



HITACHI

GE Hitachi Nuclear Energy

James C. Kinsey
Vice President, ESBWR Licensing

PO Box 780 M/C A-55
Wilmington, NC 28402-0780
USA

T 910 675 5057
F 910 362 5057
jim.kinsey@ge.com

Proprietary Notice

This letter forwards proprietary information in accordance with 10CFR2.390. Upon the removal of Enclosure 1, the balance of this letter may be considered non-proprietary.

MFN 08-169

Docket No. 52-010

March 13, 2008

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555-0001

Subject: **Response to Portion of NRC Request for Additional Information Letter No. 143 Related to ESBWR Design Certification Application – RAI Numbers 7.1-80, 7.1-81, 7.1-82, 7.1-83, 7.1-84, and 7.1-85**

Enclosure 1 contains GEH's response to the subject NRC RAIs transmitted via the Reference 1 letter.

Enclosure 1 contains GEH proprietary information. GEH customarily maintains this information in confidence and withholds it from public disclosure. A non-proprietary version is provided in Enclosure 2.

The affidavit contained in Enclosure 3 identifies that the information contained in Enclosure 1 has been handled and classified as proprietary to GEH. GEH hereby requests that the information of Enclosure 1 be withheld from public disclosure in accordance with the provisions of 10 CFR 2.390 and 9.17.

If you have any questions or require additional information, please contact me.

Sincerely,

James C. Kinsey
Vice President, ESBWR Licensing

D068
NRO

Reference:

1. MFN 08-097, Letter from U.S. Nuclear Regulatory Commission to Robert E. Brown, *Request for Additional Information Letter No. 143 Related To ESBWR Design Certification Application*, January 31, 2008

Enclosures:

1. MFN 08-169 - Enclosure 1 - Response to Portion of NRC Request for Additional Information Letter No. 143 Related to ESBWR Design Certification Application – RAI Numbers 7.1-80, 7.1-81, 7.1-82, 7.1-83, 7.1-84, and 7.1-85 - GEH Proprietary Information
2. MFN 08-169 - Enclosure 2 - Response to Portion of NRC Request for Additional Information Letter No. 143 Related to ESBWR Design Certification Application – RAI Numbers 7.1-80, 7.1-81, 7.1-82, 7.1-83, 7.1-84, and 7.1-85 Non-Proprietary Version
3. Affidavit – David H. Hinds, dated March 13, 2008

cc:	AE Cubbage	USNRC (with enclosures)
	RE Brown	GEH/Wilmington (with enclosures)
	GB Stramback	GEH/San Jose (with enclosures)
	DH Hinds	GEH/Wilmington (with enclosures)
	eDRF Sections	0000-0081-3958 RAI 7.1-80
		0000-0081-3960 RAI 7.1-81
		0000-0081-3962 RAI 7.1-82
		0000-0081-3964 RAI 7.1-83
		0000-0081-3967 RAI 7.1-84
		0000-0081-3969 RAI 7.1-85

MFN 08-169

Enclosure 2

**Response to Portion of NRC Request for Additional
Information Letter No. 143 Related to ESBWR Design
Certification Application – RAI Numbers 7.1-80, 7.1-81,
7.1-82, 7.1-83, 7.1-84, and 7.1-85**

Non-Proprietary Version

NRC RAI 7.1-80:

NEDE-33295P, Appendix B, "Cyber Security Plan Conformance Review," Item 1 states that "this document conforms to the NRC ISG on communications, DI&CISG- 04, 9/28/2007" instead of RG 1.152, Section 2.1. RG 1.152, Section 2.1 addresses the following: "Remote access to the safety system should not be implemented. Computer-based systems may transfer data to other systems through one-way communication pathways." DI&C-ISG-04 issued on September 28, 2007 does not specify any guidance on remote access. Please verify that GEH intends to comply with RG 1.152 with respect to the remote access requirements. Specifically, verify that there will be no remote access to any safety systems and discuss how this is achieved.

GEH Response

The ESBWR Cyber Security Program Plan Licensing Topical Report (LTR) NEDE-33295P complies with RG 1.152 and the clarifying statements in DI&C-ISG-04, Section 1.

