DATA PROTECTION ADDENDUM (DPA)

Leidos requires all third parties to comply with the goals and objectives of its Global Privacy Office, as set forth in this Data Protection Addendum ("DPA"). These are requirements that should be addressed at a minimum and, depending on the nature of the engagement or the Services provided, other requirements may be added in the relevant Statement of Work or the Contract Agreement.

1. DEFINITIONS.

1.1. "Applicable Law(s)" means any applicable law, rule, or regulation applicable to the Contract Agreement, the Services, Leidos or Supplier, and applicable Industry Standards concerning, but not limited to the following, privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing of Personal Information.

1.2. "Contract Agreement" means the agreement between the parties entitled [*Name of the Agreement*], dated [*Date of Named Agreement*] and the Statement of Work, dated [*Date of SOW*];

1.3. "Industry Standards" means the highest, then-current industry standard(s) as appropriate, given the associated activity, risk and/or requirement.

1.4. "Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing Personal Information, including EU Personal Data.

1.5. "Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Information on behalf of a Data Controller.

1.6. "Data Subject" means the individual about whom specific Personal Information relates.

1.7. "EU Data Protection Legislation" collectively refers to European Union's Directive 95/46/EC, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, and any other data protection or privacy legislation in force in the European Economic Area ("EEA").

1.8. "Leidos Confidential Information" means all information disclosed prior to or during the Term of the Contract Agreement: (i) as it relates to Leidos' business, including product plans, marketing plans, business opportunities, personnel, research, and development; and (ii) designated by Leidos as "confidential" or "proprietary" or which, under the circumstances, would reasonably be deemed to be confidential.

1.9. "Leidos Data" means (i) all information, whether or not Leidos Confidential Information, entered in, transmitted by or through, or otherwise transferred to software or equipment that is utilized hereunder, or that is transmitted by or through the Services, each by or on behalf of Leidos (including information that is provided by or on behalf of Leidos for the purpose of entering such information in, transmitting such information by or through, or otherwise transferring such information to software, equipment or the Services); (ii) any other information that is Processed at any time by Receiving Party or

Receiving Party personnel in connection with or incidental to the performance of the Contract Agreement; and (iii) any information derived from the information described in (i)-(ii) above. Personal Information is a component of Leidos Data.

1.10. "Personal Information" means (i) that subset of Leidos Data that relates to or can be attributed to an identified or identifiable natural person; (ii) information concerning an identified or identifiable natural person that is protected by Applicable Laws, including the EU Data Protection Legislation; and/or (iii) any information or data that can be used to identify individuals – either on its own or in combination with other information.

1.11. "Processing," or any variation thereof, means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12. "Receiving Party" means "[*Name of Supplier*]"

1.13. "Safeguard Obligations" means the requirements set forth in Exhibit A to this DPA, which may be updated by Leidos in its sole discretion from time-to-time, or more stringent requirements and all safeguard obligations in all Applicable Laws and regulations regarding such Leidos Data. Receiving Party acknowledges and agrees that (i) the standards set out in Exhibit A to this DPA are solely minimum standards of Leidos and are not represented by Leidos or relied upon by Receiving Party as sufficient security standards to comply with all Applicable Laws; and (ii) Receiving Party is responsible for ensuring that it complies with all Applicable Laws.

1.14. "Security Incident" means any suspected or actual (i) unauthorized Processing of Leidos Data (including Personal Information) (such as loss or unauthorized use, accidental or unlawful destruction, alteration, disclosure or acquisition of or access to such information) or an occurrence in which Leidos Data has been compromised or there is a reasonable suspicion that Leidos Data may have been compromised by any means, including by data breach or resulting in data loss, and for which review of Applicable Laws may be desired by Leidos or required in order to comply with Applicable Laws; or (ii) unauthorized use of, disclosure of, or access to Receiving Party's systems, Leidos Data, physical intrusion of facilities, or theft, misappropriation or loss of documents, or storage media.

1.15. "Services" means the performance of the Receiving Party under the Contract Agreement.

2. COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS. Receiving Party agrees to perform under the Contract Agreement and this DPA, in full compliance with all now or hereafter all Applicable Laws.

3. Cloud Computing and Subcontractors. Receiving Party shall provide a list to Leidos of any subcontractor that provides technology infrastructure used by Receiving Party to host, store or Process Leidos Data. Receiving Party shall remain fully responsible to Leidos for all of the acts and omissions of its subcontractors and outsourced providers with respect to the Services. Receiving Party represents and warrants that it has obtained, or will obtain, enforceable agreements with its subcontractors and outsource providers which ensure that: (i) its subcontractors are bound to adhere to and comply with the confidentiality, rights in data, audit, and regulatory compliance obligations assumed by Receiving Party under this DPA; (ii) such subcontractors and outsource providers are prohibited from further subcontracting their services without the prior written consent of Leidos; and (iii) such subcontracts will comply with all Applicable Laws.

4. STANDARD DATA PROCESSING TERMS

4.1. Receiving Party will not use, disclose, access, or Process Leidos Data except as necessary to provide the services as set forth in the Contract Agreement.

Leidos has the right to remove or request deletion of Leidos Data from the Receiving Party's systems at any time.

5. DATA STORAGE AND OFFSHORE SECURITY REQUIREMENTS

5.1. Receiving Party will ensure that while performing the Services, Receiving Party preserves Leidos Data as authentic and reliable in accordance with this DPA and Industry Standards.

5.2. Receiving Party will keep Leidos informed at all times of the physical location(s) of all Leidos Data, regardless of the country in which the Leidos Data is located. Receiving Party will not move any Leidos Data to a new physical location without the prior written approval of Leidos. In the event of any unauthorized relocation of Leidos Data, Receiving Party shall advise Leidos in writing immediately.

5.3. Leidos Data is not permitted to be hosted or stored offshore. All Leidos Data must reside on servers located in the United States for the duration of Processing.

5.4. Backup Processes at offshore locations will not receive, maintain, Process, or otherwise access or interact with Leidos Data.

