Terms of Use of Boeing Electronic Systems Supplement

1. Definitions.

"Access Controls" is defined as procedures, mechanisms, and/or measures that limit access to Boeing Systems to authorized persons or applications.

"Boeing Systems" is defined as any electronic information systems operated by or on behalf of Buyer, including without limitation: facilities, network communications systems, telecommunications systems, software, applications, information and data.

"Buyer" or "Boeing" used interchangeably within and between this supplement and any Contract means The Boeing Company including any wholly owned subsidiaries or affiliates thereof.

"Contract" or "Agreement" used interchangeably means any separate agreement between Seller and Buyer, into which these Terms of Use of Boeing Electronic Systems Supplement may be incorporated by reference.

"Electronic Access" is defined as access by authorized Seller Personnel to the Boeing Systems with the ability or the means necessary to read, write, modify, or communicate information, or otherwise use authorized system resources.

"Malware" means malicious computer software that interferes with normal computer functions or causes information leakage to unauthorized parties.

"Materials" means all data, text, graphics, animation, audio and/or digital video components that are stored on or accessible through Boeing Systems.

"Security Breach" means any actual or suspected Unauthorized Use, unauthorized access to Boeing Systems, or unauthorized interception or acquisition of Materials.

"Seller Personnel" is defined as any of Seller's employees, contract labor, consultants, advisers, or other representatives who have a need to access the Boeing Systems for Seller to perform under this Contract.

"Unauthorized Use" is defined as any use, reproduction, distribution, transfer, disposition, disclosure, possession, memory input, alteration, erasure, damage or other activity involving Materials, that is not expressly authorized under this Agreement (or any applicable Contract).

2. Access Right.

Buyer grants to Seller a limited, nontransferable, nonexclusive, revocable (at Buyer's discretion) right to access the Boeing Systems electronically solely during the term of this Contract and solely to the extent authorized in writing by Buyer in support of work to be performed by Seller pursuant to the Contract. Without limiting the foregoing, Seller hereby warrants that Seller and Seller Personnel shall not (i) introduce any Malware into Boeing Systems (whether through a laptop computer or other access device or otherwise); (ii) use the Boeing Systems for non-business purposes including, without limitation, Unauthorized Use; and/or (iii) take actions calculated to disrupt Boeing Systems.

3. Privacy and Right to Monitor.

Seller and Seller Personnel understand and consent as follows: Seller and Seller Personnel have no reasonable expectation of privacy in any communications or data, personal or otherwise, transiting or stored on Boeing Systems; any communications or data transiting or stored on Boeing Systems may be monitored, intercepted, recorded, and searched at any time and for any lawful purpose, and may be used or disclosed for any lawful purpose.

4. Electronic Access Requirements.

Seller may request, and Buyer may provide in its sole discretion for Seller's support of the Contract, Electronic Access for Seller Personnel on a "need to know" basis.

a. Accounts & Access Controls: Prior to obtaining Electronic Access, authorized Seller Personnel will be required to obtain from Buyer an Electronic Access account per individual, including Buyer Access Controls that may come from Buyer, third parties designated by Buyer or alternate controls subject to Buyer approval. Seller shall: (i) ensure that all Seller Personnel review and agree to abide by the terms of the Contract including this Terms of Use of Boeing Electronic Systems Supplement , prior to being granted Electronic Access; (ii) assign a single focal to initiate requests for Electronic Access for Seller Personnel, coordinate security briefings, maintain records of Seller Personnel granted electronic access, available for validation upon request of Buyer, and coordinate with Buyer regarding actual or potential security breaches; (iii) take all actions to prevent the loss, disclosure, reverse engineering, sharing with unauthorized Seller Personnel or compromise of Access Controls; and (iv) be responsible for the acts and omissions of all Seller Personnel with respect to their Electronic Access. Seller acknowledges that the Access Controls are for specific individual use of Seller Personnel only, are not transferable, and shall be maintained in confidence by Seller. Seller shall immediately notify Buyer if it believes that any Access Control has been compromised. Seller shall review (at least every three (3) months) each Seller Personnel's Electronic Access requirements. Seller shall promptly submit a written request to Buyer upon the reassignment, resignation, or termination of any Seller Personnel with Electronic Access, to terminate such Electronic Access. If any Seller Personnel who has Electronic Access to Boeing Systems is terminated for cause by reason of misappropriation of Boeing Proprietary Information or data, or unauthorized access to or use of Boeing systems, or similar reason, Seller shall immediately submit a written notice of name and BEMS ID(s) to Buyer. Buyer reserves the right, without notice and in its sole discretion, to terminate and/or block the access of any individual or entity to the Buyer Systems.