"Remote Access" is clarified in the NEDE-33295P, Appendix A – Definitions, change provided below as: "Communication with assets that are outside the perimeter of the Security Level being addressed."

II

]]

DCD / Licensing Topical Report Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33295P, Rev 0 will be revised as noted below:

The revised Section 2.2.1 in Cyber Security LTR (NEDE-33295P), Revision 1, will read as follows:

2.2.1 Regulatory Guide and Interim Staff Guidance

3. Regulatory Guide (RG) 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 2006.
4. Interim Staff Guidance, Revision 0, Digital Instrumentation and Controls, DI&C ISG-04, "Task Working Group #4: Section 1, "Highly-Integrated Control Rooms-Communications Issues (HICRc)," September 2007.

The revised Section 3.3 (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

The revised Section 4.1.2 in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

4.1.2 Communication Pathways

[[

]]

The revised Section 4.1.2.4 (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

4.1.2.4 [[

]]

The revised Appendix A (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

NEDE-33295-P Portion of Appendix A - Definitions

Term	Definition
Remote Access	Communication with assets that are outside the perimeter of the <u>Security Level</u> security zone being addressed

The revised **Appendix B** in **Cyber Security LTR (NEDE-33295), Revision 1**, will read as follows:

[[

NRC RAI 7.1-81

Regulatory Guide 1.152 states that the design configuration items incorporating pre-developed software into the safety system should address security vulnerabilities of the safety system. Please verify that Section 6, "Design Phase" addresses this criterion and discuss how this is achieved.

GEH Response

Regulatory Guide (RG) 1.152, Section C.2.2.1 requires, in part, that requirements specifying the use of pre-developed software and systems (e.g., reuse software and commercial off-the-shelf systems) should address the vulnerability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

RG 1.152, Section C.2.3.1 requires, in part, that design configuration items incorporating pre-developed software (PDS) into the safety system addresses security vulnerabilities of the safety system.

The following references currently demonstrate compliance of the GEH ESBWR Cyber Security Program and Software Development Program with the regulatory requirements mentioned above:

- GEH Licensing Report (LTR) NEDE-33295P, "*Cyber Security Program Plan*": Section 5, *Requirements Phase* addresses GEH's commitment to comply with RG 1.152, Sections C.2.2.1 and C.2.3.1. This applies to both GEH and sub-vendors through the Purchase Order process, as directed by NEDE-33226P, *ESBWR I&C Software Management Plan (SMP)* and NEDE-33245P, *ESBWR I&C Software Quality Assurance Plan (SQAP)*.
- GEH Licensing Report (LTR) NEDE-33295P, "*Cyber Security Program Plan*": Section 5.6, *Software* addresses that software developed for PDS on safety-related applications includes cyber security protection, per RG 1.152, Section C.2.2.1.
- GEH Licensing Report (LTR) NEDE-33245P, "*ESBWR – I&C Software Quality Assurance Plan (SQAP)*": Section 10.7.1, *Software Developed by Vendors for the Project* addresses the vendor's responsibilities to support the design and development of the software products.
- GEH Licensing Report (LTR) NEDE-33226P, "*ESBWR – I&C Software Management Plan (SMP)*": Section 5.7.5, *Application of Previously Developed Software* requires that a PDS evaluation report be produced at the Requirement Phase. The PDS evaluation at this phase shall either

conclude that the PDS is suitable for use as is or shall identify specific actions that must be performed before the PDS may be used in the application. Specific evaluation criteria and directions are also addressed in this section of the SMP.

In support of the above-mentioned justification for compliance with RG 1.152, Sections C.2.2.1 and C.2.3.1 - Section 4, *Planning Phase* of the Cyber Security LTR (NEDE-33295P) describes the Vulnerability Review and the Risk Assessment processes. These processes cover all pre-developed software applied in safety systems. The following references from Section 4 of the Cyber Security LTR (NEDE-33295P) supplement the criteria in the SMP (NEDE-33226P), Section 5.7.5, so that identified potential vulnerabilities in PDS are addressed:

- Section 4.1.1 addresses risk management of each Critical Digital Asset (CDA).
- Section 4.1.2.4 addresses engineering analysis required for Security Level 3/Security Level 4 to map out remote connections, including identification of the risk reduction techniques to be applied and mitigation strategies for system connections where vulnerabilities are identified.
- Section 4.3 describes conceptual risk assessment for each system.