6. AUDIT RIGHTS

6.1. Receiving Party will obtain attestation reports related to its security, availability, confidentiality, and data integrity safeguards at least annually and keep such reports for at least three (3) years following each attestation.

6.2. In addition to audit rights in the Contract Agreement, Leidos at its sole discretion reserves the right to audit or have audited by third-party auditors Receiving Party's compliance with the provisions in this DPA upon five (5) days prior notification, including without limitation auditing access to and use of Leidos Data, detecting violations and/or misuse by Receiving Party and ensuring compliance with the security

safeguard obligations and ensuring Receiving Party's compliance with the requirements set forth in this DPA.

6.3. If the audit right is exercised by Leidos, Receiving Party will provide reasonable assistance, including: (i) allowing inspection on Receiving Party's premises of relevant documents or records, to the extent such documents or records directly relate to Leidos Data and the services provided by Receiving Party to Leidos under the Contract Agreement; and (ii) providing appropriate management personnel to engage with Leidos and supervise any audit if needed.

6.4. If the audit right is exercised by Leidos, such audit will be conducted at a mutually agreed-upon time.

7. ADDITIONAL SAFEGUARDS AND DISCLOSURES

7.1. Receiving Party may disclose Leidos Data in accordance with a judicial or other governmental order, provided that Receiving Party either (i) gives Leidos reasonable notice prior to such disclosure to allow Leidos a reasonable opportunity to seek a protective order or its equivalent; or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford Leidos Data the highest level of protection possible under applicable law or regulation. Receiving Party shall disclose only the portion of Leidos Data that is required to be disclosed under such order.

7.2. Receiving Party will take reasonable steps to ensure the reliability of any employee, agent, or contractor who may have access to Leidos Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Leidos Data for the purposes of the Contract Agreement and/or to provide the Services.

7.3. Receiving Party further agrees to limit disclosure of and access to Leidos Data only to those employees of Receiving Party who have been advised of and have agreed in writing to the obligations and restrictions relating to such Leidos Data as set forth in this DPA. Prior to any disclosure of or provision of access to Leidos Data to such employees: (i) Receiving Party must execute appropriate written agreements with its employees requiring them to enable Receiving Party to comply with all the provisions of this DPA; (ii) such employees must also acknowledge in writing that they will comply with confidentiality obligations that are substantially the same in all material respects with regard to Leidos Data as those of Receiving Party set out in this DPA; and (iii) such employees must be trained regarding their responsibilities to protect, safeguard, and limit disclosure of Leidos Data under Receiving Party's policies and procedures.

7.4. Receiving Party agrees not to disclose or permit access to Leidos Data to any of its affiliates, subcontractors, temporary employees, consultants or agents except to those who have a bona fide need to know such Leidos Data solely as necessary to provide the Services under the Contract Agreement. Prior to any disclosure of or provision of access to Leidos Data to any such affiliates, subcontractors, temporary employees, consultants or agents (collectively "Agents"): (i) Receiving Party must execute appropriate written agreements with Agents requiring them to comply with all provisions of this DPA; (ii) such Agents must also acknowledge in writing that they will comply with confidentiality

obligations that are substantially the same in all material respects with regard to Leidos Data as those of Receiving Party set out in this DPA; and (iii) such Agents must be trained regarding their responsibilities to protect, safeguard, and limit disclosure of such Leidos Data under Receiving Party's policies and procedures. Receiving Party also agrees to disable access within twenty-four (24) hours (or by the next business day) of when those Agents with access to Leidos Data are transferred to a role that no longer requires access to Leidos Data, are terminated, or are no longer providing services to Receiving Party in connection with the Services.

7.5. Within ten (10) days of Leidos' request or as soon as Leidos Data is no longer needed or required for the Services, Receiving Party will, at Leidos' sole option: (i) return all (or in part) originals, copies, reproductions and summaries of Leidos Data and all other tangible materials and devices provided to Receiving Party as Leidos Data; or (ii) certify disposal of the same, except as necessary to comply with Applicable Laws. Both parties will agree to an acceptable transfer or disposal methodology as applicable. Receiving Party will maintain appropriate administrative, physical, organizational, and technical safeguards to ensure the security, confidentiality, and integrity of Leidos Data during such transfer or disposal.

8. INTERNATIONAL CONSIDERATIONS

8.1. In addition to the compliance with Applicable Laws set forth elsewhere in the Contract Agreement and this DPA, specifically with respect to Personal Information, Receiving Party, in providing the Services, is acting as the Data Processor of Personal Information of Data Subjects, namely employees based in the EEA, of which Leidos or an affiliate of Leidos based in the EEA is the Data Controller ("EU Personal Data").

8.2. Receiving Party will also be acting as the Data Processor of Personal Information of employees based in Australia of which an affiliate based in Australia is the Data Controller ("Australian Personal Data"). For the purposes of providing the Services, Receiving Party Agrees to Process the Australian Personal Data in the same way as, and in particular with the same protections as the EU Personal Data.

8.3. Receiving Party will:

8.3.1. Process EU Personal Data and Australian Personal Data in accordance with the EU Data Protection Legislation, including but not limited to Article 28(3) of the General Data Protection Regulation (EU) 2016/679; and

8.3.2. Comply with, and will ensure its affiliates and Suppliers will comply with, the Data Processing Obligations (Exhibit B) to the extent Leidos Data (including EU Personal Data and Australian Personal Data) is Processed;

8.3.3. Complete the Standard Contractual Clauses for Data Processors established in third countries in compliance with the obligations defined and stated in the EU commission's Decision C(2010)593 (final) given on 5 February 2010 ("EU Model Clauses") to reflect the circumstances of such Processing with Leidos, or at Leidos' request, with the applicable affiliate(s) of Leidos who act(s) as data controller(s) (as defined in the EU Data Protection Legislation) of such EU

Personal Data and Australian Personal Data. Receiving Party also agrees that it will (at Leidos' sole expense) cooperate with Leidos to register any executed EU Model Clauses with any applicable supervisory authority(ies) in any member state(s) of the EEA or to procure approval from any such supervisory authority (as the case may be) where the same is required.

