[BEFORE SENDING THIS FORM TO A SUPPLIER, GE-HITACHI LEAD TO COMPLETE ALL HIGHLIGHTED INSERTS (AREAS IN HIGHLIGHTED IN BLUE) AND REMOVE THIS AND ALL SUCH INSTRUCTIONS AND INSERTIONS, I.E., THIS FORM SHOULD BE "READY TO SIGN" WHEN SENT TO A SUPPLIER.]

This Master Services Agreement ("MSA" or "Agreement") is entered into as of [INSERT DATE] ("Effective Date") by and between **[GE-Hitachi Nuclear Energy Americas LLC][GE-Hitachi Nuclear Energy International LLC][GE-Hitachi Global Laser Enrichment LLC]** a limited liability company organized and existing in accordance with the laws of the State of Delaware with its principal place of business at 3901 Castle Hayne Road, Wilmington, North Carolina 28401 U.S.A.("Company")and [INSERT NAME] ("Supplier"), a [INSERT "CORPORATION" OR "PARTNERSHIP" OR OTHER BUSINESS TYPE] organized under the laws of the ["state" or "country"] of [INSERT STATE/COUNTRY] having its principal place of business at [INSERT ADDRESS] ("Supplier").

1. Engagement and Statements of Work.

1.1 Company engages Supplier to perform services such as [INSERT GENERAL DESCRIPTION SUCH AS "ENGINEERING SERVICES", "SOFTWARE DEVELOPMENT AND CONSULTING SERVICES", ETC.], which may include the provision of certain deliverables (collectively, the "Services") and which are further described in Company Purchase Order ("PO") and/or Statement of Work ("SOW") documents executed during the Term (defined below) of this Agreement by an authorized representative from each party.

1.2 Each SOW shall contain: (i) a detailed description of the Services to be performed, (ii) the amount, schedule and method of compensation to be paid to Supplier by Company; and (iii) the term of the SOW, if different from the term of this MSA. Each PO and/or SOW issued pursuant to this Agreement shall be deemed incorporated into and governed by the terms of this MSA, and the Supplier's provision of Services shall be governed by this MSA as supplemented by the terms of the applicable PO and/or SOW. Where the terms of a PO or SOW conflict with the terms of the MSA, which existed prior to such PO or SOW, the terms of the pre-existing MSA shall prevail, except to the extent that the PO or SOW expressly states that the MSA is to be overridden or modified. No Company financial obligation will arise without issuance of a PO.

1.3 Changes to a PO or SOW. Company may at any time, in writing, make reasonable changes in the work described in a PO or SOW. If any changes cause an increase or decrease in the cost of, or the time required for the performance of, any work under a PO or SOW, an equitable adjustment shall be made in Supplier's fee or delivery schedule, or both. Any Supplier claim for an adjustment must be asserted within ten (10) days of Supplier's receipt of the change notification, and must be approved in a written amendment ("Change Order").

1.4 Extension to Affiliates. Any Company "Affiliate" may issue a PO or SOW under this MSA. An "Affiliate" with respect to either party shall mean any entity, including without limitation, any individual, corporation, company, partnership, limited liability company or group, that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with such party. In the event that any Company Affiliate issues any PO or SOW pursuant to this Agreement, such PO or SOW: (i) shall incorporate by reference the terms of this Agreement; (ii) shall be deemed a separate contract between the parties who sign it; and (iii) is an independent contractual obligation from any other PO or SOW. The term "Company" as used in this Agreement shall, for the purposes of any PO or SOW, issued by a Company Affiliate hereunder, be deemed to include only the Company Affiliate issuing such PO or SOW. The parties expressly agree that COMPANY SHALL HAVE NO LIABILITY NOR SHALL COMPANY INCUR ANY OBLIGATION OR BE RESPONSIBLE FOR THE FAILURE OF ANY COMPANY AFFILIATE TO PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT OR ANY PO OR SOW PLACED HEREUNDER.

2. Term. The term of this Agreement ("Term") shall begin on the "Effective Date" and end on [INSERT DATE; NORMALLY NOT LONGER THAN ONE YEAR FROM THE EFFECTIVE DATE] ("Expiration Date"), unless sooner terminated as provided below. If signed after the Effective Date, the MSA shall be deemed retroactive to the Effective Date. The parties further agree that if any PO or SOW is in effect at the time of the expiration of this Agreement, then as it applies to such PO or SOW only, the Term of this Agreement will be extended until the expiration or termination of such PO or SOW.

3. Supplier's Personnel.

3.1 All persons providing Services under this Agreement are collectively referred to herein as "Supplier's Personnel". If requested by Company, Supplier shall list the names of all Supplier's Personnel in **Schedule A**

hereto, indicating the relationship between Supplier and any person who is not Supplier's full-time employee. Without Company's prior written approval, Supplier shall not use any person to render Services who is not listed on **Schedule A** and/or who has been employed by Supplier less than six (6) months prior to the start date of such person's performance under this Agreement. Company shall have the right to approve each such Supplier's Personnel before assignment to any effort to be undertaken by Supplier, the granting of access to any Company facility and the disclosure of any Company information. All Supplier's Personnel participating in the furnishing of any Services shall sign a copy of **Schedule B** hereto, Secrecy and Inventions Agreement, which shall be forwarded to Company by Supplier to the address listed on such document.

3.2 Supplier shall, before engaging in work and after securing written authorization from all Supplier's Personnel, screen against the following lists: (a) U.S. Department of Commerce Denied Persons List, which can be located here: http://www.bis.doc.gov/dpl/thedeniallist.asp; (b) U.S. Department of Commerce Entity List, which can be located here: http://www.access.gpo.gov/bis/ear/txt/744spir.txt; (c) U.S. Department of Treasury Specially Designated Nationals and Blocked Persons List, which can be located here: http://www.treasury.gov/ofac/downloads/t11sdn.pdf; and (d) U.S. Department of State Debarment List, which can be located here: http://www.pmddtc.state.gov/compliance/debar.html. No person or entity on any of these lists may provide any Services to Company.

3.3 Supplier will also ensure compliance with the U.S. Immigration and Naturalization Service's I-9 process.

3.4 Security Sensitive Work. "Security Sensitive Work" means any of the Services that requires (i) unescorted access of Supplier Personnel to any Company location, facility, or worksite; (ii) deploying any Supplier Personnel to perform Services at any Company customer location, facility, or worksite; or (iii) granting access to Company networks (i.e., having a GE-issued single sign-on account) to Supplier Personnel. To the extent permissible by applicable law, prior to Supplier or Supplier's Personnel engaging in any Security Sensitive Work, Supplier shall, after securing written authorization from Supplier's Personnel and at Supplier's expense, perform background screening consistent with Company's "Requirements for Supplier Personnel Screening" attached hereto as **Schedule C**. This screening shall include the prior seven (7) year period covering all locations in which Supplier's Personnel resided and will verify employment details during this period. Supplier shall retain a copy of this screening report for Company's inspection for at least three (3) years following the performance of such Security Sensitive Work by Supplier's Personnel. Company reserves the right to determine, in its sole discretion, the type of work that will be designated as "security sensitive" under this Agreement.

3.5 Drug Use Policies. Unless conflicting with any applicable laws, Supplier shall, consistent with the requirements set out in Company's "Requirements for Supplier Personnel Screening" attached hereto as **Schedule C**, perform an initial drug screen prior to the commencement of the Services, if the Services require Supplier Personnel to engage in Security Sensitive Work. Supplier shall likewise require a drug screen at any time during the provision of the Services (i) if Company notifies Supplier that Company believes in good faith that Supplier's Personnel is under the influence of an illegal substance, (ii) as a consequence of an accident caused by or involving Supplier's Personnel during the performance of this Agreement and likely to have been related to Supplier Personnel's use of an illegal substance, or (iii) as mandated by applicable regulations in connection with the Service being provided. Any drug screen shall be performed by Supplier at Supplier's expense and Supplier shall address any positive results and handle accordingly. Supplier's Personnel will not be permitted to perform the Services if a positive result of said drug screen is determined

3.6 Personal Data received from Supplier. "Personal Data" for the purposes of this Agreement is any information relating to an identified or identifiable, natural person, including but not limited to any data relating to Supplier's Personnel, as well as Company's employees, officers, directors, shareholders, customers, prospects, contacts, suppliers or distributors. Some jurisdictions impose restrictions on the collection and use of such information. Supplier agrees that it will be responsible for complying with any applicable laws or regulations applying to Supplier's loading of Personal Data into any databases or tools of Company or its Affiliates (collective "Other Company Databases") and to any other disclosures of Personal Data by Supplier to Company. Supplier understands and agrees that Company may use this Personal Data for purposes reasonably related to the performance of this Agreement, including those identified in **Schedule D** of this Agreement. Supplier also understands and agrees that contact information for Supplier's Personnel may be transferred to and stored in other global databases located in the U.S. and maintained by Company or one of its Affiliates, and used for purposes reasonably related to this Agreement, including but not limited to supplier administration and payment administration. Personal Data relating to Supplier Personnel will not be shared beyond Company, its Affiliates and their contractors, who will be contractually bound to use the information only as reasonably necessary for the purposes of performing under their contractual obligations with Company and its Affiliates. Company will take appropriate measures to ensure that Personal Data relating to Supplier Personnel is stored securely and in conformity with applicable data protection laws. If any laws or regulations require that any of Supplier's Personnel

whose Personal Data is entered into Company databases receive notice of or consent to such processing of his/her Personal Data, then Supplier: (1) shall provide notice to and obtain consent from such Supplier's Personnel; and (2) upon Company's request, shall provide Company with a copy of such notice and consent to Company Representative's name set forth in Section 21 of the MSA. By way of example only, an Example Personal Data Notice and Consent Form is attached hereto as **Schedule D**.

4. Compensation and Payment Terms.

4.1 Unless expressly modified in a PO or SOW:

(a) Supplier shall be paid on a time and materials basis according to the Fee Schedule attached hereto as **Schedule A** or as provided in any applicable PO or SOW with expenses reimbursed in accordance with Company's travel policies. Supplier shall comply with the guidelines set forth in **Schedule E** attached hereto; provided, however, that in the event Company determines that additional, or different, guidelines should apply to a specific project for which the Services are being performed, Supplier shall comply with any such project specific guidelines. The foregoing will be the entire compensation to be paid to Supplier and will be in full discharge of any and all liability in contract or otherwise with respect to all Services rendered by the Supplier and Supplier Personnel.

(b) All fees will be paid in U.S. dollars and delivered to Supplier's principal place of business specified in the first paragraph of this Agreement.

(c) Supplier's price for the Services includes all sovereign, state and local sales, use, excise, privilege, payroll and/or occupational taxes, any value added tax that is not recoverable by Company and any other taxes, fees, and/or duties applicable to the goods and/or Services purchased under this Order. If Supplier is obligated by law to charge any value added and/or similar tax to Company, Supplier shall ensure that if such value added and/or similar tax is applicable, that it is invoiced to Company in accordance with applicable rules so as to allow Company to reclaim such value added and/or similar tax from the appropriate government authority. Neither party is responsible for taxes on the other party's income or the income of the other party's personnel or subcontractors. If Company is required by government regulation to withhold taxes for which Supplier is responsible, Company will deduct such withholding tax from payment to Supplier and provide to Supplier a valid tax receipt in Supplier's name. If Supplier is exempt from such withholding taxes as a result of a tax treaty or other regime, Supplier shall provide to Company a valid tax treaty residency certificate or other tax exemption certificate at a minimum of thirty (30) days prior to payment being due.

(d) All payments under this Agreement are net due one hundred and twenty (120) days from the Payment Start Date. The Payment Start Date is the later of the required date identified on the applicable PO, the received date of the Services in Company's receiving system or the date of receipt of valid invoice by Company. The received date of the Services in Company's receiving system will occur within forty-eight (48) hours of Company receiving confirmation that the Services have been provided in accordance with the applicable PO or SOW. Company shall be entitled to take an early payment discount of 0.0333% of the gross invoice price ("Daily Discount Rate") for each day before one hundred and twenty (120) days from the Payment Start Date that payment is made. For example, a discount of 3.5% would correspond to payment made one hundred and five (105) days early (i.e., fifteen (15) days after the Payment Start Date) and a discount of 0.333% would correspond to payment made ten (10) days early (i.e., one hundred and ten (110) days after the Payment Start Date). The Daily Discount Rate has been calculated based on a Prime Rate (defined below) of 4.50% ("Base Prime Rate"). If the Prime Rate in effect on the last business day of any month exceeds the Base Prime Rate, the Daily Discount rate will be adjusted on such date by 0.0007% for every twenty-five (25) basis points that the Prime Rate in effect on such date exceeds the Base Prime Rate; provided, however, that if the Prime Rate ever falls below the Base Prime Rate, then the Daily Base Discount Rate will remain 0.0333%. If the Daily Base Discount Rate is adjusted on the last business day of the month as set forth above, then such adjusted Daily Base Discount Rate will be applicable to all invoices posted for payment during the following month. For purposes of this Section, "Prime Rate" shall be the Prime Rate as published in the "Money Rates" section of *The Wall Street Journal* (or, in the event that such rate is not so published, as published in another nationally recognized publication) on the last business day of each month. For example, if the Prime Rate exceeds the Base Prime Rate by 0.25%, on the last day of the month, the Daily Base Discount Rate for the following month will increase by 0.0007%. Thus, a discount of 0.34% would correspond to payment made ten (10) days early (i.e., one hundred and ten (110) days from the Payment Start Date). If the date Company uses to calculate the early payment discount falls on a weekend or a holiday, payment to Supplier will be made on the next business day with the full discount taken as if the payment had been made to Supplier on such weekend or holiday date. Notwithstanding anything to the contrary in this Order, if Company elects to take the early payment discount to settle an invoice, Supplier acknowledges and confirms that: (1) title to the deliverables, goods and services shall pass directly to Company in accordance with the terms of this Order; (2) once title to the deliverables, goods and

services has passed to Company, Company shall immediately and directly transfer such title to Company; and (3) any and all of the obligations, including representations and warranties Supplier has provided with respect to the deliverables, goods and services, shall be retained by Company, and Company may rely upon the same. Supplier's invoice shall in all cases bear Company's PO number and shall be issued no later than one hundred twenty (120) days after completion of the Services. Company shall be entitled to reject Supplier's invoice if it fails to include the Company PO number, is issued after the date set forth above or is otherwise inaccurate, and any resulting delay in payment shall be Supplier's responsibility. Supplier warrants that it is authorized to receive payment in the currency stated in this Agreement or any applicable PO or SOW. No extra charges of any kind will be allowed unless specifically agreed in writing by Company. Supplier warrants the pricing for any deliverables, goods or services shall not exceed the pricing for the same or, comparable deliverables, goods or services offered by Supplier to third parties. Supplier shall promptly inform Company of any lower pricing levels for same or comparable deliverables, goods or services, and the parties shall promptly make the appropriate price adjustment.

[NOTE: INCLUDE PARAGRAPH 4.1.(E) BELOW ONLY IF THE PAY TERMS IN PARAGRAPH 4.1.(D) ARE NET DAYS, NO DISCOUNT. IF TERMS ARE TPS DISCOUNTED TERMS, THE MONTHLY PAY PARAGRAPH DOES NOT APPLY]

(e) Notwithstanding anything to the contrary which may be contained in this Agreement:

(1) in the event the payment date, as calculated pursuant to subsection (d) above, falls on a day that is within the period from the first day through the 15th day of the month, the payment date shall be the third calendar day of such month; or

(2) in the event the payment date, as calculated pursuant to subsection (d) above, falls on a day that is within the period from the 16th day of the month through the last day of the month, the payment date shall be the third calendar day of the immediately following month.

4.2 Upon termination as provided below, all fees shall be payable on a pro-rated daily basis up to the date of termination and no installments shall be payable thereafter.

4.3 When any applicable governmental law, rule or regulation makes any payment prohibited or improper or requires the payment of a reduced fee, the portion of the fee so affected shall not be paid or if paid shall be refunded to Company.

4.4 Company shall be entitled at all times to set off any amount owing at any time from Supplier to Company or its Affiliates in connection with this or any other agreement between Supplier and Company or its Affiliates.

4.5 During the Term and for three (3) years thereafter, Supplier shall, at Company's request and without any additional charge, provide full and complete access during normal business hours to the offices, books and records of Supplier and its accountants for purposes of auditing any performance (including without limit employee screening and environmental compliance), compensation or reimbursement issue under this Agreement.

5. Confidentiality.

5.1 Supplier and all Supplier Personnel shall maintain in confidence and safeguard all Proprietary Information. "Proprietary Information" means: information that is or has been disclosed to Supplier by Company or its Affiliates (defined in Section 1.4): (a) in writing or by email or other tangible electronic storage medium and is clearly marked "Confidential" or "Proprietary"; or (b) orally or visually, and then followed within thirty (30) working days thereafter with a summary or disclosure complying with the requirements of clause (a) above. Notwithstanding the foregoing, Proprietary Information also includes, without limitation: (i) commercially valuable information of Company and its Affiliates and their successors and assigns, the design and development of which required considerable amounts of time and money; (ii) any computer software product and related information (collectively "Software Product") developed by Company and its Affiliates and/or their successors and assigns and (c) any "Company Property" (defined in Section 6.2(a)).

5.2 Supplier recognizes and acknowledges the confidential and proprietary nature of any Proprietary Information and acknowledges the irreparable harm that could result to Company if it is disclosed to a third party or used for unauthorized purposes without Company's prior written consent. Therefore, Supplier agrees, except as required by law:

(a) to protect the confidentiality of Company's Proprietary Information (including any notes, summaries, reports, analyses or other material derived by Supplier or Supplier's Personnel in whole or in part from the Proprietary Information in whatever form maintained (collectively, "Notes"));

(b) to use the Proprietary Information and/or Notes only for the purposes of conducting business with Company in a manner contemplated by this Agreement; and

(c) to use the same degree of care as with its own confidential information, which shall be at least a reasonable standard of care, to prevent disclosure of the Proprietary Information and/or Notes, except to Supplier's Personnel to the extent necessary to permit them to perform the Services as set forth in this Agreement.