b. Seller System Protection: Prior to connecting to Buyer's internal network (either directly at Buyer's site or remotely via SSLVPN or through connect.boeing.com), Seller shall take steps to protect the confidentiality, integrity and availability of Boeing Systems and information by implementing and maintaining effective controls on all Seller systems and equipment including, without limitation:

1. Fully-patched operating systems and applications – Seller shall subscribe to and apply the vendor's automatic update services;

2. Anti-malware – Seller devices shall have up-to-date anti-virus protection running with the latest signature files;

3. Software Firewall – Seller shall use an up-to-date version of a software firewall configured to limit ports/protocols to only those necessary (such software firewalls are required even when a local hardware firewall or enterprise firewall is used);

4. Access control to computing device – Seller shall use an account/password or token/PIN to access or unlock computing devices; and

5. Encryption - Whole disk or file/folder encryption shall be used to protect Materials that are being stored locally on the Seller's devices.

5. Export Control.

US Trade Control

In order to comply with applicable U.S. export control statutes and regulations, Buyer shall be required to obtain information concerning identity and citizenship, including dual or third country national status, if applicable, or place of birth of Seller Personnel with Electronic Access. Where access is granted, Seller shall be responsible for obtaining all export authorizations required, including where applicable, export authorizations related for Seller Personnel. If related to Electronic Access export authorization(s) are required to allow such Seller Personnel to perform the work to which he or she is assigned, Seller must obtain such authorizations and Seller shall comply with any additional export control restrictions as required by applicable U.S. export control statutes and regulations.

TECHNICAL DATA AND SOFTWARE ACCESSED FROM BOEING ELECTRONIC SYSTEMS MAY BE SUBJECT TO UNITED STATES GOVERNMENT EXPORT CONTROL REGULATIONS IN ACCORDNACE WITH THE DEPARTMENT OF STATE, INTERNATIONAL TRAFFIC IN ARMS REGULATIONS ("ITAR"), OR DEPARTMENT OF COMMERCE, EXPORT ADMINISTRATION REGULATION ("EAR"), AND MAY NOT BE EXPORTED, RELEASED OR DISCLOSED TO FOREIGN PERSONS, WHETHER LOCATED INSIDE OR OUTSIDE THE U.S. WITHOUT PRIOR APPROVAL FROM THE U.S. GOVERNMENT. VIOLATIONS OF EXPORT LAWS INVOKE SEVERE FINES AND PENALTIES FOR BOTH INDIVIDUALS AND THE COMPANIES THEY REPRESENT.

Non-US Trade Control

In order to comply with applicable international trade control statutes and regulations, Buyer shall be required to obtain information concerning identity and citizenship, including dual or third country national status, if applicable, or place of birth of Seller Personnel with Electronic Access. Where access is granted, Seller shall be responsible for obtaining all trade control authorizations required, where applicable, for all Seller Personnel, including to allow such Seller Personnel permission to perform the work to which he or she is assigned, and Seller shall comply with any additional trade control restrictions as required by applicable jurisdiction export control statutes and regulations.

TECHNICAL DATA AND SOFTWARE ACCESSED FROM BOEING ELECTRONIC SYSTEMS MAY BE SUBJECT TO GOVERNMENT TRADE CONTROLS IN ACCORDANCE WITH IMPORT AND EXPORT REGULATIONS IN AFFECTED JURISDICTIONS AND MAY NOT BE IMPORTED, EXPORTED, RELEASED OR DISCLOSED TO UNAUTHORIZED PERSONS, WITHOUT PRIOR APPROVAL FROM THE AFFECTED GOVERNMENT. VIOLATIONS OF TRADE CONTROL LAWS INVOKE SEVERE FINES AND PENALTIES FOR BOTH INDIVIDUALS AND THE COMPANIES THEY REPRESENT.