9. OBLIGATIONS REGARDING LEIDOS DATA. Notwithstanding that the Contract Agreement may have terminated or expired, Receiving Party will, at a minimum:

9.1. Refrain from using, disclosing, communicating, reproducing in any media, summarizing, transferring, selling, leasing, licensing, disseminating, providing access to and/or distributing any portion of Leidos Data except as necessary to accomplish the Services subject to the restrictions set forth in this DPA and for no other reason, unless otherwise agreed to in writing by Leidos in Leidos' sole discretion.

9.2. Provide access to Leidos Data to individuals and third parties as set forth in this DPA;

9.3. Notify Leidos of any notice of privacy practices maintained by Receiving Party, including without limitation any restrictions or permissions for an individual to use or disclose Leidos Data and any changes to such notification made during the term of the Contract Agreement;

9.4. Refrain from disclosing, communicating, transferring or providing access to any Leidos Data to Receiving Party's employees except as expressly provided in this DPA;

9.5. Refrain from accessing any Leidos Data that is not required in connection with the Services set out in the definitions of this DPA. If Receiving Party does accidentally access such Leidos Data, it will immediately notify Leidos of the access and take all appropriate and reasonable steps as directed by Leidos to protect and/or destroy Leidos Data in its possession; and

9.6. Refrain from contacting, creating lists of, marketing to, providing services to or engaging in any transaction with any individuals identified in Leidos Data unless it is pursuant to [Insert name of terms and conditions document if applicable], a separate written agreement between Leidos and Receiving Party, Leidos' written direction in Leidos' sole discretion, or a separate written agreement between Receiving Party and an individual; and [*if there is an accompanying contract under which the Receiving Party will do these things, then it should be identified here*.]

10. OWNERSHIP. The parties agree that all rights, title and interest in Leidos Data (including, without limitation, any intellectual property rights therein) are and will remain the property of Leidos, its employees, or its customers [*and its (Third Parties, if any)*]. Receiving Party acknowledges and agrees that no express or implied right or license to Leidos Data is granted by the Contract Agreement or by any disclosure by Leidos or its employees of information hereunder. Receiving Party agrees that it will not remove any confidentiality notice or other identification or evidence of Leidos Data contained on or included in any item of Leidos Data. Receiving Party shall reproduce any such notice or identification on any reproduction, modification or translation of such Leidos Data and shall add any notice or other evidence of confidential or Leidos Data to Leidos Data in its possession upon request by Leidos. The

provisions of the Contract Agreement and this DPA shall supersede the provisions of any inconsistent legend that may be affixed to any data, and the inconsistent provisions of such legend shall be without any force or effect.

11. TERM; TERMINATION; SURVIVAL. All sections of this DPA relating to the rights and obligations of the parties concerning Leidos Data disclosed during the term of the Contract Agreement shall survive any such termination. Notwithstanding the foregoing, Receiving Party may retain information that it is expressly required by law to retain, so long as Receiving Party does not use the information and retains it only for the period required by law in a secure and confidential manner. Provisions of this DPA which by their nature are intended to survive termination or expiration of the Contract Agreement will survive any expiration or termination of the Contract Agreement, including without limitation all sections of this DPA relating to the rights and obligations of Receiving Party concerning Leidos Data disclosed. Leidos may terminate the Contract Agreement immediately without providing an opportunity to cure upon written notice to Receiving Party if Receiving Party breaches its obligations under the DPA.

12. MISCELLANEOUS.

12.1. Notices. All notices or other written communications required or permitted to be given under any provision of this Agreement, including without limitation changes of name or address to which such notices or other written communications are to be delivered under this Section, shall be deemed to have been given by the notifying party if mailed by certified mail, return receipt requested, to the receiving party addressed to its mailing address set out below, or such other address as a party may designate in writing to the other party. All notices shall be given or made to:

Leidos:

COMPANY:

12.2. Indemnification. In addition to and without limiting any indemnification obligations of Receiving Party pursuant to other provisions of the Agreement, Receiving Party will defend at its own expense Leidos and its affiliates (and their respective officers, directors, employees, agents, successors and assigns) (collectively "Leidos Indemnitees") and others claiming through Leidos from and against any and all actual or threatened Losses arising from or in connection with, or based on allegations whenever made of, any of the following claims, and in addition, Receiving Party will indemnify and hold harmless any Leidos Indemnitees for Losses arising from or in connection with any of the following: (a) any violation or breach of this DPA and any associated Exhibits; (b) any Security Incident; (c) any fraud, negligence or willful misconduct of Receiving Party, Receiving Party personnel, or any third party to whom Receiving Party provides access to Leidos Data or to Receiving Party's systems that interact with Leidos Data; (d) remedial action(s) taken by Leidos as the result of a Security Incident (including any data breach notification and/or credit monitoring resulting from a data breach caused by Receiving Party or Receiving Party personnel); and (e) any other costs incurred by Leidos with respect to Leidos' rights in this DPA and any associated Exhibits. Receiving Party will be fully responsible for and will pay all costs and expenses incurred by Receiving Party or Receiving Party personnel with respect to this DPA.

12.3. Limitation of Liability. NOTWITHSTANDING THE LIMITATION OF LIABILITY IN THE CONTRACT AGREEMENT, PARTIES AGREE THAT DAMAGES OR LIABILITY ARISING OUT OF ANY OF THE FOLLOWING: (A) ANY VIOLATION OR BREACH OF THIS DPA AND ANY ASSOCIATED EXHIBITS; (B) ANY SECURITY INCIDENT; OR (C) ANY FRAUD, NEGLIGENCE OR WILLFUL CONDUCT OF RECEIVING PARTY, RECEIVING PARTY PERSONNEL, OR ANY THIRD PARTY TO WHOM RECEIVING PARTY PROVIDES ACCESS TO LEIDOS DATA OR TO RECEIVING PARTY'S SYSTEMS THAT INTERACT WITH LEIDOS DATA WILL NOT BE SUBJECT TO THE LIMITATION OF LIABILITY IN THE CONTRACT AGREEMENT.