5.3 Supplier further agrees that prior to disclosing any Proprietary Information to Supplier's Personnel as set forth above, Supplier will: (a) advise such Supplier's Personnel of the confidential and proprietary nature of the Proprietary Information and Notes; and (b) require them to sign the Secrecy and Inventions Agreement attached hereto as **Schedule B**.

5.4 Supplier agrees to be responsible for any breach of this Agreement by it or Supplier's Personnel. Supplier acknowledges that money damages would not be a sufficient remedy for any breach of this Section. Accordingly, in the event of any such breach, in addition to any other remedies at law or in equity that Company may have, it shall be entitled to equitable relief, including injunctive relief or specific performance or both.

5.5 Obligations in this Section shall, with respect to each disclosure of Proprietary Information hereunder, continue for three (3) years from the date of each disclosure of Proprietary Information. Nothing herein is intended to limit or abridge the protection of trade secrets under applicable trade secrets law, and trade secrets shall be maintained as such until they fall into the public domain.

5.6 Upon completion or termination of this Agreement or upon request of Company, Supplier shall promptly: (a) return all Proprietary Information disclosed to it; and (b) destroy (with such destruction certified in writing by Supplier) all Notes, without retaining any copy thereof. No such termination of the Agreement or return or destruction of the Proprietary Information and/or Notes will affect the confidentiality obligations of Supplier or Supplier's Personnel all of which will continue in effect as provided in this Agreement.

5.7 Information Not Covered. Notwithstanding the foregoing, the parties agree that Supplier's obligations with respect to handling, disclosing, reproducing and using such Proprietary Information are not applicable to any portion(s) of the Proprietary Information which: (a) is or becomes generally available to the public other than as a result of disclosure by Supplier or Supplier's Representatives; (b) was available on a non-confidential basis prior to its disclosure to Supplier and Supplier can verify such availability by written documentation; (c) is or becomes available to Supplier on a non-confidential basis from a source other than the Company when such source is not, to the best of the Supplier's knowledge, subject to a confidentiality obligation with the Company, or (d) was independently developed by Supplier or Supplier's Personnel, without reference to the Proprietary Information, and Supplier can verify the development of such information by written documentation.

5.8 Supplier Information. Knowledge or information of any kind disclosed to Company shall be deemed to have been disclosed without financial or other obligation on the part of Company to hold the same in confidence, and Company shall have full right to use and disclose such information without any compensation beyond that specifically provided by this Agreement.

5.9 Publicity. In addition to the other confidentiality obligations under this Agreement, Supplier shall not make any announcement, take or release any photographs (except for its internal operation purposes for performing the Services) or release any information concerning this Agreement or any part thereof or with respect to its business relationship with Company to any member of the public or press, any business entity or official body except as required by applicable law, rule, injunction or administrative order, unless prior written consent is obtained from Company. If Supplier determines it is obligated by law or a governmental authority to make any such announcement or release, Supplier shall promptly notify Company and cooperate with Company to ensure that suitable confidentiality obligations are afforded such information.

5.10 System Monitoring. Supplier agrees that the Company may, at any time, without further consent, access and monitor any usage by Supplier or Supplier's Personnel of any Company information, systems and resources, including without limitation: computers, computer software, electronic mail, online services, voicemail, facsimile machines, telephones and photocopiers.

5.11 Additional Safeguards and Controls. Supplier agrees that (a) Company's Proprietary Information, and (b) any "Company Data", "Company Restricted Data", "Sensitive Personal Information" or "Controlled Data" (as such terms are defined in **Schedule I**) will be subject to the organizational, technical, and physical controls and other safeguards set out in **Schedule I**. If Supplier has access to Company Data, Company Restricted Data, Sensitive Personal Information or Controlled Data, or has access to a Company information system, Supplier agrees to apply such additional safeguards and to grant Company such additional rights as are set forth in **Schedule I** for such data. Notwithstanding anything contained herein to the contrary, to the extent that there is a conflict between any terms contained in this Agreement and those contained in **Schedule I**, the terms of Schedule I shall govern.

6. Intellectual Property.

6.1 For purposes of this Agreement, "Intellectual Property" means all intellectual property and proprietary rights, including without limitation all rights of inventorship and authorship, inventions, patents, patent applications, and know-how, for any product, process, method, machine, manufacture, design, composition of matter, or any new or useful improvement thereof, as well as copyrights, trademark, trade dress and service mark rights and all rights in trade secrets, computer software, data and databases, and mask works.

6.2 Company Property.

(a) "Company Property" means: (1) Intellectual Property incorporated into the Services or any deliverables under this Agreement; (2) Intellectual Property conceived, produced or developed by Supplier, whether directly or indirectly or alone or jointly with others, in connection with or pursuant to Supplier's performance of this Agreement; and (3) creations and inventions that are otherwise made by Supplier through the use of Company's or its Affiliates' equipment, funds, supplies, facilities, materials and/or Proprietary Information; provided, however, that any techniques, technology or tools independently developed by Supplier and not developed for or paid for by Company shall not be the Intellectual Property of Company.

(b) Supplier acknowledges that Company claims and reserves all rights and benefits afforded under federal and international intellectual property laws in all Intellectual Property and Proprietary Information furnished by Company to Supplier hereunder and that Supplier is granted only a limited right of use of such Intellectual Property and Proprietary Information as set forth in this Agreement.

(c) Assignment and Recordation of Company Property. Supplier agrees that:

(1) All copyrightable Intellectual Property, which are created by Supplier pursuant to this Agreement, shall be deemed "Works Made for Hire", as that phrase is defined in Section 101 of the United States Copyright Act, 17 U.S.C. § 101, and used in 17 U.S.C. § 201, on behalf of Company, and Company shall own all right, title and interest, including the worldwide copyright, in and to such materials;

(2) Supplier hereby assigns and agrees to assign to Company all of its respective rights, title, and interest in Company Property, including all rights of inventorship and authorship, all patents and patent applications, all copyrights, all trademark and service mark rights, all rights in trade secret and proprietary information, all rights of attribution and integrity and other moral rights and all other intellectual property rights of any type (collectively referred to herein as "IP Rights");

(3) Supplier and Supplier's successors in interest will, at Company's request and without further consideration, communicate to Company any facts known to them respecting Company Property, and testify in any legal proceedings, make all rightful oaths, sign all lawful papers and other instruments and generally do everything possible for title to the IP Rights in the Company Property to be clearly and exclusively held by Company; and

(4) Supplier agrees that it will not apply for any state, federal or other U.S. or foreign jurisdiction's registration of rights in any of the Company Property and that it will not oppose or object in any way to applications for registration of same by Company or others designated by Company.

6.3 Supplier's Property. If Supplier intends to exclude any Intellectual Property from the assignment in Section 6.2(c) above, it must list such Intellectual Property on **Schedule F** hereto, Supplier's Reserved Intellectual Property, and obtain a Company representative's signature on **Schedule F** before incorporating Supplier's Intellectual Property into the Services and/or any deliverables under this Agreement. Supplier will own approved "Supplier's Reserved Intellectual Property" reflected on a properly executed **Schedule F**. However, Supplier grants Company a fully-paid, perpetual, irrevocable, world-wide, non-exclusive license to: (a) prepare derivative works from Supplier's Reserved Intellectual Property (using either Company's own employees or independent contractors), (b) reproduce Supplier's Reserved Intellectual Property and derivative works therefrom; and (c) make, use, distribute, perform, display and transmit Supplier's Reserved Intellectual Property and derivative works and reproductions thereof, and to sublicense the rights granted to Company in this paragraph.

6.4 Third Party Intellectual Property. Supplier shall not, without Company's written authorization, disclose or use, in Supplier's work with the Company, any secret or confidential information of others, nor incorporate into the Services and/or any deliverables to Company under this Agreement: (a) any software, applications, or components or other materials subject to Intellectual Property rights owned by any party (including Supplier) other than Company ("Third Party Intellectual Property"); or (b) any software, applications, or components or other materials, which are functionally dependent upon Company's use of Third Party Intellectual Property. If Company provides such written authorization, Supplier shall, in the absence of written agreement to the contrary, provide, at no expense to Company, all licenses to such Third Party Intellectual Property and which Company does not already

have and which are reasonably necessary for Company to lawfully make all uses of the Services and/or any deliverables contemplated in this Agreement.

6.5 Escrow of Code. To the extent that any deliverables provided by Supplier under this Agreement include software, upon Company's request, Supplier agrees to deposit in escrow: (a) with an escrow agent designated by Company and (b) pursuant to a written escrow agreement to be approved by Company in writing any and all materials relating to such software delivered under this Agreement, included, but not limited to a copy of the object code, source code, documentation and all annotations thereto ("Materials"). Company agrees to pay any amount necessary to create such escrow account and/or any related deposit fees. The escrow agreement shall provide, among other things, that in the event this Agreement is terminated for insolvency or default as provided in Sections 17.4 or 17.5 below, the escrowed Materials shall be delivered to Company. Company is hereby granted a license to use the Materials, when delivered to repair, modify, improve upon and use the deliverables under his Agreement as contemplated under this Agreement, including but not limited to the rights to reproduce, prepare derivative works, distribute, perform, display and transmit.

7. Personal Data Provided to Supplier.

7.1 "Company Personal Data" includes: (a) Personal Data (defined in Section 3.5(a)) obtained by Supplier from Company; (b) Personal Data (from whatever source) being "Processed" by Supplier on behalf of Company; and (c) Personal Data (from whatever source) pertaining to Company personnel.

7.2 "Processing" of Personal Data shall mean and include any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, accessing, retrieval, use, organization, storage, adaptation or alteration, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

7.3 In the event that Supplier accesses or otherwise Processes any "Company Personal Data" during its performance of the Agreement, it shall comply with the following obligations regarding Company Personal Data:

(a) Supplier shall view and Process Company Personal Data only to the extent necessary to perform this Agreement or upon Company's written instructions.

(b) Supplier undertakes to keep Company Personal Data confidential, and agrees to not disclose Company Personal Data to third parties without having first received express received written approval from Company. Supplier and Supplier's Personnel (as defined in Section 3.1) shall Process Company Personal Data only on a need-to-know basis, regarding the performance of this Agreement and any PO or SOW issued pursuant to this Agreement.

(c) Supplier shall implement technical and organizational measures to ensure the security and confidentiality of Company Personal Data in order to prevent, among other things: (i) accidental, unauthorized or unlawful destruction, alteration, modification or loss of Company Personal Data; (ii) accidental, unauthorized or unlawful disclosure or access to Company Personal Data; and/or (iii) unlawful forms of Processing. The security measures taken by Supplier shall be in compliance with all applicable data protection regulations and shall be commensurate with the risks represented by the Processing and the nature of the Company Personal Data to be Processed, taking into consideration the state of the art security measures available to protect such data and the implementation costs of such measures. Supplier shall immediately inform Company of any breach of its security and confidentiality obligations under this Section.

(d) Supplier shall implement all measures necessary to ensure compliance by Supplier's Personnel with the obligations relating to Company Personal Data and shall require Supplier's Personnel, as a condition of having access to Company Personal Data, to sign individual confidentiality agreements in which they each agree individually to comply with the obligations of this Section of the Agreement. **Schedule B** of this Agreement shall be deemed adequate for this purpose. Company may also require Supplier to require Supplier's Personnel, as a condition of participating in specific assignments, to sign individual confidentiality agreements that are tailored for specific assignments.

(e) Supplier shall comply with all applicable laws and regulations on Personal Data protection, and will process "Employment Data" consistent with the "GE Employment Data Protection Standards", a copy of which is located at http://www.gepower.com/about/suppliers/en/document.htm and may be requested from Company. In particular, if during the performance of this Agreement, Supplier obtains Company Personal Data directly from individuals to whom such data pertains ("Data Subjects"), Supplier shall provide such Data Subjects with the information required by applicable law and regulation and when necessary, obtain the Data Subjects' consent to acquire such information. However, prior to obtaining such consent from the Data Subjects, other than Supplier's employees or subcontractors, Supplier must obtain Company's written approval of the information and consent language to be

used by Supplier to gather such Company Personal Data from the Data Subjects. Failure by Supplier to comply with any obligations relating to Company Personal Data or Personal Data set forth in this Agreement is considered a material breach of this Agreement.

(f) Company may conduct at any time, subject to a prior written notice to Supplier, an onsite verification of Supplier's compliance with obligations relating to Company Personal Data, even after the termination of this Agreement. Supplier shall provide access to all applicable facilities, equipment and records in order to conduct such verification.

(g) Upon termination of this Agreement, for whatever reason, Supplier shall stop any processing of Company Personal Data and shall return to Company any copy and/or reproduction thereof. These obligations regarding Company Personal Data shall remain in full force even after termination of this Agreement for whatever reason.

8. Physical Property. Unless otherwise agreed in writing, all tools, equipment or material furnished to Supplier or specially paid for by Company, including but not limited to Software Product (defined in Section 5.1) and any related items, and any replacement thereof, or any materials affixed or attached thereto, shall be and remain Company's personal property. Such property shall be plainly marked as Company's property and shall be safely stored separate and apart from Supplier's property. Supplier shall not substitute any Company property without Company's written approval. Such property, while in Supplier's custody or control, shall be held at Supplier's risk, shall be kept insured by Supplier at Supplier's expense in an amount equal to the replacement cost with loss payable to Company and shall be subject to removal at Company's written request, in which event Supplier shall prepare such property for shipment and shall redeliver to Company in the same condition as originally received by Supplier, reasonable wear and tear excepted, all at Supplier's expense.

9. Inspections, Testing and Acceptance.

9.1 All Services and/or any deliverables shall be subject to inspection and test by Company and any of its customers at all times and places. Supplier must follow coding and testing standards and must pass quality assurance standards provided by Company.

9.2 Supplier shall provide and maintain an inspection and process control system acceptable to Company covering any Services and/or deliverables provided hereunder. Records of all inspection work by Supplier shall be kept complete and made available to Company and any of its customers during the Term and for a period of three (3) years thereafter. Without any additional charge, Supplier will: (a) allow representatives of Company and its customers access to the facilities involved in performing this Agreement in order to assess: (i) work quality; (ii) conformance with Company's specifications; and (iii) conformance with Supplier's representations, warranties, certifications and covenants in this Agreement; and (b) provide all reasonable assistance for the safety and convenience of the inspectors in the performance of their duties.

9.3 Acceptance or rejection of the Services and/or any deliverables shall be made as promptly as practical after delivery, but failure to inspect and accept or reject the Services and/or deliverables or failure to detect defects by inspection, shall neither relieve Supplier from responsibility for all requirements relating to such Services and/or deliverables nor impose liabilities on Company for its failure to identify such defects.

9.4 If any of the Services and/or any deliverables under this Agreement, are found at any time prior to delivery to be defective, or otherwise not in conformity with the requirements of this Agreement, including any applicable specifications, Company, in addition to such other rights, remedies and choices as it may have by agreement and/or by law, at its option and sole discretion, and at Supplier's expense may: (a) reject and return such deliverables; (b) require Supplier to re-perform/replace the non-conforming Services and/or deliverables with Services and/or deliverables that conform to the requirements of this Agreement; and/or (c) take such actions as may be required to cure all defects and/or bring the Services and/or deliverables into conformity with all requirements.

10. Warranties.

10.1 Supplier warrants that:

(a) Services and/or any deliverables will be in strict accordance with the specifications, designs and other requirements (including performance specifications) approved or adopted in any PO or SOW;

(b) Services will be performed in a competent and professional manner in accordance with the highest standards and best practices of Supplier's industry;

(c) All Services and/or deliverables sold will be free of any claims of any nature and by any third person, including but not limited to claims of Intellectual Property infringement and Supplier will convey clear title to Company; and

(d) All Services and/or deliverables will be of merchantable quality, free from all defects in design, workmanship and material and will be fit for the particular purpose for which they are purchased.

10.2 The warranties in Section 10.1 shall apply for a period of twenty-four (24) months from the date Supplier completes its engagement. If any of the Services and/or deliverables under this Agreement are found to be defective during the warranty period, then in addition to other rights, remedies and choices it may have under this Agreement or at law or equity, Company, at its option and sole discretion, and at Supplier's expense may: (a) reject and return such deliverables; (b) require Supplier to re-perform/replace the non-conforming Services and/or deliverables with Services and/or deliverables that conform to the requirements of this Agreement; and/or (c) take such actions as may be required to cure all defects and/or bring the Services and/or deliverables into conformity with all requirements. Any attempt by Supplier to limit, disclaim or restrict any such warranties or any remedies of Company, by acknowledgment or otherwise, in accepting or performing this Agreement, shall be null, void and ineffective without Company's written consent.

11. Indemnities and Insurance.

11.1 General. Supplier shall take all necessary precautions to prevent the occurrence of any injury to persons, property or the environment during the progress of work and ensure that its Personnel neither pose a threat to Company's safe work environment nor the integrity of its business operations. Except to the extent that any injury or damage is due solely and directly to Company, Supplier shall release, defend, hold harmless and indemnify Company, its directors, officers, employees, agents, representatives, successors and assigns against any and all suits, actions or proceedings, at law or in equity, and from any and all claims, demands, losses, judgments, damages, costs (including reasonable attorneys' fees), fines, penalties, expenses or liabilities, including without limitation claims for personal injury or property or environmental damage, resulting from or in any way connected with any act or omission of Supplier's Personnel, Supplier, its agents, employees or subcontractors, whether acting in the course of their employment or otherwise, in connection with, but not limited to, all of the representations, warranties or covenants contained in this Agreement. In addition, Supplier shall indemnify, defend and hold Company harmless from and against any claims, costs or expenses, including, but not limited to, reasonable attorneys' fees, arising out of or in connection with any employment claims, i.e., workers compensation, harassment or discrimination claims, or breaches of Sections 5.1-5.7, 14 or 15 or **Schedule B** hereto by Supplier or Supplier's Personnel. Supplier agrees to include this clause in all related subcontracts. Supplier further agrees to indemnify Company for any attorneys' fees or other costs Company incurs in the event that Company has to file a lawsuit to enforce any indemnity or additional insured provisions of this Agreement.

