BAE SYSTEMS

EXHIBIT TO THE TERMS AND CONDITIONS
PRIVACY AND DATA SECURITY

BAE Systems requires that its acquisition and retention of business be conducted in accordance with the highest standards of data protection and information security. Seller's performance of services for BAE Systems may involve access to data which may be attributable to BAE Systems and for which BAE Systems could be held liable. For that reason, Seller agrees and certifies that it shall comply with the Privacy and Data Security requirements contained in this Exhibit.

Privacy and Data Security.

a) Data Protection Standard of Care.

1. Seller acknowledges and agrees that, as part of the Services to be performed hereunder, Seller may receive or have access to Personal Information (as defined below). Seller shall comply with the terms and conditions set forth in this Exhibit in its collection, receipt, transmission, storage, disposal, use and disclosure of such Personal Information. Seller agrees and covenants that it shall be responsible for any unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of Personal Information under its control or in its possession by all Authorized Personnel.

2. Seller agrees and covenants that it shall: (i) restrict access to Personal Information to Authorized Personnel; (ii) keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure; and (iii) use and disclose Personal Information solely and exclusively for the limited and specified purposes of providing the Services set forth in the Agreement. Seller will not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for (i) cross-context behavioral advertising, (ii) Seller's own purposes, or (iii) for the benefit of anyone other than BAE Systems, in each case, without BAE Systems' prior written consent. Seller will not combine Personal Information with personal information Seller receives from or on behalf of another person or entity or collects from its own interactions with an individual except to perform a business purpose as defined in applicable Laws.

3. In no event shall Seller allow any person who is not a United States citizen or a lawful permanent resident to work on or have access to, any BAE Systems data or Proprietary Information. All Seller data and Proprietary Information will be hosted in and only accessed by individuals located in the United States of America.

4. Seller agrees and covenants that except as provided in clause (i) of Section 2 (Data Protection Standard of Care), it will not, directly or indirectly, disclose or give access to Personal Information to any third party, including any subcontractors, agents, outsourcers or auditors, without the express written consent from BAE Systems. Should it receive such consent, Seller shall select the third party after receiving and considering in good faith any input from BAE Systems. Seller shall ensure that it maintains appropriate technical, organizational and physical security measures and an adequate level of data protection safeguards, and Seller shall require the third party's agreement in writing to provide at least the same level of privacy and data protection as required of Seller under this Exhibit. Seller

shall remain responsible for, and remain liable to, BAE Systems for the actions and omissions of any such third party concerning the treatment of BAE Systems Personal Information as if they were Seller's own actions and omissions.

5. Notwithstanding the foregoing Section, Seller may disclose Personal Information as required by applicable Law or by proper Government Authorities. Seller shall use its best efforts to give BAE Systems prompt written notice of any such legal or government demand, and allow BAE Systems the opportunity to participate in any proceeding objecting to such disclosure.

b) Information Security. Seller represents and warrants that it does and will comply with all federal, state and local applicable data protection or privacy Laws and regulations Seller will immediately notify BAE Systems in writing if Seller determines that it can no longer meet its obligations under applicable Laws or this Exhibit. Without limiting Seller's obligations under this Section, Seller shall implement administrative, physical and technical safeguards that are no less rigorous than accepted industry practices to protect Personal Information against accidental, unauthorized or unlawful (i) destruction or loss, (ii) alteration and (iii) disclosure, access, acquisition or use. Seller shall ensure that all such safeguards, including the manner in which Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy Laws, as well as the terms and conditions of this Exhibit. In particular, Seller shall not use any cloud computing services (e.g., cloud-based email, document storage, etc.) in its handling of the Personal Information without the express prior written consent of BAE Systems. Seller agrees to submit, upon reasonable prior notice, Seller's processing facilities, the organizational and technical measures referenced herein for auditing by BAE Systems or its designee.

c) Security Breach Procedures. For any suspected or actual Security Breach (including the unauthorized access to, the unauthorized acquisition of, or the unauthorized use of Personal Information):

1. Seller shall: (i) provide BAE Systems with the name and contact information for an employee of Seller (or their designee) who shall serve as BAE Systems' primary security contact and shall be available to assist BAE Systems twenty-four hours per day, seven days per week as a contact in resolving obligations associated with a Security Breach; (ii) notify BAE Systems of a Security Breach as soon as practicable, but no later than twenty-four hours after Seller becomes aware of it; and (iii) notify BAE Systems of any Security Breaches by telephone at (888) 374-0123 and email at bae.privacy@baesystems.com, with a copy by email to Seller's primary business contact with BAE Systems.

