available that could be quickly setup and loaded with our UFSAR. This site would then be made available. This could be accomplished prior to the need to send CD-ROMs and would decrease the amount of time the personnel would not have access to our UFSAR. Currently, the following NRC personnel are on controlled copy distribution of our UFSAR CD-ROM:</p> <ul style="list-style-type: none"> <li>• Project Manager in Rockville, MD</li> <li>• Senior Resident at the site.</li> <li>• Project Engineer - Region IV in Arlington, TX</li> </ul>
2.	<p>How will the UFSAR website be protected from attempted and successful unauthorized entry? Can such attempted and successful unauthorized entries be reliably detected? What remedial action would be taken, and how soon, should a successful unauthorized entry be detected? Please address normal and exigent circumstances.</p>	<p>The web site is open for public viewing of the content. However, it has a comprehensive set of authoring controls, which means that only a specific set of people can write or update the site. Entergy also uses Internet Security Systems' RealSecure™ application. This automated real-time intrusion protection system monitors network traffic for attacks and other security-related events. Attack recognition, incident response, and intrusion prevention occurs immediately through the use of attack signatures and customized responses. Unauthorized attempts to "write" to the site will simply be denied. In the event of a successful unauthorized entry under either normal or exigent circumstances, information technology incident report procedures will be followed immediately following detection.</p>
3.	<p>The licensee should propose reporting requirements concerning unauthorized entry (e.g., report within 30 days in the event of a successful unauthorized entry, and annually on all attempted and successful unauthorized entries). Alternately, the licensee may commit to using their corrective action program to resolve problems associated with attempted and successful unauthorized entry.</p>	<p>A new reporting requirement would increase burden without commensurate safety improvement. "Hacking" of low profile sites does not appear to be a significant problem that would require development of criteria for detection and reporting. Website availability problems of any nature would be corrected on a case-by-case basis in a reasonable time frame. Should significant issues arise with website availability, a corrective action process would be used to address the issue.</p>

	<b>NRC QUESTIONS</b>	<b>GGNS RESPONSE</b>
4.	How can changes to the UFSAR be observed (e.g., change pages)?	Changes to the UFSAR will still be made in accordance with 10CFR50.71(e)(5) – “Each replacement page shall include both a change indicator for the area changed, e.g., a bold line vertically drawn in the margin adjacent to the portion actually changed, and a page change identification (date of change or change number or both).” Other methods to indicate change such as underlining or different color fonts could also be used to indicate changes.
5.	Are there any meaningful statistics, thus far, concerning the UFSAR website availability? What is the licensee’s expectation, when the website is mature, concerning availability?	No formal statistics have been collected to date. Availability will be as close to 24 hours a day, seven days a week as reasonably possible.