Assessment of safety requirements for PDS that are used in Q-class software will be performed using the requirements described in Section 5.7.5 of the SMP (NEDE-33226P). In the event assessment criteria are not met, PDS will be re-engineered as necessary.

Evaluation of Commercial-Off-the-Shelf (COTS) software will be performed using the requirement described in Section 5.7.6 of the SMP (NEDE-33226P).

In order to further clarify compliance with RG 1.152, Section C.2.3.1 – the following changes will be made in Sections 6 and 6.2.1 of the Cyber Security LTR (NEDE-33295P):

- Section 6. – A sentence or paragraph will be added to reinforce that other sections of the Cyber Security LTR will also commit to security assessment of PDS. This will match with the requirements of the SMP and the SQAP. (See markup below)
- Section 6.2.1 – This section will be revised to be consistent with the requirements of RG 1.152, Sections C.2.2.1 and C.2.3.1. (See markup below)

DCD / Licensing Topical Report Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33295P, Rev 0 will be revised as noted in the markup below:

The revised Section 6 in Cyber Security LTR (NEDE-33295P), Revision 1, will read as follows:

6. DESIGN PHASE

This section describes the creation of the system based on the requirements. The design phase incorporates the objectives of the ESBWR as a whole and on the individual system security level. The requirements will be translated into specific design criteria.

[[

]]

The revised Section 6.2.1 in Cyber Security LTR (NEDE-33295P), Revision 1, will read as follows:

6.2.1 Interfaces

The interface of each Critical Digital Asset is the entry point for external command and control of that system. [[

]]

NRC RAI 7.1-82

Regulatory Guide 1.152 specifies that the development process should ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications. Please indicate how Section 5, "Requirements Phase" of this GEH Cyber Security Program Plan intends to meet this criterion. In addition, provide specific information on the process that will be applied to pre-developed software to confirm it meets this criterion.

GEH Response

Regulatory Guide (RG) 1.152, Section C.2.2.1 indicates that cyber security requirements should be part of the overall system requirements, including commercial-off-the-shelf (COTS) and pre-developed software (PDS) and systems. With regard to ESBWR, this requirement applies to hardware, firmware, and software.

RG 1.152, Section C.2.2.2 requires that the development process should ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications.

In compliance with RG 1.152, Section C.2.2.1, GEH Licensing Report (LTR) NEDE-33295P, "*Cyber Security Program Plan*": Section 5, *Requirements Phase* indicates that requirements will be developed for hardware and software, in accordance with Section 5.7.7 of GEH Licensing Report (LTR) NEDE-33226P, "*ESBWR – I&C Software Management Plan (SMP)*."

Section 5.7.7 of SMP describes the *Hardware/Software Specifications (HSS)*. The HSS documents the high level, system specific requirements for the software-based product. The software development process described in the SMP requires that the software is forward and backward traceable from the top level requirements, including cyber security requirements, to the implementation. According to SMP, Section 5.7.8 - the software requirements shall be traceable to the HSS.

Also, Section 5.7.5 of SMP requires that a PDS evaluation report be produced at the requirements phase. The Cyber Security LTR in Section 5 requires a review of PDS against cyber security requirements. At the requirement phase of the software development life-cycle, the PDS evaluation should establish the extent to which cyber security has been considered in the development of the PDS, and, as necessary, document any additional requirements that the PDS design must be evaluated against in the design phase of the software development life-cycle before the PDS may be used in the application. Since it is not explicitly stated in the SMP that a cyber security review of PDS is required to be in the

PDS evaluation report, Section 5 of the Cyber Security LTR (NEDE-33295P) will be revised so that a cyber security review is performed. Because of information security concerns, the results of the cyber security review will be handled and stored separately from the PDS report. The new statement, which will be added in Section 5 of the Cyber Security LTR (NEDE-33295P) should read as follows:

[[

]]

Also, in support of the above-mentioned justification for compliance with RG 1.152, Sections C.2.2.1 and C.2.3.1 - Section 4, *Planning Phase* of the Cyber Security LTR (NEDE-33295P) describes the Vulnerability Review and the Risk Assessment processes. These processes cover all pre-developed software applied to safety systems. The following references from Section 4 of the Cyber Security LTR (NEDE-33295P) supplement the criteria in the SMP (NEDE-33226P), Section 5.7.5, so that identified potential vulnerabilities in PDS are addressed:

- Section 4.1.1 addresses risk management of each Critical Digital Asset (CDA).
- Section 4.1.2.4 addresses engineering analysis required for Security Level 3/Security Level 4 to map out remote connections, including identification of the risk reduction techniques to be applied and mitigation strategies for system connections where vulnerabilities are identified.
- Section 4.3 describes conceptual risk assessment for each system.

Assessment of safety requirements for PDS that are used in Q-class software will be performed using the requirements described in Section 5.7.5 of the SMP (NEDE-33226P). In the event assessment criteria are not met, PDS will be re-engineered as necessary.

In compliance with RG 1.152, Section C.2.2.2 a new paragraph must be added at the beginning of Section 5.6 of the Cyber Security LTR (NEDE-33295P). The new paragraph should read as follows (see markup below):

[[

]]

DCD / Licensing Topical Report Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33295P, Rev 0 will be revised as noted in the markup below:

The revised Section 5.0 in Cyber Security LTR (NEDE-33295P), Revision 1, will read as follows:

5. REQUIREMENTS PHASE (*Only an excerpt of 2nd paragraph shown*)

[[

]]

The revised Section 5.6 in Cyber Security LTR (NEDE-33295P), Revision 1, will read as follows:

5.6 Software

The use of commercial-off-the-shelf (COTS) software and pre-developed software (PDS) will be a very common solution for vendor and partners. [[

]]

NRC RAI 7.1-83

Please indicate how the outputs from activities conducted based on requirements from Section 7, "Implementation Phase" of the GEH Cyber Security Program Plan will be documented. For example, indicate which report(s) will address the requirement, "the developer shall follow the GEH Policy and Procedures addressing security controls on development processes, including scanning, where appropriate, during and after code development, to address undocumented codes or malicious functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave beyond the system requirements. This development process will account for hidden functions and vulnerable features embedded in the code, and their purpose and impact on the safety system. As a design goal, these functions should be disabled, removed, or addressed to prevent any unauthorized access." In addition, describe which GEH documented Policies and Procedures (SQAP, SMP, EOPs, etc.) will be followed to meet this requirement.

GEH Response

Reg. Guide 1.152 Section C.2.2.1 states the following:

"The security requirements should be part of the overall system requirements."

First, the requirements provide input to the "Implementation Phase" following NEDE-33295P Section 5.1 as follows:

[[

]]

The outputs of the "Implementation Phase" described in Section 7 of NEDE-33295P, are documented in a set of reports required by the SMP, SQAP and Cyber Security Program Plan, for safety-related software development, including the following:

NEDE-33245P, "ESBWR – I&C Software Quality Assurance Plan (SQAP), Section 9.3.4, Software Safety Code Analysis, which requires that an updated Criticality Analysis Report and updated Hazard Analysis Report be issued. For example, in the Criticality Analysis Report update, Section 9.3.4.1 of this LTR

documents that criticality analysis shall be performed on the Software Class Q and N3 source code to verify that no inconsistent or unintended functions are introduced during software coding.

NEDE-33245P, "ESBWR – I&C Software Quality Assurance Plan (SQAP), Section 9.3.5, Software Safety Test Analysis, which requires that the hazard analysis portion and output in the updated Hazard Analysis Report shall include review of unintended functions such as unpredictable responses, development aids not removed, and defects due to design errors.