11.2 Intellectual Property. Supplier shall indemnify, defend and hold Company harmless from any suit or proceeding brought against Company or its customers based on any claim that any Services, systems, article or apparatus, or any part thereof constituting Services and/or any deliverables furnished under this Agreement, as well as any device or process necessarily resulting from the use thereof, constitutes an infringement of any patent, copyright or other Intellectual Property right. If notified promptly in writing and given authority, information and assistance, at Supplier's expense, for the defense of same, Supplier shall pay all damages, costs and expenses incurred or awarded therein, including, but not limited to, reasonable attorneys' fees. If use of any systems, article, apparatus, part, device, process, Service and/or any deliverable is enjoined, Supplier shall, at its own expense and in the following order, subject to commercial practicality, either: (a) procure for Company the right to continue using such Service, system, article or apparatus, part, device, process or deliverable; (b) replace same with a non-infringing equivalent; or (c) remove such system, article or apparatus, part, device, process or deliverable or halt such Service and refund the purchase price and, if applicable, the transportation and installation costs thereof.

11.3 Insurance Coverage. During the Term of this Agreement, Supplier, shall at its own cost, obtain and keep in force for the benefit of Supplier and Company all insurance/and or bonds required by law and the following insurance to be issued by insurance carriers with a minimum rating in A.M. Best's of A:VIII or better with minimum limits as set forth below:

(a) Worker's Compensation and Employers Liability Insurance per statutory requirements;

(b) Commercial General Liability with minimum limits for Bodily Injury and Property Damage on an occurrence basis of: $3,000,000 per occurrence; $5,000,000 aggregate.

(c) Business Automobile Liability Insurance covering all vehicles used in connection with the work and covering Bodily Injury and Property Damage with a minimum limit equal to: $2,000,000 per accident.

(d) Professional Errors and Omissions Insurance covering the activities of Supplier written on a "claims made" basis with a minimum limit equal to: $5,000,000 per occurrence.

11.4 Additional Insurance Requirements.

(a) Company shall be named as additional insured under the policies of insurance set forth in subsections 11.3(b)-(d) above for any and all purposes arising out of or connected to the Services.

(b) It is the intent of both parties to this Agreement that all insurance purchased by Supplier in compliance with this Agreement, will be primary to any other insurance owned, secured, or in place by Company, which insurance shall not be called upon by Supplier's insurer to contribute in any way. Supplier shall secure endorsements to this effect from all insurers of such policies.

(c) At Company's request, Supplier shall furnish Company with certificates of insurance and with copies of original endorsements effecting coverage required by this clause. The certificates and endorsements shall identify Company as an additional insured and shall be signed by a person authorized by that insurer to bind coverage on its behalf. Company reserves the right to require complete, certified copies of all required insurance policies, at any time.

(d) All policies provided for herein shall expressly provide that such policies shall not be canceled, terminated or altered without sixty (60) days' prior written notice to Company.

(e) All insurance specified in this section shall contain a waiver of subrogation in favor of the Company, its Affiliates and their respective employees for all losses and damages covered by the insurance required by this section.

12. Relationship of the Parties; Assignment and Subcontracting.

12.1 Supplier is an independent contractor to Company. Supplier's Personnel are neither employees of Company nor eligible for participation in any Company employee benefit programs. The performance of Services by Supplier and receipt of payments shall have no effect on any payments or benefits that any of Supplier's Personnel is now or may later become entitled to as a result of past employment by Company.

12.2 Neither Supplier's Personnel, Supplier nor its agents, subsidiaries, affiliates and employees are in any way the legal representatives or agents of Company, and neither shall have any right or authority to assume or create any obligation of any kind expressed or implied in the name of or on behalf of Company.

12.3 This Agreement and any rights hereunder (except where expressly provided in a signed writing to the contrary) are non-exclusive and non-assignable. Any assignment by one party without the prior written consent of the other party shall be void, provided that Company may assign or transfer its rights and obligations under the Agreement to any Affiliate of Company upon written notice to Supplier. Supplier shall notify Company in writing in advance of any proposed change in its ownership, control or management and shall not without the written consent of Company delegate the performance of its obligations under this Agreement to any firm or person (other than a principal, officer or regular employee of Supplier). Notwithstanding the above, upon written notification to the other party, either party may assign this Agreement to any entity, which acquires all of (or substantially all of) the assets or voting stock of such entity.

12.4 Supplier may not subcontract or delegate any Services without Company's prior written consent.

13. Governing Law and Venue.

13.1 Each party's rights and obligations under or in connection with this Agreement shall be governed by the laws of the State of New York, U.S.A. (excluding its conflict of laws rules). The parties exclude application of the United Nations Convention on Contracts for the International Sale of Goods.

13.2 The parties shall attempt amicably to resolve any controversy, dispute or difference arising out of this Agreement, failing which either party may initiate litigation only in the United States District Court for the Southern District of New York or, if such court lacks subject matter jurisdiction, in the Supreme Court of the State of New York in and for New York County. The parties submit to personal jurisdiction in said courts and waive any defenses regarding venue or *forum non conveniens*.

14. Compliance with Laws. Supplier represents, warrants, certifies and covenants ("Covenants") that:

14.1 It will comply with all applicable laws, including, but not limited to, any national, international, federal, state, provincial or local law, treaty, convention, protocol, common law, regulation directive or ordinance and all lawful orders, including judicial orders, rules and regulations issued thereunder, including without limitation those dealing with the environment, health and safety, records retention and/or the transportation or storage of "hazardous materials". As used in this Agreement, the term "hazardous materials" shall mean any substance or material defined as a "hazardous material," "hazardous substance" or "dangerous good" under 49 CFR § 171.8 or any other

applicable requirement of any entity with jurisdiction over the activities, deliverables, goods or services, which are subject to this Order;

14.2 No Services and/or deliverables supplied under this Agreement have been or will be produced utilizing forced, indentured or convict labor or utilizing the labor of persons in violation of the minimum working age law in the country of manufacture or in any country in which the Services are provided or in violation of minimum wage, hour of service or overtime laws in the country of manufacture or any country in which Services are provided. If any such labor is determined by Company to have been used, Company shall have the right to immediately terminate the Agreement without further compensation to Supplier;

14.3 Subcontractor Flow-downs for U.S. Government Commercial Items Contracts. Where the deliverables, goods and/or services being procured by Company from Supplier are in support of a U.S. government end customer or an end customer funded in whole or part by the U.S. government, Supplier Covenants to comply with the terms of FAR 52.212-5(e) or 52.244-6 and DFARS 252.212-7001(c) or DFARS 252.244-7000 to the extent those terms are applicable to commercially available off-the-shelf ("COTS") items or commercial items and as appropriate for the dollar value of any PO or SOW under this Agreement. In addition, if a PO or SOW under this Agreement is in support of a project involving Rural Utility Service ("RUS") funds, then the following additional requirements apply: (a) Article VI, Section 4 of RUS Form 198, "Compliance with Laws", specifically the certification as to Debarment and Suspension set forth in 7 CFR part 3017; and (b) Article VI, Section 5 of RUS Form 198, "Equal Opportunity Provisions", including the requirements for Supplier to provide a certification that Supplier has filed a current report on Standard Form 100 and a Certificate of Non-segregated Facilities. The version of these clauses/provisions/requirements shall be those that are in effect as of the date of a specific PO or SOW;

14.4 Supplier represents that any Services provided hereunder will be provided in compliance with the requirements of the Fair Labor Standards Act of 1938, as amended, including Section 12(a) thereof;

14.5 Supplier certifies that it is in compliance with the requirements for non-segregated facilities set forth in 41 C.F.R. Chapter 60-1.8;

14.6 Supplier and Supplier's Personnel agree to comply fully with the import and export control laws and regulations of the United States Government. No information, technical data, software or Services, including any deliverables, will be exported or re-exported except as permitted by U.S. law and regulation and with Company's written approval. Supplier shall acknowledge its responsibilities with respect to export controlled information by signing the "GEH Export Controlled Information Acknowledgment of Responsibilities," attached hereto as **Schedule K**. In addition, at Company's request, Supplier shall execute a Supplier Subcontractor Export Controlled Information Agreement (provided by Company) with one or more of Supplier's subcontractors and provide a copy of such agreement to the Company prior to providing any such subcontractor or subcontractors with export controlled information;

14.7 Supplier shall comply with all laws dealing with improper or illegal payments, gifts and gratuities, and Supplier agrees not to pay, promise to pay or authorize the payment of any money or anything of value, directly or indirectly, to any person for the purpose of illegally or improperly inducing a decision or obtaining or retaining business in connection with this Agreement;

14.8 Supplier agrees that if the Services it provides will have a material impact on Company's ability to report financial information in an accurate and timely manner, that Supplier will certify and ensure that it is in compliance with Section 404 of the Sarbanes Oxley Act of 2002 and that Supplier will supply to Company, in a manner specified by Company, documents attesting that Supplier has in place controls that are effective and have been tested by a third party, such as an outside auditor, that monitor and ensure compliance with Section 404 of the Sarbanes Oxley Act of 2002; and

14.9 Supplier further agrees to provide at Company's request certificates relating to any applicable legal requirements or to update any and all of the certifications, representations and warranties under this Agreement, in form and substance satisfactory to Company.

15. Environmental Health and Safety; Cyber Security. Supplier represents warrants and certifies that:

15.1 It will take appropriate actions necessary to protect health, safety and the environment, including, without limitation, in the workplace and during transport;

15.2 Each chemical substance constituting or contained in deliverables or goods sold or otherwise transferred to Company is listed on: (i) the Toxic Substances Control Act ("TSCA"; 15 USC § 2601, *et seq*.), otherwise known as the TSCA Inventory, or exempted from such list under 40 CFR § 720.30-38; (ii) the Federal Hazardous Substances Act (P.L. 92-516) as amended; (iii) the European Inventory of Existing Commercial Chemical

Substances ("EINECS") as amended; (iv) the European List of Notified Chemical Substances ("ELINCS") and lawful standards and regulations thereunder; or (v) any equivalent lists in any other jurisdiction to or through which Company informs Supplier the deliverables or goods will likely be shipped;

15.3 Goods or deliverables sold or transferred to Company will not include: (i) any chemical substance prohibited pursuant to Section 6 of the TSCA; (ii) any of the following chemicals: arsenic, asbestos, benzene, beryllium, carbon tetrachloride, cyanide, lead or lead compounds, cadmium or cadmium compounds, hexavalent chromium, mercury or mercury compounds, trichloroethylene, tetrachloroethylene, methyl chloroform, polychlorinated biphenyl ("PCB"), polybrominated biphenyls ("PBB"), polybrominated diphenyl ethers ("PBDE"); (iii) designated ozone depleting chemicals as restricted under the Montreal Protocol (including, without limitation 111 trichloroethane, carbon tetrachloride, Halon-1211, 1301 and 2402, and chlorofluorocarbons ("CFCs") 11-13, 111-115, 211-217), unless Company agrees in writing; (iv) any other chemical the use of which is restricted in any other jurisdiction to or through which Company informs Supplier the deliverables or goods are likely to be shipped, unless Company expressly agrees in writing; and

15.4 If any deliverables, goods or other materials sold or transferred to Company contain hazardous materials, Supplier shall provide all relevant information required pursuant to applicable requirements, such as: (i) the Occupational Safety and Health Act ("OSHA") regulations 29 C.F.R. § 1910.1200, including a completed Material Safety Data Sheet (OSHA Form 20) and mandated labeling information and (ii) any similar requirements in any other jurisdictions to or through which Company informs Supplier the deliverables, goods or other materials are likely to be shipped.

15.5 The Services, whether conducted at Company's site or at the Supplier's own premises, are subject to all applicable regulations governing computer security, including cyber security. GEH is required to ensure that Supplier meets the regulations of the U.S. Nuclear Regulatory Commission found at Title 10 Code of Federal Regulations (CFR) Part 73.54, "Protection of digital computer and communications systems and networks." Work performed for such computer and communications systems must meet the requirements provided in **Schedule J**.

16. Conflict of Interest; Company Policies.

16.1 Supplier represents and warrants that: (a) it has no conflict of interest which would prevent Supplier from acting in the best interests of Company and that such a situation will not exist during the Term; (b) it has not entered into any contract or agreement, or executed any document whatsoever, that will in any manner prevent it from: (1) giving Company the exclusive benefit of services under this Agreement; (2) disclosing and assigning ideas, inventions, computer software, trade secrets and other Intellectual Property as provided in Section 6.2(c) of this Agreement; or (3) performing any other provision of this Agreement; (c) it will not enter into any contract or agreement, or execute any document, which will create a conflict of interest or which will prevent it from freely performing any provision of this Agreement; and (d) it will not knowingly incorporate confidential information of any person or entity not a party to this Agreement into any Services or deliverables furnished to Company without prior written notice to Company.

16.2 Supplier acknowledges that it has received a copy of the following documents: (a) Guidelines - Third Party Suppliers (the "Guidelines"), attached hereto as **Schedule G**, and (b) the GE Power & Water Integrity Guide for Suppliers, Contractors and Suppliers (the "Guide"), attached hereto as **Schedule H**. Supplier agrees that it will: (i) comply fully with the Guidelines and the Guide in the performance of the Services; (ii) provide a copy of the Guide to Supplier's Personnel; (iii) instruct Supplier's Personnel to comply with such documents; and (iv)be responsible for any failure of Supplier's Personnel to comply with such documents. Supplier further agrees that it and Supplier's Personnel shall, upon reasonable notice, attend and participate in compliance briefings conducted by Company representatives; and

16.3 Supplier agrees that neither it nor any of Supplier Personnel shall communicate in any manner with: (a) any officer or employee of any Federal agency of the U.S. for or on behalf of Company with respect to any contract or federal procurement; or (b) any member of Congress or any employee of a member of Congress for or on behalf of Company with respect to any matter.

17. Expiration, Termination and Suspension.

17.1 Expiration. This Agreement shall automatically expire at the end of the Term unless specifically renewed prior thereto by mutual written consent by the parties.

17.2 Termination by Mutual Agreement. This Agreement and any PO or SOW hereunder may be terminated before the Term by mutual written consent by the parties.

17.3 Termination for Convenience. Company may terminate all or any part of this Agreement and any PO or SOW hereunder at any time by written notice to Supplier specifying the extent of termination and the effective date. Upon

such termination (except due to Supplier's insolvency or default including failure to comply with this Agreement), Company and Supplier shall negotiate reasonable termination costs identified by Supplier within thirty (30) days of termination notice.

17.4 Termination for Insolvency. If Supplier ceases to conduct its operations in the normal course of business, including any inability to meet its obligations as they mature, if any proceeding under the bankruptcy or insolvency laws is brought by or against Supplier, if a receiver is appointed or applied for, or if an assignment for the benefit of creditors is made by Supplier, Company may terminate all or any part of this Agreement without liability, except for Services performed or deliverables delivered prior to termination or for deliverables covered by this Agreement then completed and later delivered in accordance with the terms of the Agreement.

17.5 Termination for Default. Time is of the essence in this Agreement. Except for delay, which is due to causes beyond the reasonable control and without the fault or negligence of Supplier and its suppliers (lasting not more than sixty (60) days), Company may, by written notice of default, terminate the whole or any part of this Agreement in any one of the following circumstances if:

(a) Supplier fails to perform within the time specified herein or any written extension granted by Company;

(b) Supplier fails to make progress as to endanger performance of this Agreement;

(c) Supplier breaches, violates or Company finds to be untrue, any of the certifications, representations and warranties set forth in Sections 14 and 15 of this Agreement; or

(d) Supplier fails to comply with any other terms and conditions of this Agreement.

Such termination shall become effective if Supplier does not cure such failure within a period of ten (10) days or such longer period as Company may authorize in writing. Upon termination, Supplier shall continue performance of this Agreement to the extent not terminated, Company may procure, upon such terms as it shall deem appropriate, Services and/or deliverables similar to those so terminated, and Supplier shall be liable to Company for any excess costs for such Services and/or deliverables. As an alternate remedy and in lieu of termination for default, Company, at its sole discretion, may elect to extend the delivery schedule and/or waive other deficiencies in Supplier's performance, in which case an equitable reduction in the amount of payments to be made under the Agreement shall be negotiated. If Supplier for any reason anticipates difficulty complying with any required delivery dates hereunder, or in meeting any of the other requirements of this Agreement, Supplier shall promptly notify Company in writing. If Supplier does not comply with any schedule hereunder, Company may require delivery by the fastest means available and charges resulting from any such premium transportation must be fully pre-paid and absorbed by Supplier. The rights and remedies of Company provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by contract, law or equity.

17.6 Suspension. Company may at any time, by written notice to Supplier, suspend performance of work hereunder, specifying the date of suspension and the estimated duration. Upon receiving any such notice of suspension, Supplier shall promptly suspend performance of work hereunder to the extent specified, and during the period of such suspension, properly care for and protect all work in progress and materials, supplies and equipment related to the work. Upon Company's request, Supplier shall promptly deliver copies of outstanding agreements and subcontracts for materials, equipment and services for the work and shall take such action relative to such agreements and subcontracts as directed by Company. Company may at any time withdraw the suspension by written notice to Supplier specifying the effective date and scope of withdrawal, and Supplier shall resume diligent performance of the work for which the suspension is withdrawn on the specified effective date of withdrawal.