12.4. Injunctive Relief. Receiving Party agrees that any Security Incident may cause immediate and irreparable harm to Leidos for which money damages may not constitute an adequate remedy. Accordingly, Receiving Party agrees that Leidos may seek injunctive or other equitable relief and Receiving Party, at its own expense, will take all steps reasonably requested by Leidos to limit, stop or otherwise remedy a Security Incident.

EXHIBIT A TO THE DPA

Information Security Obligations Exhibit

1. Definitions. Capitalized terms used herein shall have the meanings set forth in this Section 1.

"**Applicable Laws**" means all federal, state, local and foreign laws, statutes, regulations, ordinances, codes, rules, orders, decisions and directives including, but not limited to, Export-Control Laws and Regulations and EU Data Protection Legislation, that apply to the Parties or the subject matter of this Exhibit.

"**Authorized Agents**" means third parties who have a need to know or otherwise access Confidential Information to enable Seller to perform its obligations under this Exhibit and the Contract Document, and who are bound in writing by confidentiality and other obligations sufficient to protect Confidential Information in accordance with the terms and conditions of this Exhibit and the Contract Document.

"**Authorized Employees**" means Seller employees who have a need to know or otherwise access Confidential Information to enable Seller to perform its obligations under this Exhibit and the Contract Document, and who are bound in writing by confidentiality and other obligations sufficient to protect Confidential Information in accordance with the terms and conditions of this Exhibit and the Contract Document.

"**Authorized Persons**" means (i) Authorized Employees; and (ii) Authorized Agents.

"**Confidential Information**" means (i) any information, regardless of form and regardless of whether disclosed before, on or after the date of this Exhibit, that is proprietary or maintained in confidence by Leidos including, but not limited to, unpublished patent applications, technical data or know-how relating to discoveries, ideas, inventions, concepts, hardware, software, designs, drawings, specifications, demonstration or test scripts, content under development, techniques, processes, models, data, documentation, diagrams, flow charts, research, development, business plans or opportunities, business strategies, future projects, products or services, projects, products, services or projects under consideration, organization, methodologies, policies and procedures, and information related to finances, costs, prices, Suppliers, partners, customers and employees that is disclosed by Leidos or on behalf of Leidos, directly or indirectly, in writing, orally, by drawings or inspection of equipment or software, by entering in, transmitting by or through, or otherwise transferred to software or equipment that is used hereunder, or that is transmitted by or through the services (including information that is provided by or on behalf of Leidos for the purpose of entering such information in, transmitting such information by or through, or otherwise transferring such information to software, equipment or the services), to Seller or any of its employees or agents; (ii) any other information that is processed at any time by Seller; (iii) Highly Confidential Information, Personal Information, Controlled Data, and Sensitive Personal Information belonging to Leidos or a third party; and (iv) any information derived from the information described in (i) - (iv) above.

"**Contract Document**" means the relevant agreement, contract, statement of work, task order, purchase order, or other document governing the provision of goods, services, and/or deliverables by Seller to Leidos. In the event of any conflict or inconsistency between the Contract Document and this Exhibit, the terms of the Exhibit will take precedent.

"**Controlled Data**" means technical or government information with distribution and/or handling requirements prescribed by law including, but not limited to, controlled unclassified information, covered defense information, and license-required export controlled data, which is provided by Leidos to Seller in connection with the performance of this Exhibit or the Contract Document.

"**Disabling Devices**" means computer instructions or code intended by Seller to erase data or programming or otherwise cause the software or systems to become inoperable or incapable of being used in the full manner for which it was designed or created,.

"**Export-Control Laws and Regulations**" means laws and regulations of the United States and non-U.S. jurisdictions that restrict unauthorized release to foreign person and unauthorized export to foreign locations, including but not limited to the International Traffic in Arms Regulations (ITAR), 22 CFR §§120-130, and the Export Administration Regulations (EAR), 15 CFR §§730-774.

"**EU Data Protection Legislation**" collectively refers to European Union's Directive 95/46/EC, the General Data Protection Regulation (GDPR) (or Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016), and any other data protection or privacy legislation currently in force in the European Economic Area ("EEA").

"**Highly Confidential Information**" is Confidential Information that Leidos identifies as "Highly Confidential," "Restricted," or similar in the Contract Document or at the time of disclosure.

"Leidos Data" means (i) all information, whether or not Leidos Confidential Information, entered in, transmitted by or through, or otherwise transferred to software or equipment that is utilized hereunder, or that is transmitted by or through the services, each by or on behalf of Leidos (including information that is provided by or on behalf of Leidos for the purpose of entering such information in, transmitting such information by or through, or otherwise transferring such information to software, equipment or the services); (ii) any other information that is processed at any time by Seller or any of its employees or agents in connection with or incidental to the performance of the Contract Document; and (iii) any information derived from the information described in (i)-(ii) above.

"**Information Security Program**" means a documented set of policies, procedures, guidelines, standards and risk assessments including, but not limited to, cyber security governance business continuity and disaster recovery, change management, cryptographic protections, endpoint security, and incident response, designed to enhance effective security management practices and controls and ensure the confidentiality, integrity, and availability of data and information of clients, customers and the organization itself.

"**Leidos Information System(s)**" means any system(s) and/or computer(s) managed by Leidos, which includes laptops and network devices.

"**Mobile Devices**" means tablets, smartphones, and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

"**Personal Information**" means (i) that subset of Confidential Information that relates to or can be attributed to an identified or identifiable natural person; (ii) information concerning an identified or identifiable natural person that is protected by Applicable Laws; and (iii) any information or data that can be used to identify individuals – either on its own or in combination with other information.

"**Process(ing)**" means to perform any operation or set of operations upon Personal Information, 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.