NEDE-33226P, "ESBWR I&C Software Management Plan," Section 5.9 and Table 5.9-1 provide the Implementation Phase Output Documents including the Software Functional Test Report as well as the Implementation Phase Requirements Traceability Matrix, which document compliance with the software requirements.

Various cyber security output reports as noted in Section 5.5 and 5.7 of NEDE-33295P, which document compliance with cyber security requirements.

The primary GEH documents required to comply with Reg. Guide 1.152 in the "Implementation Phase" are the SMP, SQAP and the Cyber Security Program Plan (NEDE-33295P), as well as implementing procedures (Engineering Operating Procedures, etc) and reports described above and documented in NEDE-33295P Section 7.3, "Cyber Security Plan Coordination with SMP and SQAP." The implementing procedures will comply with all of the commitments documented in LTR NEDE-33295P.

DCD / Licensing Topical Report Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33295P, Rev 0 will be revised as noted in the markup below:

The revised Section 1.7.1 (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

1.7.1 GEH ESBWR Licensing Position

[[

]]

The revised Section 3 and 3.1 in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

3. PROGRAM MANAGEMENT

This section describes the management components needed to lay the foundations for an effective cyber security program, including the specific roles and responsibilities assigned to carry out the program. Cyber security program management ensures that all necessary cyber security issues are addressed programmatically within the GEH ESBWR Cyber Security Policy and Procedures to achieve a reasonable level of risk at each ESBWR site. It allows the licensee to incorporate components of the utility corporate security program within a current site framework of policies, programs, practices and procedures.

3.1 Roles and Responsibilities

In accordance with NEI 04-04, Section 4.1 [2.2.4 (1)], and the associated NRC documents, GE-Hitachi Nuclear Energy (GEH) commits to a cyber security program with the following explicit roles and responsibilities for assigned program management, within the GEH scope of supply:

[[

]]

[[

]]

The revised Section 3.2 (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

The revised Section 5.3 (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

The revised Section 6.1 in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

6.1 Design of Physical and Logical Access

The analysis has been completed and the list of Critical Digital Assets has been made in the planning and requirements phases. [[

]]

The revised Section 7 in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

7. IMPLEMENTATION PHASE

This section is focused on implementation of the secure design for creation of secure hardware and software. [[

]]

7.1 Code Design

The planning phase, the requirements phase and the design phase have led to this step. [[

]]

The revised Section 9 in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

The revised Section 10.3 in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

The revised Section 13(Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

NRC RAI 7.1-84

Please describe the specific GEH Policies and Procedures that will provide additional guidance on specific actions applicable to GEH during the Installation, Checkout, and Acceptance Testing phase as indicated in Section 9 of GEH Cyber Security Program Plan.

GEH Response

Regulatory Guide (RG) 1.152, Section C.2.6.2 requires, in part, that a Cyber Security Program be in place covering policies, standards, and procedures, to ensure that installation of the digital system will not compromise the security of the digital system, other systems, or the plant.

Cyber Security LTR (NEDE-33295P), Chapter 9, *Installation, Checkout and Acceptance Testing Phase* commits to the development of ESBWR Cyber Security Policy and Procedures, or equivalent, that provides specific details meeting the guidelines of RG 1.152 and the objectives of the Cyber Security LTR.

[[

]]

The SMP activities provide the details needed to meet the requirements of RG 1.152, Section C.2.6.2.

However, a couple of changes to the Cyber Security LTR (NEDE-33295P) shall be made: (a) the heading of Section 9 shall be changed to "*Installation Phase*" to be consistent with the SMP, and (b) the textual content of Section 9 shall be revised to add information describing the specific ESBWR Cyber Security Policies and Procedures to provide additional guidance on specific actions applicable to GEH during the Installation Phase. All changes to the LTR are provided below.

Cyber Security LTR (NEDE-33295P), Section 7.3, *Cyber Security Plan Coordination with SMP and SQAP* describes the process of integrating the SMP, Software Quality Assurance Program Manual (SQAP), and Cyber Security LTR.