17.7 Obligations Upon Expiration or Termination.

(a) Neither Company nor Supplier shall be liable by reason of the termination, expiration or non-renewal of this Agreement to the other for compensation, reimbursement or damages on account of the loss of prospective or anticipated revenues or on account of expenditures, investments, leases or commitments in connection with the business or good will of Company or Supplier or otherwise. However, this limitation is not intended to limit the liability of either party for defaults under Section 17.5. Upon expiration or after receipt of a notice of termination, Supplier shall immediately:

(i) stop work as directed in the notice;

(ii) place no further subcontracts or POs for materials, services or facilities hereunder, except as necessary to complete the continued portion of this Agreement; and

(iii) terminate all subcontracts to the extent they relate to work terminated.

(b) After termination, Supplier shall deliver to Company all completed work and work in process, including all designs, drawings, specifications and other documentation and material required or produced in connection with such work and submit a final termination settlement proposal in the form and in the manner prescribed by Company. Company shall reimburse Supplier for the cost of all work performed under this Agreement before the date of receipt of the notice of termination, including a *pro rata* portion of Supplier's profit, less any costs Company incurred as a result of the termination, or due to Supplier's breach of any of its representations, warranties or covenants in this Agreement. The following terms of this Agreement shall survive any such expiration or termination: Sections 5, 6, 7 and 10-19.

18. Limitation of Liability. Neither party to this Agreement shall have liability to the other with respect to claims arising out of, in connection with or resulting from this Agreement, whether in contract, tort (including negligence of any degree) or otherwise except as provided under the terms of this Agreement.

19. Release of Claims. In consideration of the execution of this Agreement by Company, Supplier hereby releases Company from all claims, demands, contracts and liabilities, if any, as of the date of execution of this Agreement, except indebtedness, which may be owing upon a written contract signed by Company.

20. Waiver and Failure to Enforce. No claim or right arising out of a breach of this Agreement can be discharged in whole or in part by a waiver or renunciation unless the waiver or renunciation is supported by consideration and is in writing signed by the aggrieved party. Company's failure to enforce at any time or for any period of time any provision hereof shall not be construed to be a waiver of such provision or of the right to Company thereafter to enforce each and every such provision.

21. Notices. Notices and other communications between the parties shall be in English and shall be deemed to be validly given if transmitted in writing, by registered mail, overnight courier or personal delivery, in all cases signature required, to the other party at the address and to the contact set forth below. Either party may change its address by giving notice to the other party as provided for herein.

Company		Supplier	
Name:	_____	Name:	_____
Address:	_____	Address:	_____
Phone:	_____	Phone:	_____
Email:	_____	Email:	_____

22. Acceptance of Terms and Conditions. The parties agree to be bound by and to comply with all the terms and conditions of this Agreement, including any supplements thereto and all specifications and other documents referred to in this Agreement. This Agreement does not constitute an acceptance by Company of any offer to sell, any quotation or any proposal. Reference in this Agreement to any such offer to sell, quotation or proposal shall in no way constitute a modification of any of the terms of this Agreement. The terms of this Agreement take precedence over any alternative terms and conditions in any other document connected with this transaction unless such alternative terms are expressly incorporated by reference on the face of this Agreement. **ANY ATTEMPTED ACKNOWLEDGMENT OF THIS AGREEMENT CONTAINING TERMS AND CONDITIONS INCONSISTENT WITH OR IN ADDITION TO THE TERMS AND CONDITIONS OF THIS AGREEMENT IS NOT BINDING UPON COMPANY UNLESS SPECIFICALLY ACCEPTED BY COMPANY IN WRITING.**

23. Electronic Commerce. Supplier agrees to participate in all Company's current and future electronic commerce applications and initiatives. For contract formation, administration, changes and all other purposes each electronic message sent between the parties within such applications or initiatives will be deemed: (a) "written" and a "writing"; (b) "signed" (in the manner below); and (c) an original business record when printed from electronic files or records established and maintained in the normal course of business. The parties expressly waive any right to object to the validity, effectiveness or enforceability of any such electronic message on the ground that a "statute of frauds" or any other law requires written, signed agreements. Between the parties, any such electronic documents may be introduced as evidence in any proceedings as business records originated and maintained in paper form. Neither party shall object to the admission of any such electronic document under either the best evidence rule or the business records exception to the hearsay rule. By placing a name or other identifier on any such electronic message, the party doing so intends to sign the message with his/her signature attributed to the message content. The effect of each such message will be determined by the electronic message content and by New York law, excluding any such law requiring signed agreements or otherwise in conflict with this paragraph.

24. Execution and Modification.

24.1 This Agreement and all documents incorporated herein by reference constitute the complete and final agreement concerning the subject matter hereof. Any representations, terms or conditions not incorporated herein shall not be binding upon either party. No course of prior dealings between parties, no course of performance and no usage of trade shall be relevant to determine the meaning of this Agreement even though the accepting or acquiescing party has knowledge of the performance and opportunity for objection. The invalidity, in whole or in part, of any of the foregoing sections of this Agreement shall not affect the remainder of such sections or any other section of this Agreement.

24.2 This Agreement wholly cancels, terminates and supersedes all previous negotiations, commitments and writings between the parties in connection therewith. This Agreement shall not become effective or binding upon Company until signed by an authorized representative of Company at which time it will be deemed retroactively effective upon the Effective Date.

24.3 No change, modification, extension, renewal, ratification, rescission, termination, notice of termination, discharge, abandonment or waiver of this Agreement or any of the provisions hereof, nor any representation, promise or condition relating to this Agreement, shall be binding upon Company unless made in writing and signed by an authorized representative of Company.

24.4 The parties agree that they will contract in the English language and that there shall be no requirement to translate this Agreement or any of the documents incorporated herein into any other language.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their respective authorized representatives as of the Effective Date first written above.

[GE-HITACHI NUCLEAR ENERGY AMERICAS LLC [GE-HITACHI NUCLEAR ENERGY INTERNATIONAL LLC][GE-HITACHI GLOBAL LASER ENRICHMENT LLC]	**[SUPPLIER NAME]**
Signature: _____	Signature: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____

SCHEDULES

Schedule	Subject
A	Schedule of Fees for Supplier's Personnel
B	Secrecy and Inventions Agreement
C	Requirements for Supplier Personnel Screening
D	Personal Data Consent Form
E	Travel and Living Policies
F	Supplier's Reserved Intellectual Property
G	Guidelines - Third Party Suppliers
H	GE Power & Water Integrity Guide for Suppliers, Contractors and Consultants
I	Privacy and Data Protection
J	Requirements for Cyber Security Related Goods or Services
K	GEH Export Controlled Information: Acknowledgment of Responsibilities

SCHEDULE A

SCHEDULE OF FEES FOR SUPPLIER'S PERSONNEL

[TO BE INSERTED, IF APPLICABLE]

Name	Hourly Rate	Relationship to Supplier if not a full time employee

SCHEDULE B

SECRECY AND INVENTIONS AGREEMENT

Supplier Name: [Insert Supplier Name]

Employee Name: [Insert Employee Name] **Email Address:** [Insert Email Address]

In consideration of [**GE-Hitachi Nuclear Energy Americas LLC][GE-Hitachi Nuclear Energy International LLC][GE-Hitachi Global Laser Enrichment LLC]** ("Company") approval of my furnishing of services under the Master Services Agreement ("Agreement") between Company and Supplier, I agree to be personally bound by the following terms for Company's benefit:

1. Law and Conflict of Interest

I warrant that: (i) my work with Company will not violate any law or conflict with any continuing interests or obligations I may have with my current or prior employers; and (ii) during performance under the Agreement, I will avoid any other activities that would present a conflict of interest regarding such performance.

2. Confidentiality and Personal Data

I will hold in confidence all proprietary and confidential information I obtain from or develop for Company ("Proprietary Information"). I agree not to use Proprietary Information on my own behalf or on behalf of others, or disclose to others, at any time such Proprietary Information without Company's prior written consent. I also will not knowingly disclose to Company or its employees any information that is known to be secret, confidential or proprietary to any other person or firm. I further agree to keep confidential any "Company Personal Data", which is any information relating to an identified or identifiable, natural person: (a) obtained by Supplier from Company, (b) being "Processed by Supplier on behalf of Company or (c) pertaining to Company's employees, officers, directors, shareholders, customers, prospects, contacts, suppliers or distributors, and I agree to only access and use such Company Personal Data to the extent necessary to perform this Agreement, to use reasonable measures to endure the security and confidentiality of Company Personal Data and to comply with all applicable laws, regulations and Company or its Affiliates' policies relating to such data as are made known to me.

3. Inventions

I agree that any inventions, suggestions, ideas, innovations or reports made or conceived by me as a result of services performed hereunder ("Inventions") shall be promptly disclosed to, and shall be the sole property of, Company. I will cooperate with Company in obtaining patents on any such Inventions and shall execute any documents tendered by Company to convey or perfect ownership in such Inventions. I will assist Company, at its expense, in any manner Company deems necessary to obtain, maintain or sustain such patents. Should any such Inventions be the result of combined efforts with, or the invention of any person or persons other than myself, I will so inform Company at the time of submission thereof. My obligations hereunder shall survive termination of this Agreement.

4. Copyrights

All copyrightable material resulting from work performed by me during the term of the Agreement shall be deemed to be "works made for hire" under U.S. copyright law and shall belong exclusively to Company. If by operation of law any such copyrightable materials are not deemed works made for hire, I agree to and hereby assign to Company the ownership of such materials including all copyrights thereto. Company may obtain and hold in its own name copyrights, registrations and other protection that may be available therein and I will provide Company any assistance required to perfect such protection. I expressly waive any "artist's rights" or "moral rights" I might otherwise have in the materials developed under this Agreement. To the extent I cannot effectively waive such rights, I agree that I will not seek to enforce such rights against Company or any licensee or purchaser of such materials from Company.

5. Employer-Employee Relationship

In furnishing services under this Agreement, I will at all times be acting as an employee of Supplier. I will not be a Company employee and will not through this Agreement or my services be entitled to participate in or receive any benefit or right under any Company employee benefit or welfare plans, including without limitation, employee insurance, pension, savings and stock bonus or savings and security plans.

6. IM Security Guidelines

I shall be bound by any additional password or security documents, NT guidelines, UNIX guidelines, software licenses and IM security guidelines provided by Company.

My signature below indicates my intent to be personally bound by this document.

AGREED: _____

Name: _____

Mail to:
Company Representative Name
Listed In Section 21 Of The MSA

Title: _____

Date: _____

SCHEDULE C

REQUIREMENTS FOR SUPPLIER PERSONNEL SCREENING

To the extent permissible by applicable law, if (i) unescorted access to any Company location, facility, or worksite; (ii) deploying any Supplier Personnel to perform Services at any Company customer location, facility, or worksite; or (iii) granting access to Company networks (i.e., having a GE-issued single sign-on account) is required, Supplier shall, before any such access is granted:

1. Conduct **background screening** as follows:

1.1. Verify Supplier Personnel's identity (e.g., using social security numbers and credit reporting databases to verify identity gaps); Verify such Supplier Personnel's identity (e.g., using social security numbers and credit reporting databases to verify identity gaps);

1.2. Perform watch lists screening to ensure that no Supplier Personnel are included on the following government or organization lists, and not place any Supplier Personnel that are identified on such lists:

- Consolidated List of Financial Sanctions Targets (formerly the Bank of England Consolidated List)
- Bureau of Industry and Security Lists
- Consolidated List – Australia
- Consolidated List – Canada
- DTC Debarred List
- EU Consolidated List
- FBI Most Wanted Terrorists
- FBI Seeking Information
- FBI Top Ten Most Wanted
- FBI Most Wanted
- Hong Kong Monetary Authority List
- Interpol Most Wanted
- Ministry of Export, Trade, and Investment (METI) – Japan
- Monetary Authority of Singapore List
- OFAC Sanctions Programs
- OFAC List of Specially Designated Nationals and Blocked Persons
- Primary Money Laundering Concern List (US Department of the Treasury List of Financial Institutions Specially Designated as Being of Primary Money Laundering Concern)
- State Department Proliferation List
- Terrorist Exclusion List
- United Nations Consolidated List

1.3. Conduct a background check as follows:

1.3.1. Perform a criminal record check through an authorized background-reporting agency (including in-person searches of county courthouse records, where such records are available (e.g. United States, Mexico, etc.) covering at least the last seven (7) years, including all locations of residence and locations of employment, as stated on his or her resume, which the Supplier Personnel resided and worked during that period;

1.3.2. Verify the past seven (7) years of employment (e.g., position or job title held, dates of employment and duties); and

1.3.3. Not place any Supplier Personnel with Company if such Supplier Personnel lied or failed to disclose any relevant information, including but not limited to any prior criminal conviction on his or her pre-placement or employment application.

1.3.4. If the Supplier Personnel has been convicted of, or plead guilty to, any of the following felonies at any time, the supplier or subcontractor are required to notify Company and seek approval prior to assigning a worker to Company in a "security sensitive" position:

- Homicide
- Burglary
- Aggravated Assault
- Criminal Sexual Abuse
- Kidnapping, Abduction, Unrestraint
- Threatening or Harassing
- Altering or tampering with Motor Vehicle ID Numbers
- All offenses involving drugs
- Offenses involving Criminal enterprises and Racketeering
- Prostitution, Sexual Exploitation of minors and Obscenity
- Individual Rights (Peonage, Involuntary Servitude and Slave Trade)
- Antitrust
- Public Safety (Explosives and Arson, Firearms, Mailing Injurious Articles)

1.3.5. Other types of felonies and misdemeanors also require prior approval from Company before assignment to a "security sensitive" assignment if:

- The worker is serving probation[1] for any criminal conviction, whether or not a felony;
- The nature of the act is such that it would cause Company to doubt the trustworthiness of the worker; or
- Assigning the worker to GE could cause GE to be put in a significantly increased risk of litigation or negative publicity.

1.3.6. Supplier may not exclude a candidate solely on the basis of a prior criminal conviction unless the conviction relates to **dishonesty** or **breach of trust**; or **a matter that directly relates to the Supplier Personnel's suitability for assignment to the position for which he or she is intended**. Care should be taken to ensure that decisions are in accordance with applicable state and federal regulations regarding hiring practices. Supplier should consult with its local Human Resources and/or Legal Department to ensure compliance with these guidelines and applicable law. In reaching a placement decision based on criminal background checks, consideration should be given to the following factors that may mitigate the doubts and/or risks that may be indicated by the Supplier Personnel's criminal record:

- Whether the criminal record is correct;
- The amount of time that has elapsed since the conviction(s);
- The facts and circumstances surrounding the act(s) or event(s);
- The number of and type/severity of the offenses for which the individual was convicted;
- Age at time of the conviction or release from prison;
- Evidence that the individual has successfully performed similar work post-conviction;
- Length and consistency of employment history before and after the conviction(s);
- Rehabilitation efforts, education and training.
- Employment or character references and other information regarding fitness for the particular position; and
- Whether the individual is bonded under a federal, state or local bonding program.

1.4. GEH, in its sole discretion, may determine certain Services the Supplier Personnel will be performing to be security sensitive in nature, in which case GE may mandate, to the extent permitted by applicable law, the foregoing screenings/verifications be conducted regardless of whether or not the Supplier Personnel are performing the Services on Company premises or having network access to Company's networks. Additionally, GE may require further verifications and/or searches as may be deemed necessary, to the extent permitted by applicable law, such as, for example, verifying the Supplier Personnel's highest level of education and conducting a department of motor vehicle search.

1.5. At the completion of the required background check, the Supplier shall provide an identification number, ideally not a Social Security Number, which uniquely identifies a completed background check for their employees on their access screening completion certification letter that GEH Security can use to audit when required. The GE-preferred vendors

[1] Typically, background checks will not give sufficient details to permit a determination of whether an applicant remains on probation. Often, the record will show when probation began. Based on the date probation began, the applicant should be interviewed to determine current status.

(available at www.gehsupplier.com) will provide a GE Access Number for this purpose. Other vendors can be utilized if agreed to by Company, and if a similar unique tracking number is provided. The vendor name shall be provided in addition to the tracking number.

2. Implement a **drug screening** program that meets the following standards:

2.1. It is the policy of Company to maintain a work place free from the use/abuse of alcohol and/or illegal drugs and the effects of such use/abuse, to identify workers who exhibit the effects of such use/abuse. Supplier Personnel are prohibited from engaging in or attempting to engage in the sale, use, possession or transfer of alcohol, illegal drugs, unauthorized controlled substances, and/or drug-related paraphernalia on Company Premises, from reporting to work in an unfit/impaired condition, and/or from performing or attempting to perform their duties in an unfit/impaired condition. The aforementioned prohibitions include impairment due to a valid prescription medication if use of that medication prevents the Supplier Personnel from performing safe and competent work. Supplier Personnel who violate this policy will be subject to immediate access revocation.

2.2. Urine drug testing and breath alcohol testing will follow US Department of Transportation (DOT) collection procedures. All other testing methods will follow guidelines set by a US Department of Health and Human Services (DHHS)-certified laboratory.

2.3. The responsible collection site shall send collected samples to a designated DHHS-certified laboratory in accordance with appropriate chain-of-custody procedures.