"**Security Breach**" means (i) disclosure or potential disclosure of information to unauthorized persons, or a violation of the security policy of a Seller Information System, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred; (ii) a material violation of Seller's Information Security Program, where any such breach may have, or has, resulted in unauthorized access to, the Confidential Information; (iii) receipt of a complaint in relation to the privacy, data protection, and/or data security practices of Seller relating to Leidos Data; and/or (iv) a breach or alleged breach of this Exhibit relating to such privacy, data protection, and/or data security practices. Without limiting the foregoing, a Security Breach shall include any unauthorized access to, disclosure of, or acquisition of Personal Information.

"**Sensitive Personal Information**" means that category of Personal Information considered to be especially sensitive and subject to additional protections, which includes: (i) medical records and other health information - such as Protected Health Information (PHI) as defined in and subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) - and "personal health information" or "health information" as defined in similar laws; (ii) bank account and payment card information and other financial account information; (iii) Leidos' bank account and payment card information; (iv) government and national identifiers (*e.g.*, National Identification Numbers; Social Security Numbers); (v) Sensitive or Special Categories of Personal Data under Directive 95/46/EC of 24 October 1995; and (vi) genetic and biometric data and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, familial or home life information and sexual orientation.

"**Subcontractor**" means an entity providing good, products, services and/or deliverables under this Exhibit and a Contract Document to Leidos pursuant to a subcontract.

"**Supplier**" means an entity providing goods, products, services, and/or deliverables to Leidos under this Exhibit and a Contract Document to Leidos pursuant to a supply agreement.

"**Seller**" means Supplier and/or Subcontractor.

"**Seller Information System(s)**" means any system(s) and/or computer(s), including laptops, network devices and Mobile Devices, owned or operated by or on behalf of Seller and used to process, store, transmit and/or access Confidential Information.

"**Viruses**" means computer instructions, devices or techniques that can or were designed to, threaten, infect, assault, analyze, defraud, disrupt, damage, disable, alter, inhibit, or shut down Leidos' systems including, but not limited to, other programs, data storage, and computer libraries or otherwise prevent Leidos from using the information as intended.

2. Information Security.

(a) Seller represents and warrants that (i) the products and services provided by Seller do not contain any Viruses and Disabling Devices; and (ii) it will use the latest available and most

comprehensive Virus detection/scanning program prior to any attempt to access any of Leidos' computing systems and/or networks and upon detecting a Virus, all attempts to access Leidos' systems and/or networks will immediately cease and will not resume until any such virus has been eliminated.

(b) Seller shall (i) implement and maintain an Information Security Program that is audited at least annually; (ii) upon request by Leidos, provide a copy of the results of a security audit within five (5) business days of such request; (iii) fully cooperate, in a timely manner, with Leidos and provide Leidos with assistance as it may reasonably require in connection with its review of the results of a security audit; (iv) remediate any deficiencies impacting the Confidential Information identified by a security audit within thirty (30) days.

(c) Receiving Party will maintain a comprehensive written security policy that (a) complies with Industry Standards including, but not limited to DFAR 252.204 7012 requirement to be compliant with NIST 800-171 and any successor standards; (b) complies with the ongoing requirements of this DPA including the Safeguard Obligations; and (c) applies across its entire organization and those of its subcontractors. Receiving Party will regularly, but in no event less than annually, evaluate, test and monitor the effectiveness of the security policy and will promptly adjust and/or update the security policy as reasonably warranted by the results of such evaluation, testing, and monitoring.

Receiving Party will:

(i) Provide Leidos with information regarding all Receiving Party's policies, procedures and security practices, including without limitation [*insert known documents of Receiving Party*], and if confidential, provide Leidos with the right to review any such information deemed confidential or proprietary at Receiving Party's facilities upon Leidos' reasonable request;

(ii) Benchmark Receiving Party's policies and procedures and improve and update them from time-to-time to reflect new laws and regulations, new industry standards, and new threats, vulnerabilities, hazards and accidents.

(d) Without limiting Seller's obligations under Section 3(a), Seller shall implement administrative, physical, and technical safeguards to protect Leidos Information from unauthorized access, acquisition, disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than best industry practices, including, but not limited to, the International Organization for Standardization's standards: ISO/IEC 27001 – Information Security Management Systems – Requirements, ISO/IEC 27002 – Code of Practice for International Security Management, and the National Institute of Standards and Technology (NIST) SP 80053r4 Security and Privacy Controls for Federal Information System and Organizations . Seller shall ensure that all such safeguards, including the manner in which Leidos Information is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with Applicable Laws as well as the terms and conditions of this Exhibit.

(e) Seller shall cooperate with Leidos in Leidos' compliance with current and future regulatory requirements applicable to Leidos. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (*e.g.*, E.U. Model Contractual Clauses, U.S. Protected Health Information Agreement), compliance with additional security requirements (*e.g.*, DFARS 252.204-7012, Payment Card Industry Data Security Standard (PCI DSS) requirements), completion of regulatory filings and participation in regulatory audits.

(f) At a minimum, Seller's safeguards for the protection of Leidos Information shall include: (i) limiting access of Confidential Information to Authorized Persons; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) ensuring export-controlled data is stored within territories specified by applicable export laws and regulations; (vii) restricting access to export controlled data to only those persons permitted access under applicable export-control laws and regulations; (viii) encrypting Confidential Information stored on any media; (ix) encrypting Confidential Information transmitted over public or wireless networks; (x) segregating Confidential Information from information of Seller or its other customers so that Confidential Information is not commingled with any other types of information; (xi) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Seller's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (xii) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xiii) providing to Seller's employees at least annual privacy and information security training – which shall, at a minimum, meet the requirements of all applicable privacy, data protection, and information security laws, regulations, and industry standards.