DCD / Licensing Topical Report Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33295P, Rev 0 will be revised as noted in the markup below:

The revised Section 9 in Cyber Security LTR (NEDE-33295P), Revision 1, will read as follows:

9. INSTALLATION, ~~CHECKOUT AND ACCEPTANCE TESTING~~ PHASE

[[

o

]]

NRC RAI 7.1-85

Please provide additional details on how the Cyber Security Program Plan is related to the SMP and SQAP documents with regards to software development. Will there be one master Cyber Security Program Plan for the whole system, or will there be separate application specific components referenced back to the overall plan? Alternately will any application specific information be included in the specific detailed software development plans (i.e. SMP, SQAP, etc.)

GEH Response

GEH NEDE-33295P, "Cyber Security Program Plan," Section 7.3 documents the following:

[[

]]

GEH recognizes that the SMP and SQAP were issued prior to issuing the Cyber Security Program Plan. Therefore, Section 3.2 of NEDE-33295P included the following commitments from GEH. Note the correction to the first commitment as shown below:

[[

]]

[[

]]

This review will be completed and the results included in Revision 3 of the SMP/SQAP.

[[

]]

DCD / Licensing Topical Report Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33295P, Rev 0 will be revised as noted in the markup below:

The revised Section 3.2 (Excerpt only) in Cyber Security LTR (NEDE-33295), Revision 1, will read as follows:

[[

]]

MFN 08-169

Enclosure 3

Affidavit

GE Hitachi Nuclear Energy

AFFIDAVIT

I, **David H. Hinds**, state as follows:

- (1) I am the General Manager, New Units Engineering, GE Hitachi Nuclear Energy ("GEH") and have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.
- (2) The information sought to be withheld is contained in Enclosure 1 of GEH letter MFN 08-169, Mr. James C. Kinsey to U.S. Nuclear Regulatory Commission, "Response to Portion of NRC Request for Additional Information Letter No. 143 Related to ESBWR Design Certification Application – RAI Numbers 7.1-80, 7.1-81, 7.1-82, 7.1-83, 7.1-84, and 7.1-85," dated March 13, 2008. GEH Proprietary Information is identified in Enclosure 1, "Response to Portion of NRC Request for Additional Information Letter No. 143 Related to ESBWR Design Certification Application – RAI Numbers 7.1-80, 7.1-81, 7.1-82, 7.1-83, 7.1-84, and 7.1-85 – GEH Proprietary Information," in dark red font and a dashed underline inside double square brackets. [[This sentence is an example.⁽³⁾]] Figures and large equation objects are identified with double square brackets before, and after the object. In each case, the superscript notation ⁽³⁾ refers to paragraph (3) of this affidavit, which provides the basis of the proprietary determination. Specific information that is not so marked is not GEH proprietary. A non-proprietary version of this information is provided in Enclosure 2, "Response to Portion of NRC Request for Additional Information Letter No. 143 Related to ESBWR Design Certification Application – RAI Numbers 7.1-80, 7.1-81, 7.1-82, 7.1-83, 7.1-84, and 7.1-85 Non-Proprietary Version."
- (3) In making this application for withholding of proprietary information of which it is the owner, GEH relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.390(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).
- (4) Some examples of categories of information which fit into the definition of proprietary information are:
 - a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by GEH's competitors without license from GEH constitutes a competitive economic advantage over other companies;
 - b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

- c. Information which reveals aspects of past, present, or future GEH customer-funded development plans and programs, resulting in potential products to GEH;
- d. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a., and (4)b, above.

- (5) To address 10 CFR 2.390(b)(4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GEH, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GEH, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.
- (6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge, or subject to the terms under which it was licensed to GEH. Access to such documents within GEH is limited on a "need to know" basis.
- (7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GEH are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.
- (8) The information identified in paragraph (2), above, is classified as proprietary because it identifies the models and methodologies GEH will use in developing a Cyber Security program for the ESBWR.

The development of the models and methodologies along with their application is derived from the extensive experience database that constitutes a major GEH asset.

- (9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GEH's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GEH's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical

methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GEH.

The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GEH's competitive advantage will be lost if its competitors are able to use the results of the GEH experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GEH would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GEH of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 13th day of March 2008.



David H. Hinds
GE Hitachi Nuclear Energy