2.4. The designated laboratory shall conduct screening panels for the following drugs:

2.4.1. Amphetamines

(a) Amphetamine
(b) Methamphetamine
(c) MDA Analogues (MDA, MDMA, MDEA)
(d) MDA (Methylenedioxy-Amphetamine)
(e) MDMA (Methylenedioxy-Methamphetamine)

2.4.2. Cocaine / Metabolites

(a) Benzoylecgonine
(b) Cocaine
(c) Cocaethylene
(d) Norcocaine

2.4.3. Cannabinoids (Marijuana Metabolite) ($THC\text{-}COOH)^3$

2.4.4. Opiates

(a) Morphine
(b) Codeine
(c) Hydromorphone
(d) Oxycodone
(e) Hydrocodone
(f) 6-Monoacetylmorphine

2.4.5. Phencyclidine (PCP)

2.5. The designated laboratory shall also test each specimen for adulteration by running a selected adulteration panel of tests.

2.6. The designated laboratory shall communicate the results of the tests to the responsible Medical Review Officer (MRO).

2.7. The MRO shall meet or otherwise directly communicate with each Supplier's Personnel who tests positive for drugs in order to determine if an acceptable explanation can account for the positive result.

2.8. If no such explanation is forthcoming, the MRO shall report the positive results to the Supplier.

2.9. Supplier will not place any Supplier Personnel with Company who have received a positive test result within one year.

2.10. A negative test result for the initial drug screen shall be obtained before any Supplier Personnel are placed with Company. A negative test is defined as the result of a drug test that indicates no presence of a prohibited substance or its metabolites above the established cutoff set by a DHHS-certified laboratory or that the MRO has found a supportable reason for the presence of a controlled substance.

2.11. It is recognized that performance of substance abuse testing under this policy may, in certain locations, be limited by state or local regulations. Local management shall, in all instances, administer this policy in accordance with applicable local or state statutes and regulations.

3. Ensure compliance with access requirements under applicable **export control laws** by:

3.1. Verifying US Person status of Supplier Personnel by reviewing one of the documents:

(a) US Passport,
(b) Original US Birth Certificate,
(c) Permanent Resident Card, aka "Green Card" (USCIS Form I-551),
(d) Original Certificate of US Citizenship (USCIS Form N-560 or N-561),
(e) Original Certificate of Naturalization (USCIS Form N-550 or N-570), OR

3.2. Obtaining individual approval from Company Export Control Leader for access by non-US Persons.

4. For the Purposes of this agreement, understand "Supplier Personnel" shall mean any employee, worker, leased worker, personnel, consultant, agent, Subcontractor, or any of the foregoing of such Subcontractors provided by Supplier to perform Services or Deliverables. "Subcontractor" means any individual, firm, corporation or third party engaged directly or indirectly by the Service Provider in the performance of any part of the Services and/or Deliverables, including any individual, firm or corporation furnishing materials or services necessary for the performance of the obligations under the Agreement and/or applicable statement of work.

5. Submit requests for access authorization via a designated workflow (i.e., www.gehsupplier.com).

6. Maintain, as records, all of the foregoing screenings/verifications for the duration of the Term, and for three (3) years thereafter.

7. Understand that if any screened/verified Supplier Personnel providing the Services to Company or any Business Component leaves the employ of Service Provider for a period of twelve (12) months or more, and such Supplier Personnel are then rehired by Service Provider and reassigned to servicing Company, or any Business Component, a new screening/verification must be ordered.

8. Agree to cooperate with Company, in good faith, to establish and implement any background verification process that Company may propose to verify that any or all of the foregoing background checks have been satisfied. Company will retain the right to audit any Supplier's compliance with this procedure.

SCHEDULE D

EXAMPLE PERSONAL DATA NOTICE AND CONSENT FORM (CONTINGENT WORKER)

***** THIS PERSONAL DATA CONSENT FORM IS PROVIDED TO SUPPLIER AS AN EXAMPLE ONLY. SEE SECTION 3.5(a).**

A. DISCLOSURE

1. Introduction. Since you will be providing services as a Contingent Worker ("CW" or "you") assigned by your employer ("Supplier") to work on a project for **[GE-Hitachi Nuclear Energy Americas LLC][GE-Hitachi Nuclear Energy International LLC][GE-Hitachi Global Laser Enrichment LLC]** (" Company") or its successors in interest, Company needs to collect, track and process certain information about you that may be deemed "personal data" and regulated by law. The law requires Company and its employees to observe certain standards when processing personal data. For example, Company and its employees must maintain accurate, up-to-date personal data, which is not kept longer than necessary and which is protected against loss or disclosure. This form describes the types of data which Company intends to process in connection with your assignment, ways in which it will be processed and the reasons for such processing. The term "processing" for these purposes includes obtaining, recording, holding, transferring, adapting, disclosing, erasing and otherwise using data. Company will be the data "Controller" for this processing.

2. Data Held. The following is a list of the types of data relating to you that will be held by Company and may be deemed "personal data":

(a) data about you, including your name, nickname, office address, office telephone, mobile telephone, pager and facsimile number, office email address, email mailing list memberships, direct reports, country of citizenship (necessary for access controls on export-controlled information), Company Directory Initiative ("CDI") ID (a database identifier assigned by Company), whether you are a prior Company employee, whether Supplier has performed a satisfactory background check on you, and whether you have signed certain agreements and acknowledgements that may apply to your assignment, such as this Personal Data Consent Form, Assignment Limitation Acknowledgement, Company Integrity Acknowledgement, Network Access Agreement, End User License Agreement, and Secrecy and Invention Agreement; and

(b) data about your Company assignment, including the name of the assignment, your job title on the assignment, your function (work skill) on the assignment, your role within that function, your assignment location, your contract type (i.e., fixed price, time & materials, etc.), your hourly billing rate, your normal billing hours per week, your assignment start date, assignment target end date and assignment actual end date, the payment method for your services, Purchase Order ("PO") number, Request for Proposal ("RFP") number, Funding Cost Center Code, and Cost Tracking Type used for the assignment, and whether a Purchase Service Agreement was signed; and

(c) data about projects you work on while in the assignment, including Contingent Worker's Project ID number, the project name, project description, the name of the Company IT Organization leading the project, the Company business unit supported by the project, the Company function supported by the project, the primary technology used on the project, and the Company-assigned category of the project (such as Make, Buy or Sell, and RTS or Program); and

(d) data about your employer (Company's Supplier), such as Supplier's name, the Supplier's primary contact person's name, telephone number and email address, the percentage of Company ownership in Supplier, whether Supplier is a Minority/Women Owned Enterprise (yes/no), whether Supplier has signed a Master Services Agreement ("MSA") with Company (yes/no, MSA Effective Date, MSA end date); and

(e) data about your Company Assignment Leader, such as his name, location, job title, Company function and/or organization, manager, and human resources manager.

3. Use of Personal Data.

There are many systems in which Company stores and processes personal data, which include but are not limited to: Single Sign On ("SSO") (access control for applications), eAdmin (access control for applications), Exchange 2000 (email servers), Global Address List (lookup directory for email system), Phonebook Application (directory assistance for company telephone numbers), Company Directory Initiative ("CDI") Database (master list of directory information), and the Standard Decision Support and Reporting Systems, (reporting on workforce utilization).

4. Sensitive Personal Data. Sensitive personal data refers to specific types of data that are treated as particularly sensitive, such as racial or ethnic origin, religion, criminal convictions, trade union membership and health data (collectively, "Sensitive Data"). Additional security and protection measures (e.g., physical security devices, restricted access) are provided for Sensitive Data. Company will obtain, where required by law, your explicit consent to the processing of any Sensitive Data about you.

5. Sharing Data with Third Parties. Company may provide certain data to third party providers of outsourced data processing. These third party providers will be allowed to process the data only in accordance with Company's instructions. Company will select reliable suppliers who undertake, by contract or equivalent means, to put in place appropriate security measures to ensure an adequate level of protection under your local data protection legislation. Company may also be required to disclose

certain of your personal data: (1) as a matter of law (e.g., to tax and social security authorities); (2) to protect Company's legal rights (e.g., to defend a litigation suit); or (3) in an emergency where the health or security of an employee or contingent worker is endangered (e.g., a fire).

6. Data Transfer Across National Boundaries. As Company operates internationally, we need to make your data available to Company offices outside of the nation where you reside, including the United States (where many of the centralized database servers are located) and other nations outside of the European Union. National laws vary regarding the level of protection for personal data, but Company will seek to ensure that the data has at least an adequate level of protection under your local data protection legislation.

7. Data Maintenance and Inquiries. You are permitted to inquire (at reasonable intervals) as to the nature of the personal data about you that is stored or processed about you by Company. You may also request access (through your Assignment Leader) to personal, factual information about you that is held by Company, subject to applicable legal requirements. In the event that any such data is inaccurate or out of date, you are entitled to request that the data be amended. If access or rectification is denied, the reason for the denial will be communicated and a written record will be made of the request and reason for denial. If you demonstrate that the purpose for which the data is being processed is no longer legal or appropriate, then the data will be deleted, unless the law requires otherwise. It is your responsibility to notify your Assignment Leader of any change in your personal data relevant to your assignment records (see for example the fields listed in Section 2 above), so that Company can maintain accurate contingent worker assignment records. Inquiries regarding the manner in which Company maintains your personal data can also be addressed to your Assignment Leader.

8. Storage. Personal data shall not be stored for longer than is reasonably necessary for the purposes detailed above, and Company will take adequate measures to ensure the security of the data.

9. Exemptions. Company is generally permitted under exemptions in local data protection legislation to process the personal data of contingent workers as reasonably necessary to the performance of its contracts, even without consent. However, to the extent that Company's processing does not fall within this exemption and in relation to (i) the transfer of your personal data across national boundaries and (ii) any processing of your sensitive data, your consent is requested so that such processing may be carried out.

CONSENT

I confirm that I have read and fully understand the provisions detailed above concerning the purposes for which personal data is required from me by Company and the way in which Company shall treat such data, and I consent to such processing.

Signed: _____

Date: _____

Name: _____

Employer: _____

SCHEDULE E

TRAVEL and LIVING POLICIES

Company will not reimburse any travel expenses unless such expenses are: (i) pre-approved in writing by Company; (ii) supported by documentation; and (iii) incurred in accordance with the guidelines set forth in this Agreement.

TRANSPORTATION

Air Travel

- Coach class is required for all reimbursable flights, regardless of destination.
- Supplier's Personnel may retain credits from frequent traveler programs. However, travel plans, routing requirements, etc., should not result in additional expense to Company nor require an increase in travel time during regularly assigned working hours.
- The cost of upgrading an airline ticket to another class is not reimbursable.

Reservations

- Make your own travel reservations and when possible schedule meetings to allow for travel during off-peak hours.
- Take the "best buy" airfare recommended by the agent.
- Book tickets as early as possible.
- Use teleconferencing and/or videoconferencing to minimize travel costs.
- Minimize number of employees taking same trip, e.g., to trade shows, conferences, etc.
- Consider non-refundable fare for frequent trips to the same location.
- Consider staying over on Saturday night to obtain lower airfare (Company will reimburse hotel and meal costs if the total cost is lower).
- **Ground Transportation**
- Use hotel/airport shuttle services when practical.
- Book smallest rental car practical for traveler's purpose.
- When using your personal vehicle, you will be reimbursed for mileage that qualifies as business mileage under the Internal Revenue Code.
- For New York airports private limos are not allowable expenses, except:
    - When traveling outside normal working hours (very early in the morning or late in the evening) or when there is a safety concern.
    - When there are at least two passengers and a private limo would be a lower cost option than other alternatives such as a rental car or scheduled limo service with Red Dot.
- From Fairfield use Hertz or Red Dot Limo Service.
- Minimize Company costs on rental cars by returning rental cars with a full tank of gas.
- **Living, Meals & Other Expenses**
- **Personal Meals**
- Meals are reimbursable provided you are on Company business away from your normal place of business with an overnight stay.
- On a day trip, meals eaten outside your regularly assigned work hours are reimbursable.
- **Other Reimbursables**
- Gratuities for bellhop, taxi, meals, etc.
- Highway tolls and parking fees.
- Laundry and dry cleaning services if the employee is away for five consecutive days.

- Telephone and fax expenses incurred on behalf of the Company, including essential calls to home.
- **Business Meals & Business Meetings**
- Costs for meetings, including meals, incurred in connection with provision of the Services are reimbursable, provided there is a legitimate business purpose for such meeting.
- Expense account must indicate date, time, place, business purpose and business relationship of attendees.
- Exercise good judgment.
- Expenses Not Reimbursable: The following items are considered to be of a personal nature, and therefore are not normally reimbursable by the Company.
- Airline club membership fees
- Clothing or toiletries, except if caused by airline delay or overbooking of airplane reservations
- Cost of a circuitous or side trip for personal convenience or benefit
- Fines for traffic violations
- Gifts of any type for Supplier's Personnel or their families
- Insurance on personal property; personal travel insurance
- Items for personal use, such as: hairstyling, shoe shine, magazines, newspapers, movies (including in-room movies), shows, and sporting events (unless for entertainment on behalf of the Company) and other similar items
- Loss or theft of personal property (e.g., clothes, jewelry, etc.), cash advance, personal funds or tickets
- Maintenance or repair of personal property (e.g., home and grounds) while out of town on Company business
- Parking or garage charges at the employee's regularly assigned place of business
- Personal credit card fees or charges incurred as a result of third-party misuse of lost credit cards
- Traveling expense between home and regularly assigned place of business
- **Unusual Expenses**
- In the event there are valid business reasons to incur expenses not reimbursable under these guidelines, these expenses may be reimbursed with appropriate Company approval.
- Review unusual circumstances with your Company contact in advance.

SCHEDULE F

SUPPLIER'S RESERVED INTELLECTUAL PROPERTY

_____

_____

_____

_____

_____

Approved by:

[GE-HITACHI NUCLEAR ENERGY AMERICAS LLC][GE-HITACHI NUCLEAR ENERGY INTERNATIONAL LLC][GE-Hitachi Global Laser Enrichment LLC]

By: _____

Name: _____

Title: _____

Date: _____

SCHEDULE G

GUIDELINES - THIRD PARTY SUPPLIERS

As a condition to providing Services pursuant to the Agreement, Supplier and Supplier's Personnel shall comply with applicable law and the following Guidelines:

1. **Source of Information.** During performance of the Agreement, Supplier and Supplier's Personnel may occasionally solicit or obtain competitive and market information from customers and suppliers of Company, and other non-competitive sources of information (e.g., architect-engineers, power brokers) and which is publicly disseminated (e.g., annual reports, investment banking analysis). However, Supplier and Supplier's Personnel shall not solicit or obtain competitive information from turbine-generator or energy product and services competitors of Company (including Company manufacturing associates and licensees), including with respect to:

-- prices
-- costs
-- product or service offerings
-- production or sales volume
-- production capacity
-- customer, consortium partner or supplier classification or selection
-- distribution methods or channels
-- terms or conditions of sale
-- profits or profit margins
-- market share
-- decisions to quote or not to quote
-- sales territories

2. **Multi-line or Competitor Distributors.** Supplier and Supplier's Personnel shall not solicit or obtain any competitive information from a multi-line or other distributor that represents a Company competitor.

3. **Government Procurement.** Supplier and Supplier's Personnel shall not solicit or obtain any information from a U.S. Federal, State or Foreign government agency, official or employee concerning a current procurement, whether pre-bid, post-bid, pre-award or post-award. Supplier and Supplier's Personnel may solicit or obtain historical and other publicly available information from a government agency, official or employee with the prior approval of Company counsel.

4. **Use of Agents or Representatives.** Supplier and Supplier's Personnel shall not use any agents or representatives to solicit or obtain information prohibited under these Guidelines.

5. **Competitor-Originated Documents.** Any Company competitor-originated documents obtained by Supplier and Supplier's Personnel during the performance of the Services shall be marked in a prominent location as follows:

"Received from (name of source organization)

Through (name of source individual) [with authority] {if appropriate}

On (date received)

By (name of recipient and component)"

6. **Retention of Records.** Supplier shall retain all files and records related to Services and competitor-originated documents obtained by Supplier during performance if the Services for a period of three (3) years following the Term of this Agreement. Supplier shall make such files, records and documents available during normal business hours to Company counsel upon request.

7. **Questions or Concerns.** If Supplier or Supplier's Personnel have any questions about these Guidelines or their obligations under the Agreement or concerns related to the performance of the Services with respect to these Guidelines, Supplierr shall promptly contact the cognizant Company manager or Company counsel.

SCHEDULE H

GE POWER & WATER INTEGRITY GUIDE FOR SUPPLIERS, CONTRACTORS AND CONSULTANTS

A Message from GE Power & Water

The General Electric Company and its GE Power & Water business ("GE") are committed to unyielding Integrity and high standards of business conduct in everything we do, especially in our dealings with suppliers, contractors and consultants of GE, its subsidiaries and affiliates (collectively "Suppliers"). For well over a century, GE people have created an asset of incalculable value: the company's worldwide reputation for integrity and high standards of business conduct. That reputation, built by so many people over so many years, depends on upholding it in each business transaction we make.

GE bases its Supplier relationships on lawful, efficient and fair practices, and expects its Suppliers to adhere to applicable legal and regulatory requirements in their business relationships, including those with their employees, their local environments, and GE. The quality of our Supplier relationships often has a direct bearing on the quality of our customer relationships. Likewise, the quality of our Suppliers' products and services affects the quality of our own products and services.

To help GE Suppliers understand both: (1) the GE commitment to unyielding Integrity and (2) and the standards of business conduct that all GE Suppliers must meet, GE has prepared this GE Power & Water Integrity Guide for Suppliers, Contractors and Consultants. Suppliers are expected to collaborate with GE's employees so that those employees can continue to consistently meet these GE integrity commitments.