(g) The baseline safeguards described in Section 2(e) shall include:

(i) Physical Access. Seller shall maintain physical security standards designed to prohibit unauthorized physical access to Seller facilities and equipment by using the following practices:

(A) Limiting physical access to locations to Seller employees, subcontractors, and authorized visitors;

(B) Issuing identification cards that must be worn while on premises to Seller employees, subcontractors, and authorized visitors;

(C) monitoring access to Seller facilities, including restricted areas and equipment within facilities;

(D) logging, monitoring and tracking access to the data center where Leidos data is hosted; and

(E) securing data centers with alarm systems and video cameras.

(ii) Access Control and Administration. The Seller shall maintain the following standards for access control and administration of the relevant IT environment:

(A) Restrict administrator accounts to only for the purpose of performing administrative activities;

(B) Require each account with administrative privileges to be traceable to a uniquely-identifiable individual;

(C) Require all access to computers and servers to be authenticated and within the scope of an employee's job function;

(D) Require initial passwords be changed by the user on first use;

(E) Mask, suppress, or otherwise obscure the display and printing of passwords such that unauthorized parties are not be able to observe or subsequently recover them;

(F) Require that passwords must be uniquely identifiable to an individual;

(G) Require passwords must be encrypted when transmitted;

(H) Require password complexity or more than 3 out of 4 character classes and require character class choices such as upper case letters, lower case letters, numeric digits or special characters;

(I) Password length must be configured to be at a minimum 8 characters;

(J) Passwords must expire every 90 days;

(K) Require automatic time-out of access to computers and servers if left idle with the requirement for password authentication for re-access; and,

(L) Require that accounts be set to lockout after several erroneous failed login attempts.

(iii) Virus Scanning and Logging. Seller shall ensure that computers and servers have reasonable up-to-date versions of system security software, which includes host firewall, anti-virus protection, and up-to-date patches and virus definitions. Software shall be configured to scan for and promptly remove or fix identified findings. Seller shall maintain logs of various components of the infrastructure and an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks. Seller shall review access logs on servers and security events and retain network security logs for 180 days.

(iv) Vulnerability Assessment and Penetration Testing. Upon request, Seller shall provide to Leidos a summary of vulnerability assessments for Seller Information Systems.

(h) During the term of each Authorized Employee's employment by Seller, Seller shall at all times cause such Authorized Employees to comply with Seller's obligations under this Exhibit, the applicable Contract Documents, and Seller's Information Security Program. Seller further agrees that it shall maintain a disciplinary policy and procedure to address any unauthorized access, use, or disclosure of Confidential Information by any of Seller's officers, partners, principals, employees, agents, or contractors. Upon Leidos' written request, Seller shall promptly identify for Leidos in writing all Authorized Persons as of the date of such request.

(i) Seller shall provide thirty (30) days prior written notice to Leidos containing a reasonably detailed description of a proposed modification which may impact the security of the Seller Information Systems, including a reasonably detailed description of any new or additional risks to the Confidential Information.

3. Security Breach Procedures.

(a) Seller shall:

(i) provide Leidos with the name and contact information or Seller authorized contact person which shall serve as Leidos' primary security contact and shall be available to assist Leidos twenty-four (24) hours per day, seven (7) days per week in resolving issues associated with a Security Incident;

(ii) notify Leidos of a Security Incident as soon as practicable and without undue delay, but no later than forty-eight (48) hours after Seller becomes aware of the Security Incident, by telephone at the following numbers with notice to Seller's primary business contact within Leidos.

U.S.: 855-9-LEIDOS (855-953-4367)
U.K.: 0800 999 5533
AU: +61 (1) 800 LEIDOS (534 367)
Africa, Europe, Middle East: + 44 1489 568564
Other Non-U.S.: 00 + 1 + 601-460-2000

(b) Immediately following Seller's notification to Leidos of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident.

(c) Seller shall, at its own expense, immediately contain and remedy any Security Incident and prevent any further Security Incident including, but not limited to, taking any and all actions necessary to comply with applicable privacy and data protection rights, laws, regulations, and standards.

(d) Receiving Party shall, at its expense, investigate any Security Incident, including without limitation, (i) if possible, recover Leidos Data and prevent further unauthorized use, disclosure or loss of Leidos Data, including without limitation seeking appropriate injunctive relief or otherwise preventing or curtailing such threatened or actual breach; and (ii) comply with any Applicable Laws, including without limitation laws requiring notice to be provided to affected individuals regarding any such unauthorized disclosure of Leidos Data.

(e) Receiving Party shall provide Leidos and third party Suppliers and investigators acting on behalf of Leidos with access to all information, individuals, officers, networks, software, hardware, systems and any other person, place or thing necessary to respond to the Security Incident, including without limitation investigating the incident, making a determination of legal and contractual responsibilities, identifying the risk of harm to affected individuals, identifying the names and contact information for the affected individuals, mailing notifications, providing remediation to affected individuals, responding to questions from affected individuals, regulators and customers, and responding to regulators and any criminal or civil actions arising out of the Security Incident.

(f) Seller shall reimburse Leidos for all actual costs incurred by Leidos in responding to, and mitigating damages caused by, any Security Incident directly or indirectly caused by Seller's acts or omissions, including all costs of notice and/or remediation pursuant to Section 3(e).

(g) Seller shall not inform any third party of any Security Breach without first obtaining Leidos' prior written consent. Further, Seller agrees that Leidos shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in Leidos' 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.

(h) Seller shall maintain and preserve all documents, records, and other data related to any Security Incident.

(i) Seller shall fully cooperate at its own expense with Leidos in any litigation, investigation, or other action deemed necessary by Leidos including providing any required forensic computer work, to protect its rights relating to the use, disclosure, protection, and maintenance of Confidential Information.

(j) Seller shall provide (i) individuals affected by the unauthorized acquisition and/or misuse of Personal Information with credit monitoring services designed to protect against potential fraud associated with identity theft crimes for a specific period not to exceed twelve (12) months, to the extent the unauthorized acquisition and/or misuse of the affected individual's personal information could lead to a compromise of the individual's credit or credit standing; and (ii) reasonable call center support for such affected individuals for a specific period not to exceed thirty (30) calendar days.