2. Immediately following Seller's notification to BAE Systems of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Seller agrees to reasonably cooperate with BAE Systems in its handling of the matter, including: (i) assisting with any investigation; (ii) providing BAE Systems with physical access to the facilities and operations affected; (iii) facilitating interviews with Seller's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable Law, industry standards or as otherwise reasonably required by BAE Systems.

3. Seller shall use best efforts to immediately remedy any Security Breach and prevent any

further Security Breach at Seller's expense in accordance with applicable privacy rights, Laws and standards. Seller shall reimburse BAE Systems for actual costs incurred by it in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation pursuant to Section c)4 (Security Breach Procedures) below.

4. Seller agrees that it shall not inform a third party of any Security Breach without first obtaining BAE Systems' prior written consent, and where it has received a complaint, only that the matter has been forwarded to BAE Systems' legal counsel. Further, Seller agrees that BAE Systems shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by Law, or otherwise in BAE Systems' discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

5. Seller agrees to reasonably cooperate with BAE Systems in any litigation or other formal action deemed reasonably necessary by BAE Systems to protect its rights relating to the use, disclosure, protection and maintenance of Personal Information.

6. Seller shall maintain records of any known or suspected Security Breaches in accordance with commercially accepted industry practices.

7. In the event of any Security Breach, BAE Systems shall retain the right to preclude temporarily or permanently Seller's further processing of Personal Information.

d) Return or Destruction of Personal Information. At any time during the term of this Exhibit at BAE Systems' written request or upon the termination or expiration of this Exhibit for any reason, Seller shall, and shall instruct all Authorized Personnel to, promptly return to BAE Systems all copies, whether in written, electronic or other form or media, of Personal Information in its possession or the possession of such Authorized Personnel, or securely dispose of all such copies, and certify in writing to BAE Systems that such Personal Information has been returned to it or disposed of securely. Seller shall comply with all reasonable written directions provided by BAE Systems with respect to the return or disposal of Personal Information.

e) Additional Assistance. Seller agrees and covenants that upon request by BAE Systems, it will cooperate with BAE Systems in promptly responding to communications or requests made by individuals in relation to their Personal Information, including, among other things: (i) providing information to an individual regarding the Personal Information held by the Seller, and (ii) irrevocably deleting Personal Information held by the Seller about such individual. To the extent that Seller transmits Personal Information to BAE Systems concerning any of its employees, Seller will provide each such employee with a copy of BAE Systems privacy policy.

f) Equitable Relief. Seller acknowledges that any breach of its covenants or obligations set forth in this Privacy and Data Security Exhibit may cause BAE Systems irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, BAE Systems is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which BAE Systems may be entitled

at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Exhibit to the contrary.

g) Indemnification. Seller shall defend, indemnify and hold harmless BAE Systems, its parent, subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors and permitted assigns (each, an " Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, to the extent arising out of or resulting from any third party claim against any Indemnitee arising out of or resulting from Seller's failure to comply with any of its obligations under Privacy and Data Security provisions of this Exhibit.

Definitions:

a) "**Authorized Personnel**" means Seller's employees and contractors (i.e., workers serving in a staff augmentation capacity to Seller) (i) who have a strict need to know or otherwise access Personal Information to enable Seller to perform its obligations under this Exhibit, and (ii) who are bound in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Exhibit. In addition, Seller will have performed a background check on each Authorized Person it gives access to Personal Information. Such background check will include a review of the individual's criminal history, if any. Seller will not grant access to Personal Information if the background check or other information in the Seller's possession would lead a reasonable person to suspect that the individual has committed identity theft or otherwise misused third party data or that the individual presents a threat to the security of the Personal Information.

b) **"Highly Sensitive Personal Information"** means an (i) individual's government-issued identification number (including social security number, driver's license number or state-issued identified number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; or (iii) biometric or health data.

c) " **Personal Information"** means information provided to Seller by or at the direction of BAE Systems, or to which access was provided to Seller by or at the direction of BAE Systems, in the course of Seller's performance under this Exhibit that: (i) identifies or can be used to identify an individual (including names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers), in case of both sub-clauses (i) and (ii), including all Highly-Sensitive Personal Information. BAE Systems' business contact information is not by itself deemed to be Personal Information.

d) **"Security Breach"** means (i) any act or omission, that compromises either the security, confidentiality or integrity of Personal Information or the physical, technical, administrative or organizational safeguards put in place by Seller or any Authorized Personnel that relate to the protection of the security, confidentiality or integrity of Personal Information, or (ii) receipt of

a complaint by Seller in relation to the privacy practices of Seller or any Authorized Persons or a breach or alleged breach of this Exhibit relating to such privacy practices.