The Guide is divided into four sections:

- GE Code of Conduct
- GE Compliance Obligations
- Responsibilities of GE Suppliers
- How to Raise an Integrity Concern

Suppliers should carefully review this Guide, including but not limited to the section entitled "Responsibilities of GE Suppliers." Suppliers are responsible for ensuring that they and their employees, workers, representatives and subcontractors comply with the standards of conduct required of GE Suppliers. Please contact the GE manager you work with or any GE Compliance Resource if you have any questions about this Guide or the standards of business conduct that all GE Suppliers must meet.

Steve Bolze, President & CEO
Jeffrey Connelly, Vice President, Global Supply Chain Chain Management

GE Code of Conduct

GE's commitment to total, unyielding Integrity is set forth in GE's compliance handbook, *The Spirit & The Letter*. The policies set forth in *The Spirit & The Letter* govern the conduct of all GE employees and are supplemented by compliance procedures and guidelines adopted by GE business components. All GE employees must not only comply with the "letter" of the Company's compliance policies, but also with their "spirit."

The "spirit" of GE's Integrity commitment is set forth in the GE Code of Conduct, which each GE employee has made a personal commitment to follow:

- Obey the applicable laws and regulations governing our business conduct worldwide.
- Be honest, fair and trustworthy in all of your GE activities and relationships.
- Avoid all conflicts of interest between work and personal affairs.
- Foster an atmosphere in which fair employment practices extend to every member of the diverse GE community.
- Strive to create a safe workplace and to protect the environment.
- Through leadership at all levels, sustain a culture where ethical conduct is recognized, valued and exemplified by all employees.

No matter how high the stakes, no matter how great the challenge, GE will do business only by lawful and ethical means. When working with customers and Suppliers in every aspect of our business, we will not compromise our commitment to integrity.

GE Compliance Obligations

All GE employees are obligated to comply with the requirements - the "letter" - of GE's compliance policies set forth in *The Spirit & The Letter*. These policies implement the GE Code of Conduct and are supplemented by compliance procedures and guidelines adopted by GE business components and/or affiliates. A summary of some of the key compliance obligations of GE employees follows:

IMPROPER PAYMENTS

- Always adhere to the highest standards of honesty and integrity in all contacts on behalf of GE. Never offer bribes, kickbacks, illegal political contributions or other improper payments to any customer, government official or third party. Follow the laws of the United States and other countries relating to these matters.
- Do not give gifts or provide any entertainment to a customer or supplier without prior approval of GE management. Make sure all business entertainment and gifts are lawful and disclosed to the other party's employer.
- Employ only reputable people and firms as GE representatives and understand and obey any requirements governing the use of third party representatives.

INTERNATIONAL TRADE CONTROLS

• Understand and follow applicable international trade control and customs laws and regulations, including those relating to licensing, shipping and import documentation and reporting, and record retention requirements.
• Never participate in boycotts or other restrictive trade practices prohibited or penalized under United States or applicable local laws.
• Make sure all transactions are screened in accordance with applicable export/import requirements; and that any apparent conflict between U.S. and applicable local law requirements, such as the laws blocking certain U.S. restrictions adopted by Canada, Mexico and the members of the European Union, is disclosed to GE counsel.

MONEY LAUNDERING PREVENTION

• Follow all applicable laws that prohibit money laundering and that require the reporting of cash or other suspicious transactions.
• Learn to identify warning signs that may indicate money laundering or other illegal activities or violations of GE policies. Raise any concerns to GE counsel and GE management.

PRIVACY

• Never acquire, use or disclose individual information in ways that are inconsistent with GE privacy policies or with applicable privacy and data protection laws, regulations and treaties.
• Maintain secure business records of information, which is protected by applicable privacy regulations, including computer-based information.

SUPPLIER RELATIONSHIPS

• Only do business with suppliers who comply with local and other applicable legal requirements and any additional GE standards relating to labor, environment, health and safety, intellectual property rights and improper payments.
• Follow applicable laws and government regulations covering supplier relationships.
• Provide a competitive opportunity for suppliers to earn a share of GE's purchasing volume, including small businesses and businesses owned by the disadvantaged, minorities and women.

REGULATORY EXCELLENCE

• Be aware of the specific regulatory requirements of the country and region where the work is performed and that affect the GE business.
• Gain a basic understanding of the key regulators and the regulatory priorities that affect the GE business.
• Promptly report any red flags or potential issues that may lead to a regulatory compliance breach.
• Always treat regulators professionally and with courtesy and respect.
• Assure that coordination with business or corporate experts is sought when working with or responding to requests of regulators.

WORKING WITH GOVERNMENTS

• Follow applicable laws and regulations associated with government contracts and transactions.
• Be truthful and accurate when dealing with government officials and agencies.
• Require any supplier or subcontractor providing goods or services for GE on a government project or contract to agree to comply with the intent of GE's Working with Governments policy and applicable government contract requirements.
• Do not do business with suppliers or subcontractors that are prohibited from doing business with the government.
• Do not engage in employment discussions with a government employee or former government employee without obtaining prior approval of GE management and counsel.

COMPLYING WITH COMPETITION LAWS

• Never propose or enter into any agreement or understanding with a GE competitor to fix prices, terms and conditions of sale, costs, profit margins or other aspects of the competition for sales to third parties.
• Do not propose or enter into any agreements or understandings with GE customers restricting resale prices.
• Never propose or enter into any agreements or understandings with suppliers that restrict the price or other terms at which GE may resell or lease any product or service to a third party.

ENVIRONMENT, HEALTH & SAFETY

• Conduct your activities in compliance with all relevant environmental and worker health and safety laws and regulations and conduct your activities accordingly.
• Ensure that all new product designs or changes or service offerings are reviewed for compliance with GE guidelines.
• Use care in handling hazardous materials or operating processes or equipment that use hazardous materials to prevent unplanned releases into the workplace or the environment.
• Report to GE management all spills of hazardous materials; any concern that GE products are unsafe; and any potential violation of environmental, health or safety laws, regulations or company practices or requests to violate established EHS procedures.

FAIR EMPLOYMENT PRACTICES

• Extend equal opportunity, fair treatment and a harassment-free work environment to all employees, co-workers, consultants and other business associates without regard to their race, color, religion, national origin, sex (including pregnancy), sexual orientation, age, disability, veteran status or other characteristic protected by law.

SECURITY AND CRISIS MANAGEMENT
• Implement rigorous plans to address security of employees, facilities, information, IT assets and business continuity.
• Protect access to GE facilities from unauthorized personnel.
• Protect IT assets from theft or misappropriation.
• Create and maintain a safe working environment.
• Ensure proper business continuity plans are prepared for emergencies.
• Screen all customers, suppliers, agents and dealers against terrorist watchlists.
• Report any apparent security lapses.
CONFLICTS OF INTEREST
• Financial, business or other non-work related activities must be lawful and free of conflicts with one's responsibilities to GE.
• Report all personal or family relationships, including those of significant others, with current or prospective suppliers you select, manage or evaluate.
• Do not use GE equipment, information or other property (including office equipment, email and computer applications) to conduct personal or non-GE business without prior permission from the appropriate GE manager.
CONTROLLERSHIP
• Keep and report all GE records, including any time records, in an accurate, timely, complete and confidential manner. Only release GE records to third parties when authorized by GE.
• Follow GE's General Accounting Procedures ("GAP"), as well as all generally accepted accounting principles, standards, laws and regulations for accounting and financial reporting of transactions, estimates and forecasts.
• Financial statements and reports prepared for or on behalf of GE (including any component or business) must fairly present the financial position, results of operations and/or other financial data for the periods and/or the dates specified.
INSIDER TRADING OR DEALING & STOCK TIPPING
• Never buy, sell or suggest to someone else that they should buy or sell stock or other securities of any company (including GE) while you are aware of significant or material non-public information ("inside information") about that company. Information is significant or material when it is likely that an ordinary investor would consider the information important in making an investment decision.
• Do not pass on or disclose inside information unless lawful and necessary for the conduct of GE business - and never pass on or disclose such information if you suspect that the information will be used for an improper trading purpose.
INTELLECTUAL PROPERTY
• Identify and protect GE intellectual property in ways consistent with the law.
• Consult with GE counsel in advance of soliciting, accepting or using proprietary information of outsiders, disclosing GE proprietary information to outsiders or permitting third parties to use GE intellectual property.
• Respect valid patents, trademarks, copyrighted materials and other protected intellectual property of others; and consult with GE counsel for licenses or approvals to use such intellectual property.

Responsibilities of GE Suppliers

GE will only do business with Suppliers that comply with all applicable legal and regulatory requirements. Today's regulatory environment is becoming more challenging, subjecting GE and its Suppliers to a growing number of regulations and enforcement activities around the world. This environment requires that GE and its Suppliers continue to be knowledgeable about and compliant with all applicable regulations and committed to regulatory excellence. Suppliers that transact business with GE are also expected to comply with their contractual obligations under any purchase order or agreement with GE and to adhere to the standards of business conduct consistent with GE's obligations set forth in the "GE Compliance Obligations" section of this Guide and to the standards described in this section of the Guide. A Supplier's commitment to full compliance with these standards and all applicable laws and regulations is the foundation of a mutually beneficial business relationship with GE.

GE expects its Suppliers, and any Supplier's subcontractors, that support GE's work with government customers to be truthful and accurate when dealing with government officials and agencies, and adhere strictly to all compliance obligations relating to government contracts that are required to flow down to GE's suppliers.

As stated above, GE requires and expects each GE Supplier to comply with all applicable laws and regulations. Unacceptable practices by a GE Supplier include:

• Minimum Age. Employing workers younger than sixteen (16) years of age or the applicable required minimum age, whichever is higher.
• Forced Labor. Using forced, prison or indentured labor or workers subject to any form of compulsion or coercion or trafficking in persons in violation of the U.S. Government's zero tolerance policy or other applicable laws or regulations.
• Environmental Compliance. Lack of commitment to observing applicable environmental laws and regulations. Actions that GE will consider evidence of a lack of commitment to observing applicable environmental laws and regulations include:
— Failure to maintain and enforce written and comprehensive environmental management programs, which are subject to periodic audit.
— Failure to maintain and comply with all required environmental permits.

— Permitting any discharge to the environment in violation of law or issued/required permits or that would otherwise have an adverse impact on the environment.
• Health & Safety. Failure to provide workers a workplace that meets applicable health, safety and security standards.
• Human Rights.
— Failure to respect human rights of Supplier's employees.
— Failure to observe applicable laws and regulations governing wage and hours.
— Failure to allow workers to freely choose whether or not to organize or join associations for the purpose of collective bargaining as provided by local law or regulation.
— Failure to prohibit discrimination, harassment and retaliation.
— Failure to adopt policies and establish systems to procure tantalum, tin, tungsten, and gold from sources that have been verified as conflict free, or to provide supporting data on your supply chain for tantalum, tin, tungsten, and gold to GE when requested, on a platform to be designated by GE.
• Code of Conduct. Failure to maintain and enforce GE policies requiring adherence to lawful business practices, including a prohibition against bribery of government officials.
• Business Practices and Dealings with GE. Offering or providing, directly or indirectly, anything of value, including cash, bribes, gifts, entertainment or kickbacks, to any GE employee, representative or customer or to any government official in connection with any GE procurement, transaction or business dealing. Such prohibition includes the offering or providing of any consulting, employment or similar position by a Supplier to any GE employee (or their family member or significant other) involved with a GE procurement. GE also prohibits a GE Supplier from offering or providing GE employees, representatives or customers or any government officials with any gifts or entertainment, other than those of nominal value to commemorate or recognize a particular GE Supplier business transaction or activity. In particular, a GE Supplier shall not offer, invite or permit GE employees and representatives to participate in any Supplier or Supplier-sponsored contest, game or promotion.
• Business Entertainment of GE Employees and Representatives. Failure to respect and comply with the business entertainment (including travel and living) policies established by GE and governing GE employees and representatives. A GE Supplier is expected to understand the business entertainment policies of the applicable GE business component or affiliate before offering or providing any GE employee or representative any business entertainment. Business entertainment should never be offered to a GE employee or representative by a Supplier under circumstances that create the appearance of an impropriety.
• Collusive Conduct and GE Procurements. Sharing or exchanging any price, cost or other competitive information or the undertaking of any other collusive conduct with any other third party to GE with respect to any proposed, pending or current GE procurement.
• Intellectual Property and Other Data and Security Requirements. Failure to respect the intellectual and other property rights of others, especially GE. In that regard, a GE Supplier shall:
— Only use GE information and property (including tools, drawings and specifications) for the purpose for which they are provided to the Supplier and for no other purposes.
— Take appropriate steps to safeguard and maintain the confidentiality of GE proprietary information, including maintaining it in confidence and in secure work areas and not disclosing it to third parties (including other customers, subcontractors, etc.) without the prior written permission of GE.
— If requested by GE, only transmit information over the Internet on an encrypted basis.
— Observe and respect all GE patents, trademarks and copyrights and comply with such restrictions or prohibitions on their use as GE may from time-to-time establish.
— Comply with all applicable rules concerning cross-border data transfers.
— Maintain all personal and sensitive data, whether of GE employees or its customers in a secure and confidential manner, taking into account both local requirements and the relevant GE policies provided to the Supplier.
• Trade Controls & Customs Matters. The transfer of any GE technical information to any third party without the express, written permission of GE. Failure to comply with all applicable trade control laws and regulations in the import, export, re-export or transfer of goods, services, software, technology or technical data including any restrictions on access or use by unauthorized persons or entities, and failure to ensure that all invoices and any customs or similar documentation submitted to GE or governmental authorities in connection with transactions involving GE accurately describe the goods and services provided or delivered and the price thereof.
• Use Of Subcontractors or Third Parties to Evade Requirements. The use of subcontractors or other third parties to evade legal requirements applicable to the Supplier and any of the standards set forth in this Guide.
The foregoing standards are subject to modification at the discretion of GE. Please contact the GE manager you work with or any GE Compliance Resource if you have any questions about these standards and/or their application to particular circumstances. Each GE Supplier is responsible for ensuring that its employees and representatives understand and comply with these standards. GE will only do business with those Suppliers that comply with applicable legal and regulatory requirements and reserves the right, based on its assessment of information available to GE, to terminate, without liability to GE,

any pending purchase order or contract with any Supplier that does not comply with the standards set forth in this section of the Guide.

How to Raise an Integrity Concern

Subject to local laws and any legal restrictions applicable to such reporting, each GE Supplier is expected to promptly inform GE of any Integrity concern involving or affecting GE, whether or not the concern involves the Supplier, as soon as the Supplier has knowledge of such Integrity concern. A GE Supplier shall also take such steps as GE may reasonably request to assist GE in the investigation of any Integrity concern involving GE and the Supplier.

I. Define your concern: Who or what is the concern? When did it arise? What are the relevant facts?

II. Prompt reporting is crucial - an Integrity concern may be raised by a GE Supplier as follows:

- By discussing it with a cognizant GE Power & Water Manager;
- By calling the GE Power & Water Integrity Helpline at +1-800-443-1391 or +1-678-844-4967 or the GE Corporate Integrity Helpline at +1 800 227 5003 or +1-203-373-2603;
- By emailing ombudsperson@corporate.ge.com; or
- By contacting any Compliance Resource (e.g., GE legal counsel or auditor). A GE Compliance Resource will promptly review and investigate the concern.

III. GE Policy forbids retaliation against any person reporting an Integrity concern.

SCHEDULE I

COMPANY PRIVACY AND DATA PROTECTION

This Schedule governs whenever a Supplier Processes Company Data, including Personal Data, Sensitive Personal Data, or Company Restricted Data, or has access to a Company Information System in connection with the relevant Contract Document (as those terms are defined below). In the event of any inconsistency or conflict between this Schedule and the Contract Document with respect to a subject covered by this Schedule, the provision requiring the higher level of protection for Company Data shall prevail. The requirements in this Schedule are in addition to any confidentiality obligations between Company and the Supplier under the Contract Document. Capitalized terms used in this Schedule without definition shall have the meanings set forth in the Company Master Services Agreement of which this Schedule forms a part ("**MSA**").

PART A: DEFINITIONS

(i) ***Affiliate***, if not defined in the Contract Document, with respect to either party, shall mean any entity (including but not limited to, joint ventures, corporations, limited liability companies, partnerships, limited partnerships, business trusts or other entities, subsidiaries, businesses, operating divisions, units thereof) that is directly or indirectly in control of, controlled by, or under common control with such party whether now existing, or subsequently created or acquired during the Term of the Contract Document.

(ii) ***Contract Document,*** as used in this Schedule, means the MSA and the relevant SOW or PO governing the provision of services and/or deliverables by Supplier to Company.

(iii) ***Controlled Data*** is technical information with distribution and/or handling requirements proscribed by law or regulation, including but not limited to sensitive but unclassified government data and license required export controlled data. Controlled Data shall be subject to the same controls specified below for Company Restricted Data.

(iv) ***Company*** has the meaning set forth in the MSA.

(v) ***Company Data*** is any Company or its Affiliate's Confidential Information, as defined in the Contract Document that is Processed in connection with performance of the Contract Document. For clarity, Personal Data, Sensitive Personal Data, Controlled Data and Company Restricted Data are Company Data.

(vi) ***Company Information System(s)*** means any systems and/or computers managed by Company, which includes laptops and network devices.

(vii) ***Company Restricted Data*** is information that Company or its Affiliate identifies as 'restricted data' in the Contract Document, or at the time of disclosure that Company identifies as "Restricted," "Highly Confidential," or similar in connection with performance of the Contract Document. Company Restricted Data, includes, but is not limited to:

- Critical business information, including details of mergers, acquisitions or dispositions; financial results prior to public reporting; and security vulnerability information relating to Company Information Systems and/or products, and
- Critical technical information, including computer source code; non-public invention disclosure and/or patent data.