6. Seller Security Controls:

a. Physical Controls: Seller shall implement and maintain physical controls that prevent any Unauthorized Use, Security Breaches, and loss of Materials.

b. Seller Access Controls: Seller shall implement and maintain access controls that prevent any Unauthorized Use of Information, Security Breaches and loss of Materials. Seller shall implement a policy that adopts Information Security Management principles in accordance with ISO/IEC 27001 and ISO/IEC 27002, or NIST SP 800-53 as applicable. The Seller shall implement and maintain security controls no less comprehensive that the most current version of the Critical Controls for Effective Cyber Defense as found at www.counciloncybersecurity.org, or the controls in NIST SP 800-53. Seller shall provide relevant and credible evidence of its compliance with the above-stated controls. Such evidence of compliance may be provided through self-audits or use of a third-party audit, results of which shall be provided to Buyer.

c. Encryption: Seller shall in the support of the work to be performed under the Contract comply with Buyer requirements in the use of and strength of encryption, but no less than that required by law, regulation, or government standard, based on the sensitivity of the Materials involved in the Contract.

d. Access to Buyer Systems - Virtual Office Work: Seller Personnel may work from locations that have not been assessed (provided they are not public locations and both Buyer and Seller have mutually approved of such locations). Buyer reserves the right to require virtual Personnel to follow virtual office requirements as provided to Seller by Buyer from time to time.

e. Personnel Security: Seller shall perform background checks on Seller Personnel in accordance with the terms herein or terms as indicated within the Statement of Work (and any relevant terms included in a Contract) that Buyer authorizes electronic access to view, alter, copy or delete Materials, and provide Buyer details on the extent of the background check process and criteria, including any change or variation to such process or criteria due to restrictions imposed by applicable laws. Seller shall use at least the same effort that Seller uses for its own proprietary and confidential information and in no event less than a reasonable amount of effort, to enforce Seller's obligations under the Contract against current and former employees. Buyer shall have the option to require that Seller Personnel with access to Materials are U.S. persons and are located within the U.S. unless otherwise specified in the applicable Statement of Work.

7. Administrative Controls.

Seller shall implement and maintain administrative controls that protect information through standard procedures and processes. The administrative controls shall include, but not be limited to: measures that protect (a) Materials while in transit and at rest; (b) computing equipment on which Materials reside; and (c) environments in which Materials are accessed and used. Prior to initial handling of, use of, or access to Materials, Seller hereby agrees to provide Seller Personnel with current and relevant security education with respect to their obligations hereunder. Seller may request, and Buyer may provide, certain educational materials to communicate security obligations.

8. Prohibited Use.

Seller shall not, unless authorized in writing by Buyer: (a) export or save any Materials from the Boeing Systems except in support of the work to be performed under this Contract; (b) make any derivative uses of the Boeing Systems or the Materials except in support of the work to be performed under this Contract; (c) use any data mining, robots, or similar data gathering and extraction methods; (d) use any frame or framing techniques to enclose any Materials found on

the Boeing Systems; (e) through reverse engineering, decompiling, or disassembling any portion of the Access Controls, access or attempt to access any unauthorized Materials or restricted portions of the Boeing Systems, or remove any restrictive markings; or (f) access the Boeing Systems through any mechanism other than the authorized Access Controls.

9. Security Breach Notification.

Seller hereby represents, warrants and covenants that it is and shall remain in compliance with all applicable laws that require notification of Security Breaches.

If Seller discovers or is notified of a Security Breach or potential Security Breach, Seller shall immediately: (a) cease access to any Materials that are the subject of the Security Breach and shall not review any unauthorized Materials; (b) notify Buyer of such Security Breach or potential Security Breach and notify Buyer of the Materials involved; (c) if Buyer's Materials were in the possession of Seller at the time of such Security Breach or potential Security Breach, Seller shall (i) investigate and cure the Security Breach or potential Security Breach; (ii) except with respect to Security Breaches that were caused by Buyer, provide Buyer with assurance satisfactory to Buyer that such Security Breach or potential Security Breach will not recur; (iii) take any other steps determined by and provided in writing by Buyer's related to the incident; and (iv) assist Buyer in investigating, remedying, and taking any other action Buyer deems necessary to address such Security Breach, including related to any dispute, inquiry, or claim related to such Security Breach.