(k) Receiving Party shall indemnify, defend and hold harmless Leidos against all costs, fees, expenses, damages and fines related to or arising out of the Security Incident and any violation of Receiving Party's privacy and security obligations in this DPA and the Contract Agreement, including without limitation the following:

(i) Receiving Party's costs, fees, expenses, damages and fines;

(ii) Third party forensic review or investigation of the Security Incident;

(iii) Payments for the return of Leidos Data involved in the Security Incident;

(iv) Notification to customers or regulatory authorities as required by Applicable Law or contract provision;

(v) Notification to all affected individuals if notification is required to any affected individual by Applicable Law or contract provision;

(vi) Notification to all affected individuals whose non-electronic Leidos Data is involved in the Security Incident if notification would have been required by Applicable Law, regulation or contract provision, if Leidos Data were in electronic form;

(vii) Establishing a call center to answer the calls of individuals affected by the Security Incident;

(viii) Remedying and otherwise mitigating any potential damage or harm posed by the Security Incident to the affected individuals, including without limitation any costs of providing credit monitoring or credit restoration services, as appropriate;

(ix) Payments to attorneys and Suppliers who assist Leidos or Receiving Party in responding to the Security Incident, including without limitation responding to individuals, regulators and lawsuits arising out of the Security Incident and the Parties' actions once aware of the Security Incident;

(x) Amounts Leidos or Receiving Party must pay arising out of actions of a regulator with respect to a Security Incident, including without limitation any fines, penalties, costs, or other amounts arising out of compliance with orders or consent decrees; and

(xi) Amounts arising from any criminal or civil litigation regarding the Security Incident and the actions taken or not taken by Receiving Party with respect to the Security Incident.

(l) In the event of a Security Incident, Leidos may suspend or discontinue Receiving Party or its subcontractor's access or connectivity to the Leidos system or Leidos Data. Under no circumstances will such suspension or discontinuance of access or connectivity constitute a breach or default by Leidos of this DPA, the Contract Agreement and/or any other agreement established with Leidos.

4. Oversight of Security Compliance.

(a) At least once per year, Seller shall conduct site audits of the information technology and information security controls for all Seller Information System(s) and facilities used in performing its obligations under this Exhibit and the applicable Contract Document including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices. Upon Leidos' written request, Seller shall make available to Leidos for review all of the following, as applicable: Seller's latest Payment Card Industry (PCI) Compliance Report, Statement on Standards for Attestation Engagements (SSAE) No. 16 audit reports for Reporting on Controls at a Service Organization, Service Organization Controls (SOC) Type 1, 2, or 3 audit reports, and any reports relating to its ISO/IEC 27001 certification. Leidos shall treat such audit reports as Seller's Confidential Information under this Exhibit. Seller will promptly address any exceptions noted on the SOC reports, or other audit reports, with the development and implementation of a corrective action plan by Seller's management.

(b) Upon Leidos' written request, no more than once per year, Seller agrees to respond to a reasonable information security questionnaire concerning its security practices specific to the provision of goods, services and/or deliverables provided hereunder.

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

6. Equitable Relief. Seller acknowledges that any breach of this Exhibit or Seller's Information Security Program, a copy of which has been provided to Leidos, may cause Leidos irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Leidos shall be entitled to 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 Leidos may be entitled at law or in equity, without the posting of a bond or other security. 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.

7. Material Breach. Seller's failure to comply with any of the provisions of this Exhibit is a material breach of this Exhibit. In such event, Leidos may terminate this Exhibit and/or applicable Contract Document effective immediately upon written notice to Seller without further liability or obligation to Seller.

8. Indemnification. Seller shall defend, indemnify, and hold harmless Leidos and its subsidiaries, affiliates, and its respective officers, directors, employees, agents, successors, and permitted assigns (each, a "Leidos 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, arising out of or resulting from (i) any Security Breach directly or indirectly caused by Seller's acts or omissions; (ii) Seller's breach of this Exhibit; (iii) Seller's violation of Applicable Laws; and (iv) Seller's gross negligence or willful misconduct.

9. Lower-Tier Subcontracts. Seller shall include the applicable provisions of this Exhibit in all subcontracts under the applicable Contract Document if Seller's subcontractors and/or suppliers will have access to Confidential Information.

EXHIBIT B TO THE DPA

DATA PROCESSING OBLIGATIONS

This Exhibit B (Data Processing Obligations) is entered by and between _____ ("Data Controller") and _____ ("Data Processor") in connection with the agreement between the parties entitled [*Name of the Agreement*], dated [*Date of Agreement*] ("Contract Agreement").

This Exhibit B is entered into to provide adequate safeguards with respect to the protection of Personal Information and/or EU Personal Data (as defined below) that Data Processor will Process on behalf of Data Controller in accordance with the Contract Agreement and Services.

Data Controller and Data Processor agree that this Exhibit B and the Processing performed under this Exhibit B are subject to the terms and conditions of the Contract Agreement.

1. DEFINITIONS.

1.1. To the extent they are not defined below, capitalized terms in this Exhibit B have the meaning given to them in the Contract Agreement, the Statement of Work, dated [*date of SOW*] and Data Protection Addendum ("DPA"), as applicable.

1.2. "Applicable Law(s)" means any applicable law, rule, or regulation applicable to the Contract Agreement, the Services, Leidos or Supplier, and applicable Industry Standards concerning, but not limited to the following, privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing of Personal Information.

1.3. "Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing Personal Information, including EU Personal Data.

1.4. "Data Processor" means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of a Data Controller.

1.5. "Data Subject" means the individual about whom specific Personal Information relates.

1.6. "EU Data Protection Legislation" collectively refers to European Union's Directive 95/46/EC, GDPR, and any other data protection or privacy legislation in force in the European Economic Area ("EEA").

1.7. "EU Personal Data" means any information that relates to an identified or identifiable living individual who resides in the European Union ("EU"), either on its own or in combination with other information. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

1.8. "GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of the EU.