(viii) ***Highly Privileged Accounts, or HPAs***, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

(ix) ***Mobile Devices*** means tablets and smartphones running mobile operating systems (e.g., iOS, Blackberry OS, Android, or Windows Mobile operating systems). Laptops are not considered to be Mobile Devices.

(x) ***Personal Data*** is a category of Company Data that includes any information that relates to an identified or identifiable natural person ("Data Subject"), as such relation is defined under applicable law or regulation. Legal entities are Data Subjects where required by law or regulation.

(xi) ***Process or Processing*** means to perform any operation or set of operations upon Company Data, whether or not by automatic means, including but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

(xii) ***Security Incident*** is any actual or suspected event in which Company Data is or may have been lost, stolen, improperly altered, improperly destroyed, used for a purpose not permitted under the Contract Document or this Schedule, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this Schedule.

(xiii) ***Security Notices*** are any written communications, notices, filings, press releases, or reports related to any Security Incident.

(xiv) ***Sensitive Personal Data*** is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information ("PHI") subject to the

U.S. Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated under that Act (collectively, "HIPAA"), and/or any medical, demographic, visual or descriptive information that can be used to identify a particular patient/individual under HIPAA or other similar law and regulations; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special data categories of data under applicable data protection law (such as race, nationality, political opinions, trade union membership, home life, and sexual orientation). Sensitive Personal Data shall be subject to the same controls specified below for Company Restricted Data.

(xv) ***Supplier*** has the meaning set forth in the MSA.

(xvi) ***Supplier Information System(s)*** means any Supplier systems and/or computers used to Process Company Data pursuant to the Contract Document, which includes laptops and network devices.

(xvii) ***Supplier Personnel*** means "Supplier's Personnel", as such term is defined in the MSA.

NOTE: Parts B-E and I-K apply to all Suppliers that Process any Company Data.

PART B: COLLECTING, PROCESSING AND SHARING COMPANY DATA

Supplier shall implement appropriate organizational, technical, and physical measures and controls to protect and ensure the security and confidentiality of Company Data to prevent accidental, unauthorized or unlawful destruction, alteration, unauthorized disclosure or access, modification or loss of Company Data; misuse of Company Data; and unlawful Processing of Company Data. Supplier is responsible for compliance with all terms of the Contract Document and this Schedule by Supplier Personnel and for following Company or the applicable Company Affiliate's instructions concerning the Processing of Company Data. Organizational security controls shall include the following at a minimum:

1. Supplier and Supplier Personnel shall Process Company Data, and access and use Company Information Systems, only on a need-to-know basis and only to the extent necessary to perform services under the Contract Document or as otherwise instructed by Company or the applicable Company Affiliate in writing.
2. Prior to providing access to any Company Data to any Supplier Personnel, Supplier must obligate them to comply with the level of security required in the Contract Document and this Schedule and verify such compliance through an appropriate due diligence process. Unless otherwise agreed upon in the Contract Document, Supplier must obtain Company's prior written approval to provide access to any Company Data to any of its own suppliers or subcontractors or agents that were not pre-qualified by or otherwise disclosed to Company in writing prior to Supplier's performance of services under the Contract Document. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel, with this Schedule and shall remain responsible at all times for their compliance.
3. Supplier must maintain formal written policies and procedures for the administration of information security throughout its organization consistent with the requirements of this Schedule.
4. Supplier Personnel with access to Company Data must participate in appropriate information security awareness training provided by the Supplier prior to obtaining access to Company Data and thereafter on at least an annual basis while such personnel have access to Company Data.
5. Supplier shall maintain a current inventory of Supplier Information Systems.
6. Supplier must ensure each account (including Company assigned accounts) through which Company Data may be accessed is attributable to a single individual with a unique ID (not shared) and each account must require authentication (e.g., password) prior to accessing Company Data.
7. Supplier shall undertake reasonable measures to terminate Supplier Personnel access to Company Data, whether physical or logical, no later than the date of personnel separation or personnel transfer to a role no longer requiring access to Company Data; where Supplier Personnel have been assigned Company SSO credentials, Supplier must notify Company of any such separation or transfer no later than the day of that event.
8. Company Data shall not be Processed on personal accounts (e.g., individual email or cloud services accounts (e.g., Gmail, Yahoo, Dropbox, Google Drive)) or on personally-owned computers, devices or media.
9. Unless prohibited by applicable law or regulation, Supplier shall notify Company promptly and act only upon Company's instruction concerning any request by a third party, including without limitation law enforcement, governmental authority, or in connection with litigation or other court process for disclosure of Company Data or for information concerning the Processing of Company Data in connection with the Contract Document or this Schedule, as well as any

request received from an individual concerning his/her Personal Data.

10. Technical security controls on Supplier Information Systems shall include the following at a minimum:

    (a) Supplier must use strong passwords consistent with technology industry practices, including minimum password length, lockout, expiration period, complexity, encryption, changing of default passwords, and usage of temporary passwords. User account credentials (e.g., login ID, password) must not be shared.

    (b) Supplier must implement and maintain controls to detect and prevent unauthorized access, intrusions and computer viruses and other malware. At a minimum such controls must include network layer security devices (e.g. firewalls and intrusion detection/prevention systems), client and server-side antivirus programs that include up-to-date antivirus definitions, and installation into production of all critical patches or security updates as soon as possible, but not later than thirty (30) days from the release of any such updates or patches.

    (c) Supplier must maintain documented change management procedures that provide a consistent approach for controlling, implementing and documenting changes (including emergency changes) for Supplier Information Systems that includes appropriate segregation of duties.

    (d) Unless otherwise expressly agreed in the Contract Document, development and testing environments must be physically and/or logically separated from production environments and must not contain Company Data unless specified in the Contract Document. Production changes must be approved by the Supplier's appropriate system owner, as such person is designated in the Contract Document, and such changes must not be made by any Supplier developers.

    (e) Any back-up media containing Company Data stored at Supplier's site must be kept in a secure location (e.g., locked office or locked file cabinet) and be encrypted to a standard consistent with industry practice. If off-site media storage is used, Supplier must have a media check-in/check-out process with locked storage for transportation. Back-up information must be given the same level of physical and environmental protection as the level of control applied at the main site.

    (f) Workstations must not be left authenticated when unattended and must be password or PIN protected when not in use. An inactivity lock must be implemented on workstations.

    (g) Network layer security devices must allow only authorized connections and rule sets must be reviewed at minimum semi-annually.

    (h) Mobile Devices used to Process Company Data (including emails) must have strong mobile device security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

11. Physical security controls shall include the following at a minimum on all Supplier facilities where Company Data may be Processed:

    (a) Physically secure perimeters and external entry points must be suitably protected against unauthorized access (e.g. barriers such as walls, card controlled entry gates). Access to all locations must be limited to Supplier Personnel and authorized visitors only. Reception areas must be manned or have other means to control physical access.

    (b) Visitors must be required to sign a visitors register (maintained for at least one year) and be escorted or observed at all times, upon each entry to and exit from the premises.

    (c) A clear desk policy must be enforced throughout the Supplier facilities. Documents that contain Company Data must be kept secured (e.g. locked office or file cabinet) when not in use.

PART C: SECURITY INCIDENTS

1. Security Incidents on Supplier Information Systems must be logged, reviewed on a periodic basis (minimum quarterly), secured, and maintained for a minimum of twelve (12) months.

2. Supplier must develop and maintain an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents and perform any required recovery actions to remedy the impact.

3. Supplier shall notify Company within a reasonable period, in no event to exceed seventy-two (72) hours after discovery, or shorter if required by applicable law or regulation, of any Security Incident experienced by Supplier involving any Company Data. Supplier shall report any Security Incidents to the Cyber Incident Response Team at gecirt@ge.com or 1-800-4GE-CIRT, or at such contact information communicated to Supplier from time to time. Supplier shall reasonably cooperate with Company in its investigation of an incident, whether discovered by Supplier, Company, or a third party, which shall include providing Company a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, the identity of each affected person, and any other information Company reasonably may request concerning such affected persons and the details of the Security Incident, as soon as such information can be collected or otherwise becomes available. Supplier shall designate an individual responsible for management of the Security Incident, and shall identify such individual to Company promptly.
4. If requested by Company or its Affiliate, and at Company's direction, Supplier shall send Security Notices regarding a Security Incident. Unless prohibited by applicable law or regulation, Supplier shall provide Company or its Affiliate with reasonable notice of, and the opportunity to comment on and approve, the content of such Security Notices prior to any publication or communication thereof to any third party, except neither Company nor its Affiliate shall have the right to reject any content in a Security Notice that must be included in order to comply with applicable law or regulation. Should Company or its Affiliate elect to send a Security Notice regarding a Security Incident, Supplier shall provide all reasonable and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.
5. Other than approved Security Notices, or to law enforcement or as otherwise required by law or regulation, Supplier may not make or permit any public statements concerning Company's involvement with any such Security Incident to any third-party without the explicit written authorization of Company's Legal Department.

PART D: AUDITS

Supplier responsibilities:

1. Supplier shall monitor the effectiveness of its security program by conducting self-audits and risk assessments of Supplier Information Systems against the requirements of written policies and procedures maintained as required by this Schedule no less frequently than every twelve (12) months. Supplier shall be responsible for ensuring consistency of its security operations, including proactive monitoring and mitigation of all vulnerabilities across all of its sites.
2. Upon request, Supplier must provide to Company formal reports of any audits and assessments conducted on Supplier Information Systems, which shall include, at a minimum, the scope of the audit and/or assessment and any vulnerabilities/issues/findings/concerns/recommendations in so far as they impact Company Data. Such formal reports provided by Supplier to Company shall be treated as confidential.
3. Supplier must use commercially reasonable efforts to remediate within thirty (30) days any items rated as high or critical (or similar rating indicating similar risk) in any audits or assessments of Supplier Information Systems.
4. Company audit rights:
   (a) Upon request, with reasonable advance notice and conducted in such a manner not to unduly interfere with Supplier's operations, Company reserves the right to conduct an audit of Supplier's compliance with the requirements in this Schedule relating to Company Data including but not limited to: (i) a review of Supplier's applicable policies, processes, and procedures, (ii) a review of the results of Supplier's most recent vulnerability assessment (e.g., application vulnerability scanning, penetration testing, and similar testing results) and accompanying remediation plans, and (iii) on-site assessments of Supplier's physical security arrangements and Supplier Information Systems during Supplier's regular working hours that will not unreasonably interfere with Supplier's operations, pursuant to a mutually agreeable audit plan. Company reserves the right to conduct an onsite audit of Supplier on thirty (30) days prior written notice during regular business hours. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes Company Data provided under the Contract Document. Supplier agrees to cooperate fully with Company or its designee during such audits and shall provide access to facilities, appropriate resources, provide applicable supporting documentation to Company, and complete security assessment questionnaires that may be requested.
   (b) Company acknowledges and agrees that nothing in Section D4 above shall oblige Supplier to divulge any information relating to its other

customers to Company in such a manner that may put Supplier in breach of its obligations of confidentiality to such customers or any other legal requirements.

(c) Subject to the confidentiality provisions of the Contract Document, Company or its representative may review, audit, monitor, intercept, access and, disclose any information provided by Supplier that is Processed or stored on Company Information Systems or on Company Mobile Devices accessing the Company network.

PART E: REGULATORY REQUIREMENTS

In the event Supplier Processes Company Data that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with Company to comply with such requirements. Such cooperation may include, without limitation:

1. Execution of additional agreements required by applicable law or regulation.
2. Implementation of additional security controls required by applicable law (e.g. Department of Defense FAR Supplement (cross referencing NIST), U.S. Federal Information Security Management Act (FISMA), HIPAA, US Sarbanes-Oxley Act, U.S. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) Section 501(b) Standards for Securing Customer Information, Payment Card Industry Data Security Standards (PCI DSS) security requirements, Federal Financial Institutions Examination Council (FFIEC) guidance).
3. Completion of regulatory filings applicable to Supplier.
4. Completion of required regulatory audits (e.g., U.S. Food and Drug Administration (FDA), central banks such as the U.S. Federal Reserve).

NOTE: Part F applies to any Supplier that Processes Personal Data (including Sensitive Personal Data)

PART F: PERSONAL DATA

1. Unless and except to the extent expressly provided in the Contract Document, Supplier must, in each case, seek and obtain Company's prior written approval regarding the scope of any Personal Data to be collected directly by Supplier, as well as any notices to be provided and any consent language to be used when collecting such information from a Data Subject. In the case of Personal Data collected directly from Data Subjects by Supplier, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access and correction/deletion.
2. Supplier warrants and represents that it shall comply with all applicable laws and regulations applicable to Supplier's activities concerning Personal Data governed by this Schedule, including those concerning notice and consent, onward transfer to a third party, and international transfer, and shall act only on Company's written instruction concerning any such transfers. Supplier must receive approval from Company prior to (i) moving Personal Data from its Company-approved hosting jurisdiction to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than the hosting jurisdiction or other Company-approved jurisdiction.
3. Encryption must be implemented in any of the following instances: (i) any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing Personal Data must be encrypted at rest; and/or (ii) transferring Personal Data over public networks (such as the Internet). In either case, Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.
4. In the event Supplier Processes Personal Data that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with Company to comply with such requirements.

NOTE: Part G applies to Suppliers that Process Sensitive Personal Data, Controlled Data, and/or Company Restricted Data. The requirements of this Part G are in addition to all other applicable requirements of Parts A through F above. References to Company Restricted Data in this Part G shall be deemed to also refer to Sensitive Personal Data and/or Controlled Data as the context requires.

PART G: PROTECTING COMPANY RESTRICTED DATA, CONTROLLED DATA, AND SENSITIVE PERSONAL DATA

1. Supplier must have an IT security organization with clearly defined information security roles, responsibilities and accountability.
2. Supplier must perform vulnerability assessments on Supplier Information Systems at least annually. For Supplier Information Systems that are internet facing, Supplier must engage an independent external party to perform the vulnerability assessment and shall remediate as required in Part D.3.

3. Supplier Information Systems consisting of networks used to access or store Company Restricted Data must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention Systems (IDS/IPS) in a risk based manner (e.g., between the Internet and DMZ, and between DMZ and internal servers containing Company Restricted Data). IDS/IPS high and critical priority alerts must be continuously monitored and responded to as soon as reasonably practicable.
4. Any Supplier Personnel accessing Supplier's internal network remotely must be authenticated using a minimum two-factor authentication method and such transmissions must be encrypted at a level consistent with industry standards.
5. Supplier must have or implement hardening and configuration requirements consistent with industry practices.
6. Supplier must have or implement appropriate data loss prevention ("DLP") controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of Company Restricted Data from Supplier Information Systems.
7. Supplier must implement processes to support the secure creation, modification, and deletion of these accounts and any HPAs. Supplier must review and update access rights at least annually, and at least quarterly for HPAs. HPA usage must be reviewed at minimum weekly. All HPA access must be established using encrypted mechanisms (e.g., secure shell).
8. Supplier must use an auditable process (e.g., certification of destruction) to remove Company Restricted Data from Supplier Information Systems prior to disposal or re-use in a manner that ensures that the Company Restricted Data may not be accessed or readable.
9. Encryption must be implemented in any of the following instances: (i) any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing Company Restricted Data must be encrypted at rest; (ii) where technically feasible, Company Restricted Data must be stored in encrypted form, except where encryption is mandatory in such cases as set forth above; and/or (iii) transferring Company Restricted Data over public networks (such as the Internet).
10. Where encryption is required, Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.
11. Supplier Information Systems consisting of servers and/or network equipment used to store or access Company Restricted Data must be kept in a secure room containing additional access control mechanisms, located on the interior of the building with no windows unless safeguards are in place to prevent shattering and unauthorized entry. Telecommunications equipment, cabling and relays receiving data or supporting services must be protected from interception or damage.
12. Physical access must be monitored, recorded and controlled with physical access rights reviewed at minimum annually. Physical access logs detailing access must be stored for a period of one (1) year unless prohibited by local law. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained for at least thirty (30) days.
13. Supplier must receive approval from Company prior to moving Company Restricted Data from its Company-approved physical location or jurisdiction to a different physical location or jurisdiction.

NOTE: Unless otherwise provided for in the Contract Document, Part H applies to any Supplier Information System (i) that Processes Company Restricted Data, Controlled Data, and/or Sensitive Personal Data, and/or (ii) where an outage of the Supplier Information System(s), as identified in the Contract Document, is likely to significantly adversely impact Company or overall Company operations, financial position, regulatory compliance, and/or reputation.

PART H: DISASTER RECOVERY

Unless a disaster recovery ("DR") program is otherwise set forth in more detail elsewhere in the Contract Document, Supplier must maintain a DR program for all Supplier Information Systems and facilities used to provide services under the Contract Document to Company. The DR program must be designed to ensure that Supplier has a methodology by which a system can continue to function through an operational interruption or disaster. At a minimum, the DR program should include the following elements:

1. Supplier's operational procedures must verify the successful completion of backups and the backup media must be tested regularly (at minimum quarterly) to ensure that it will operate in the event of an emergency.
2. For rooms containing Supplier Information Systems consisting of servers and/or network equipment used to provide services to Company, controls must be implemented to mitigate the risk of power failures (e.g.,

surge protectors, uninterruptible power supplies, and generators), and environmental conditions (e.g., temperature and humidity).

3. Supplier must maintain inventories that list all critical Supplier Information Systems. The inventories must be updated at minimum annually.
4. DR plans must be developed for all Supplier Information Systems and facilities that are used to provide services to Company and reviewed/approved at minimum annually.
5. Supplier must conduct full scale DR tests annually against DR plans (unless otherwise agreed with Company) for Supplier Information Systems that Supplier reasonably believes are critical for providing services to Company to ensure that such Supplier Information Systems can be recovered in a manner that meets the contractual service levels specified in the Contract Document. DR results must be documented and provided to Company upon request.