Seller shall make the notification required in this section by immediately complying with the notice requirements in the Contract, and sending email message to abuse@Boeing.com (or any other address specified in writing by Buyer) setting forth the information required in this section. The Seller shall copy the Buyer procurement agent on all related email notifications.

In addition to any other rights and obligations set forth in a relevant Contract, Seller agrees to permit Buyer to review its security control procedures and practices via physical or electronic access by Buyer, including access to Seller facilities in which such systems are located, as well as any and all premises where maintenance, storage or backup activities are performed.

Any material breach of this article by Seller may be considered a default for which Buyer may suspend or revoke Electronic Access.

Seller acknowledges that any attempts by Seller or any Seller Personnel to circumvent any security measures designed to prevent unauthorized access to the Boeing Systems may be subject to criminal or civil penalties under the U.S. Federal Computer Fraud and Abuse Act and other applicable laws and regulations. In addition to any other remedy available to Buyer under the Contract, or available to Buyer under law or equity, Seller and Buyer hereby agree that Buyer shall be entitled to injunctive relief because a breach of any provision related to Electronic Access may result in irreparable harm to Buyer or its affiliates, for which monetary damages may not provide a sufficient remedy, Buyer may seek both monetary damages and equitable relief.

10. REMEDIES

Indemnification: Seller shall indemnify, defend, and hold harmless Buyer, its subsidiaries, and affiliates and their respective officers, shareholders, directors and employees from and against any and all third-party liabilities, obligations, losses, claims, damages, costs, charges, and other expenses of any kind (including, without limitation, reasonable attorneys' fees and legal expenses) that arise out of or relate to any failure by Seller or any of its subcontractors to comply with any obligation enumerated in these Terms of Use of Boeing Electronic Systems Supplement. Buyer may participate in the defense and settlement of any claim for which it is entitled to indemnification hereunder, using attorneys selected by Buyer, at Seller's expense. Notwithstanding any other provision of the Contract to the contrary, in no event will any limitation of liability provision (including, but not limited to, any limitation on the amount or type of damages, e.g., consequential damages) in the Contract apply to any breach or right that relates to this Terms of Use of Boeing Electronic Systems Supplement.

11. DISCLAIMER OF WARRANTIES AND LIABILITY

SELLER HEREBY WAIVES, RELEASES AND RENOUNCES ALL WARRANTIES, OBLIGATIONS AND LIABILITIES OF BOEING AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES AGAINST BOEING, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS, MATERIALS AND ANY INFORMATION, GOODS, SERVICES, OR OTHER THINGS PROVIDED PURSUANT TO THIS AGREEMENT. BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS, AND MATERIAL ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS AND BOEING MAKES NO REPRESENTATION OR WARRANTY AS TO THE COMPLETENESS OR ACCURACY THEREOF. TO THE FULLEST EXTENT PERMITTED BY LAW, SELLER (AND SELLER'S SUBSIDIARIES AND AFFILIATES, IF ANY) HEREBY WAIVE, RELEASE AND RENOUNCE ALL WARRANTIES, OBLIGATIONS AND LIABILITIES OF BOEING AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES AGAINST BOEING, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS AND MATERIALS, EVEN IF BOEING HAS BEEN ADVISED OF THE POSSIBILTY OF ANY DAMAGES, INCLUDING WITHOUT LIMITATION: (A) ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, (B) ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE, (C) ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN CONTRACT OR TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING, AND (D) ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OF OR DAMAGE TO ANY PROPERTY BELONGING TO SELLER OR SELLER PERSONNEL.

EXCLUSION OF CONSEQUENTIAL AND OTHER DAMAGES. BOEING SHALL HAVE NO OBLIGATION OR LIABILITY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING), OR OTHERWISE, FOR LOSS OF USE, REVENUE OR PROFIT OR FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES WITH RESPECT TO BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS, MATERIALS AND ANY INFORMATION, GOODS, SERVICES, OR OTHER THINGS PROVIDED PURSUANT TO THIS AGREEMENT. THIS PROVISION SHALL SURVIVE TERMINATION OR CANCELLATION OF THIS AGREEMENT.

DEFINITIONS: For the purpose of this Terms of Use of Boeing Electronic Systems Supplement section, 11, "Boeing" includes The Boeing Company, its divisions, subsidiaries, the assignees of each, subcontractors, suppliers and affiliates, and their respective directors, officers, employees and agents.