PART I: TERMINATION

1. Subject to Part I.2 below and to any provision of the Contract Document to the contrary, Supplier shall within 30 (thirty) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of Company Data and shall return to Company all copies and reproductions of such Company Data. In lieu of returning copies and reproductions, Company may, at its sole discretion, require Supplier to destroy, using agreed upon methods to ensure such Company Data is not recoverable, all copies and reproductions of Company Data provided to, developed by, or used by Supplier in the performance of services under the Contract Document and certify to such destruction.
2. Company acknowledges that due to its standard back-up procedures and/or a requirement of certain laws/regulations to which Supplier is subject, Supplier may be required to maintain copies and/or back-up copies of Company Data (including as part of records, documents or broader data sets) beyond the period described in Part I.1. In such cases, notwithstanding the requirements of Part I.1, Company agrees that Supplier may continue to retain such Company Data in copies and/or back-up copies beyond the period prescribed in Part I.1 provided that (i) Supplier notifies Company prior to the Contract Document's effective date of termination or expiration (whichever the case may be) and the specific laws/regulations mandating such retention; (ii) Supplier has a documented retention period and secure deletion procedure for such copies and back-up copies, with back-up copies retained no longer than 6 (six) months from the date on which they were captured, and legally required copies retained only to the end of their legally required retention period; (iii) such copies and back-up copies shall be deleted in accordance with such documented procedure; (iv) Supplier shall perform no Processing of Company Data other than that necessitated by retaining or deleting the relevant copies and back-up copies; and (v) Supplier shall continue to comply with all the requirements of this Schedule in relation to any such retained Company Data until the same is securely deleted.
3. Termination or expiration of the Contract Document, for any reason, shall not relieve the Supplier from obligations to continue to protect Company Data against the impermissible disclosure in accordance with the terms of the Contract Document and this Schedule.

Part J: Material Breach

1. Notwithstanding anything to the contrary herein or in the Contract Document, Supplier's (including Supplier Personnel) failure to comply with the obligations set forth in this Schedule also constitutes a material breach of the Contract Document, with such rights and remedies set forth therein or under applicable law and regulation.
2. Company or the applicable Company Affiliate owning any of the Company Data being accessed pursuant to the Contract Document may enforce the terms of this Schedule as permitted or required by applicable law and regulation.
3. Supplier shall pay for or reimburse Company or the applicable Company Affiliate for all costs, losses and expenses relating to any Security Incident experienced by Supplier, including without limitation, costs of forensic assessments, Security Notices, credit monitoring or other fraud alert services, and all other remedies either required by applicable law and regulation or which are customary in the industry or required under Company's then-current policies or contractual commitments.

PART K: MISCELLANEOUS

Supplier understands and agrees that Company or its Affiliate may require Supplier to provide certain personal information such as the name, address, telephone number, and e-mail address of Supplier's representatives in transactions to facilitate the performance of the Contract Document, and that Company, its Affiliates, and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of

the Contract Document, including but not limited to Supplier payment administration. Company or the applicable Company Affiliate will be the Controller of this data for legal purposes, and agrees to use reasonable technical and organizational measures to ensure that such information is processed in conformity with applicable data protection laws. Supplier may obtain a copy of the Supplier personal information by written request, or submit updates and corrections by written notice to Company.

SCHEDULE J

REQUIREMENTS FOR CYBER SECURITY RELATED GOODS OR SERVICES

As a condition to providing Services pursuant to the Master Services Agreement ("MSA") of which this Schedule forms a part, Supplier and Supplier's Personnel shall comply with the supplementary terms and conditions set forth in this Schedule, which are based on governmental regulatory requirements. Capitalized terms used in this Schedule without definition shall have the meanings set forth in the MSA.

Toward an understanding of such supplemental terms and conditions the following definitions are provided.

1. Definitions

1.1 Cyber Security. A comprehensive program and method for the protection of digital computer and communication systems and networks, specifically such digital computer and communication systems and networks those having safety-related and important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

1.2 COTS. Commercial off the shelf tools provided by Supplier to Company or Customer as hardware, software or both in any combination; software development services for hire; on-site staff augmentation; or any digital product or service that affects safety-related or important to safety functions.

1.3 Checksum. A value used to ensure data are stored or transmitted without error. It is created by calculating the binary values in a block of data using some algorithm and storing the results with the data. For example, a basic checksum may simply be the number of bytes in a file. However, this type of checksum is not very reliable since two or more bytes could be switched around, causing the data to be different, though the checksum would be the same. Therefore, more advanced checksum algorithms are typically used to verify data. These include cyclic redundancy check ("CRC") algorithms and cryptographic hash algorithms.

1.4 Compensating controls. A technical, operational, or management cyber security control employed by an organization in lieu of a required or recommended cyber security control that provides an equivalent or better level of protection for a critical asset.

1.5 Critical data. The digital information that is contained within a critical asset and that, if compromised by a malicious attack, could affect the performance of the critical asset. Critical data includes digital information beyond just the process data. The following are examples of critical data: process control data, such as process variables; set point data; tuning data; firmware; application software and operating system software, and all associated files; security software and all associated files; files that contain data, such as data tables, configuration, numbers, logs, and security information; database tables and associated database files; network or transmission protocol data; test equipment files and information that could be connected to the critical asset; macros, formulas, and calculations whose resultant data are used as design input or to directly control plant equipment**.**

1.6 Critical Digital Assets ("CDA"). Those Digital Assets that are part of or are associated with safety class systems and components, or items relied on for safety, or safety related items.

1.7 Customer. The nuclear utility for which the Services, if any, are performed.

1.8 Digital assets. Computer, including computers integrated in tools and machinery, and network related hardware, firmware, operating systems, or application software.

1.9 Exploit information. Software, data, or a sequence of commands that take advantage of a bug or vulnerability in a software system with may cause unintended or unanticipated behavior.

1.10 Factory acceptance test. A factory acceptance test (FAT) is necessary to verify that all features and functions, including security features, function properly and provide the expected levels of functionality. Factory acceptance testing is a process, not an event, and could, in fact, extend over several weeks or months.

1.11 Hash algorithm. A hash algorithm is a commonly used function for validating data integrity. The algorithm is applied against the source data (typically a file and its content) in order to generate a unique, hash value (often called a checksum). One approach for data-integrity verification is to generate a hash when the content is created or when it is shipped and, later, to generate another hash after the content has been received or after a period of storage. The hash values are compared and, if they match, this indicates that the data is intact and has not been altered.

1.12 Operational cyber security controls. Operational cyber security controls are primarily implemented and executed by people (as opposed to systems). Examples of operational controls include cyber security awareness and training and the configuration management cyber security controls.

1.13 Secure development and secure operational environment. Secure development environment is the condition of having appropriate physical, logical, and programmatic controls in place during the digital system's development phases; i.e., concept, requirements, design, implementation, and testing, to ensure that unwanted, unneeded, and undocumented functionality (such as superfluous code) is not introduced into the Digital Assets of Supplier or its customers. Secure operational environment is the condition of having appropriate physical, logical, and administrative controls in a facility to ensure that the reliable operation of safety systems is not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the system. Regulatory Guide 1.152 Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," defines the requirements for a secure development and operational environment for nuclear safety systems.

1.14 System or software development life cycle ("SDLC"). Each organization is generally expected to have its own life cycle that is thoughtfully and purposefully created and followed to ensure high quality software development activities. Several standards and methodologies are available as references for use, such as NEI-13-10, "Cyber Security Control Assessments" or EPRI's Handbook for Verification and Validation of Digital Systems (TR-103291-R1).

1.15 Technical cyber security controls. Cyber security controls (such as, safeguards or countermeasures) for a Critical Digital Asset that are primarily implemented and executed by the Critical Digital Asset through mechanisms contained in the hardware, software, or firmware components of the asset. Examples of technical cyber security controls include session lock and audit storage capacity.

2. Supplier cyber security program requirements

2.1 Supplier must provide evidence that it has a Cyber Security Program that is fully compliant with all applicable regulations including those of the US Nuclear Regulatory Commission set out at Title 10 Code of Federal Regulations (CFR) Part 73.54, and as amplified in Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities." Such a program must consist of security policies, procedures and controls that were applicable throughout the development and product life cycles of the goods or services provided. Alternatively, if Supplier does not have its own Cyber Security Program, Supplier may adopt Company's Cyber Security Program. If Supplier choses to adopt Company's Cyber Security Program, such adoption will not relieve Supplier of the need to meet the NRC requirements.

2.2 Supplier's cyber security program must be designed to:

(a) Implement security controls to protect Digital Assets from cyber-attacks;

(b) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber-attacks;

(c) Mitigate the adverse effects of cyber-attacks; and

(d) Ensure that the functions of protected Digital Assets are not adversely impacted due to cyber-attacks.

2.3 Minimum requirements of Supplier's Cyber Security Program include process and procedures for:

(a) Defense-in-depth of digital perimeter defense, examples include physical controls, secure data centers, firewalls, intrusion protection, virus protection, and other secure digital assets. Where applicable, Supplier's Cyber Security Program should be part of its physical security program including period auditing requirements;

(b) Methods for determining Supplier's Critical Digital Assets, if applicable, and cyber security controls used in development of the Services; and

(c) Where compensating cyber security controls are currently used, inventory, list of components and systems for which associated cyber security controls are applied.

(d) Supplier's program for ensuring that sub-tier suppliers are vetted for compliance with Supplier or Company Cyber Security requirements or both.

(e) Supplier's methods to verify the integrity of software. Methods may include techniques, such as a hash algorithm or checksum, for all delivered binaries that can be validated against a transmittal letter or bill of materials prior to use.

2.4 Shipping and handling procedures must:

(a) Provide direct point to point shipment of products to Company where practical.

(b) Have methods to track the chain of custody of products shipped to Company, e.g., FedEx or UPS special handling that ensures chain of custody.

(c) Use tamper-resistant seals on all electronics equipment and packaging for products delivered to Company or our customers.

(d) Retain all records and supporting technical documentation required to satisfy the requirements of its Cyber Security Program.

(e) Provide assurance that its Cyber Security Program has continuity of operations (aka disaster recovery/contingency plan) requirements.

2.5 Prior to initiation of each the factory acceptance test, the Supplier shall install all operating systems and application patches, service packs, or other updates certified for use with the provided system by the time of test, and documentation of the configuration baseline.

2.6 Supplier's Cyber Security Program should be fully integrated into the existing Software Development Life Cycle ("SDLC"), engineering design and change process, configuration management, equipment life cycle, and procurement processes. It is critical that there be full traceability with documented evidence that the component or system was developed, installed, tested, and placed into operation in accordance with cyber security and other requirements that were established as part of the overall secure development life cycle.

2.7 Supplier's Cyber Security Program shall be documented in a cyber security plan or similar document, a copy of which shall be provided to Company upon request.

2.8 For networks and computer systems used to develop digital products for Company, Supplier shall protect the systems and networks from cyber-attacks that would:

(a) Adversely impact the integrity or confidentiality of data, software or both;

(b) Deny access to systems, services, data, individually or in any combination; and

(c) Adversely impact the operation of systems, networks, and associated equipment.

2.9 In order to provide this protection, Supplier shall:

(a) Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber-attacks to guarantee the integrity of digital products and software delivered or developed for Company.

(b) Establish, implement, and maintain a cyber security program for the protection of the assets used to develop and deliver Company digital products and software.

(c) Incorporate the Cyber Security Program as a component of the physical protection program.

2.10 The Cyber Security Plan should describe how the Supplier will:

(a) Detect and respond to cyber-attacks in a timely manner;

(b) Mitigate the consequences of cyber-attacks;

(c) Correct exploited vulnerabilities;

(d) Restore affected systems, networks, or equipment affected by cyber-attacks.

(e) Identify methods for collection, handling, storage, and tracking of information relating to exploited vulnerabilities.

(f) Include a provision for training that ensures personnel, including sub-tier supplier and contractors, are aware of Cyber Security requirements and receive the training necessary to perform their assigned duties and responsibilities.

(g) Describe how Supplier plans to evaluate and manage cyber events or incidents associated with the development of the goods or services. Supplier shall report to GEH within one hour of validation of any event whether such event occurs on its premises, at testing facilities, or at another customer's facilities that may have NRC or Customer cyber security notification requirements.

(h) Ensure that modifications to Digital Assets are evaluated before implementation so that the cyber security performance objectives are maintained.

(i) Describe Supplier's process to prevent counterfeit, fraudulent, and suspect goods (CFSI) from entering Supplier's supply chain.

3. Program for control of portable media, devices and equipment

Company prohibits the use of non-approved or unencrypted USB memory sticks and restricts the use of other portable media, devices and equipment. Supplier must be able to provide evidence that it has an established whole disk encryption program and has a means to ensure that this equipment on which the Work will be performed is free from virus and other malware.

4. Right of access

Company, its agents or assignees, shall have the right to inspect and evaluate those applicable areas of Supplier or its sub-tier suppliers' facilities and activities that are

affected by these requirements at a mutually agreed time during the procurement process. Inspections, surveillances, tests or non-financial audits performed by Customer or its agents shall in no way relieve Supplier or its sub-tier suppliers of any responsibilities under this Agreement.

During the course of performance of this Agreement, Supplier will report all breaches of its systems to Company in a timely manner and within 24 hours if the breach directly affects Company's systems. When a cyber security breach directly affects Company's systems, Company reserves the right to audit Supplier's remediation and recovery as it affects Company's goods or services.

5. Control of sub-tier supplier

Supplier shall be responsible for ensuring that all sub-tier suppliers work under the guidelines of NEDO-11290-A, Company Quality Assurance Program Description, a Company Quality Assurance Plan, or its own Quality Assurance Program that was pre-qualified and approved by Company, commensurate with the goods supplied or services rendered. Supplier shall provide assurance for all sub-tier suppliers that such sub-tier suppliers have a quality assurance program comparable to its own.

6. Records retention

Records required for retention include, but are not limited to, all digital records, log files, audit files, and non-digital records that capture, record, and analyze network and Critical Digital Assets (CDA) events. These records are retained to document access history and discover the source of cyber-attacks or other security-related incidents affecting those Critical Digital Assets. Supplier shall retain superseded portions of these records for at least three years after the record is superseded.

7. Procurement of equipment, parts and material

Supplier's written Quality Assurance Program shall include appropriate procedures for controlling the quality of equipment, parts, or material (hardware), supplied under this PO, either individually or in any combination. Such procedures shall ensure that all hardware design and design changes are documented in a hardware design specifications, all software or other design changes or revisions are documented. Such specification and documents evidencing the requirements of this paragraph shall be retained for review by Company or its customers.

8. Suppliers unescorted access to Company facilities

When providing services for Company's Digital Assets on the Wilmington site, Supplier agrees to follow Company's physical and cyber security program requirements as follows:

8.1 Before being permitted access to the Company's facilities, Supplier employees or contractors shall be made aware of Company's Cyber Security Program and shall agree to perform the work under the policies of Company's Cyber Security Program.

8.2 Supplier employees or contractors shall participate in Company's cyber security training programs and be added to the plant access control list.

8.3 Supplier employees or contractors shall adhere to the following Company cyber security policies:

(a) Configuration management of the Supplier's computers shall include virus protection, patch management, authentication requirements and secure Internet connections.

(b) Supplier digital devices (including personal laptops) shall be available for scanning prior to entry for malware and vulnerabilities.

(c) Supplier shall maintain secure transfer and storage of information and code while offsite.

a. Supplier has a duty to protect confidentiality.

b. Supplier shall clearly indicate approved and disapproved software.

c. Supplier shall maintain requirements and procedures for background investigations. (as applicable)

d. Supplier shall create and maintain a portable media control procedure.

e. Supplier shall establish cyber security awareness and training requirements

(d) Notify Company the same day that personnel with Company Critical Digital Asset electronic, physical, or information access, leave or change positions.

(e) Supplier shall provide detailed documentation on how the control system security can be maintained and supported in the event Supplier leaves the business (for

example, security-related procedures and products placed in escrow).

9. References

1. NEI-13-10, “Cyber Security Control Assessments”
2. EPRI Document 3002001824, 12/2013, “Cyber Security Procurement Methodology, Rev. 1”
3. 10 CFR 73.54 “Protection of digital computer and communication systems and networks”
4. NRC Regulatory Guide 5.71 “Cyber Security Programs for Nuclear Facilities”
5. NRC Regulatory Guide 1.152 “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”
6. TR-103291-R1, “Handbook for Verification and Validation of Digital Systems” EPRI
7. NEDO-11290-A, GEH Quality Assurance Program Description.

SCHEDULE K
GEH EXPORT CONTROLLED INFORMATION ACKNOWLEDGEMENT OF RESPONSIBILITIES

Capitalized terms used in this Schedule without definition shall have the meaning set forth in the Master Services Agreement ("MSA") to which this Schedule forms a part.

Information to be provided by Company to Supplier pursuant to the MSA may be subject to the export control restrictions in 10 CFR 810. To the extent that such regulations are applicable to any such information, the same must be strictly controlled.

Accordingly, no such export controlled information may be transferred by Supplier, directly or indirectly, to any non-US citizen (other than Legal Permanent Residents) in the US or outside the US. This includes providing access to Export Controlled Information ("ECI") inside the US.

The release by Supplier of ECI to a non-US citizen may result in imprisonment and/or fines. It is Supplier's responsibility to ensure that Supplier is in full compliance with the Export Control laws of the US.

Supplier's written acknowledgement of the terms and conditions contained in this Schedule are a representation and assurance that Supplier is able and willing to comply with the Export Control laws of the United States, as well as that no non-US citizen under Supplier's direction or control, whether by virtue of employment or otherwise, will have access to any ECI provided by Company to Supplier.

_____
Printed Name

_____
Supplier's Company Name

_____ _____
Signature Date