1.9. "Leidos Data" means (i) all information, whether or not Leidos Confidential Information, entered in, transmitted by or through, or otherwise transferred to software or equipment that is utilized hereunder, or that is transmitted by or through the Services, each by or on behalf of Leidos (including information that is provided by or on behalf of Leidos for the purpose of entering such information in, transmitting such information by or through, or otherwise transferring such information to software, equipment or the Services); (ii) any other information that is Processed at any time by Receiving Party or Receiving Party personnel in connection with or incidental to the performance of the Contract Agreement; and (iii) any information derived from the information described in (i)-(ii) above. Personal Information is a component of Leidos Data.

1.10. "Personal Information" means (i) that subset of Leidos Data that relates to or can be attributed to an identified or identifiable natural person; (ii) information concerning an identified or identifiable natural person that is protected by Applicable Laws, including the EU Data Protection Legislation; and/or (iii) any information or data that can be used to identify individuals – either on its own or in combination with other information. Personal Information may include EU Personal Data.

1.11. "Processing," or any variation thereof, means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12. "Receiving Party" means "[*Name of Supplier*]."

1.13. "Security Incident" means any suspected or actual (i) unauthorized Processing of Leidos Data (including Personal Information) (such as loss or unauthorized use, accidental or unlawful destruction, alteration, disclosure or acquisition of or access to such information) or an occurrence in which Leidos Data has been compromised or there is a reasonable suspicion that Leidos Data may have been compromised by any means, including by data breach or resulting in data loss, and for which review of Applicable Laws may be desired by Leidos or required in order to comply with Applicable Laws; or (ii) unauthorized use of, disclosure of, or access to Receiving Party's systems, Leidos Data, physical intrusion of facilities, or theft, misappropriation or loss of documents, or storage media.

1.14. "Services" means the performance of the Receiving Party under the Contract Agreement.

1.15. "Sub-processor" means any Third Party appointed by or on behalf of Receiving Party to Process Personal Information and/or EU Personal Data on behalf of Leidos.

1.16. "Third Party" means: (i) a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, or Data Processor; and (ii) persons who, under the direct authority of the Data Controller or Data Processor, are authorized to Process Personal Information and/or EU Personal Data.

2. **Processing of Personal Information and/or EU Personal Data.**

2.1. Receiving Party:

2.1.1. Acts as a Data Processor and will Process Personal Information and/or EU Personal Data on behalf of Leidos;

2.1.2. Will comply with all Applicable Laws, including the EU Data Protection Legislation (including but not limited to Article 28(3) of the GDPR), in Processing Personal Information and/or EU Personal Data on behalf of Leidos;

2.1.3. Will assist Leidos in ensuring compliance with any obligations under Applicable Laws with respect to the Processing (including but not limited to Articles 32 to 36 of the GDPR), taking into account the nature of Processing and the information available to the Receiving Party;

2.1.4. Will Process Personal Information only on documented instructions from Leidos, including with regard to transfers of Personal Information to a third country or an international organization, unless Processing is required by Applicable Laws; in which case, Receiving Party will inform Leidos of that legal requirement before the relevant Processing, to the extent permitted by Applicable Laws and/or unless that law prohibits such information on important grounds of public interest;

2.1.5. Will ensure that persons authorized to Process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.1.6. Will take all measures required pursuant to Article 32 of the GDPR; and

2.1.7. Will immediately inform Leidos if, in its opinion, and instruction from Leidos infringes the GDPR or other EU Data Protection Legislation.

2.2. Leidos will provide instructions to Receiving Party to Process Personal Information and/or EU Personal Data and transfer Personal Information and/or EU Personal Data to any country or territory as reasonably necessary for the services contemplated in the

Contract Agreement and consistent with the terms in the Contract Agreement, the DPA, and/or this Exhibit B.

2.3. Appendix 1 to this Exhibit B sets out certain details regarding the Processing of Personal Information and/or EU Personal Data on behalf of Leidos. Leidos may make reasonable amendments or updates to Appendix 1 by written notice to Receiving Party as Leidos reasonably considers necessary to meet the requirements in the Contract Agreement, the DPA, and/or this Exhibit B or in connection with the Services.

3. **Sub-processors**. Receiving Party may appoint and engage Sub-processors in accordance with the terms of this Exhibit B. Receiving Party will also respect the conditions referred to in Article 28(2) and Article 28(4) of the GDPR for engaging another Data Processor.

3.1. Receiving Party must not appoint, engage, or change any Sub-processor to Process Personal Information and/or EU Personal Data on behalf of Leidos, except with the prior written consent of Leidos.

3.2. Receiving Party must carry out adequate due diligence to ensure that the Sub-processor is capable of complying with the requirements of all Applicable Laws, the Contract Agreement, the DPA, this Exhibit B and [*insert any other documents as appropriate*]. Receiving Party will provide Leidos with the results of that due diligence within ten (10) days of Leidos' request.

3.3. Receiving Party must give Leidos written notice of the appointment, engagement, or change of a Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. Such written notice may take the form of Appendix 2 of this Exhibit B. If, within fifteen (15) days of receipt of that notice, Leidos provides any written objections to the proposed appointment:

3.3.1. Receiving Party will not appoint that proposed Sub-processor until reasonable steps have been taken to address the objections raised by Leidos and Leidos has been provided with a response to those objections and agrees to the appointment of that proposed Sub-processor. In the event that Leidos continues to have objections to the proposed Sub-processor, Leidos may by written notice to Receiving Party with immediate effect terminate the Contract Agreement to the extent it requires the use of a proposed Sub-processor.

3.3.2. Receiving Party will work with Leidos in good faith to avoid the use of that proposed Sub-processor for the Services and/or Processing Personal Information and/or EU Personal Data on behalf of Leidos. In the event that the use of the proposed Sub-processor cannot be avoided, Leidos may by written notice to Receiving Party with immediate effect terminate the Contract Agreement to the extent it requires the use of a proposed Sub-processor.

3.4. Prior to the appointment or engagement by a Sub-processor, Receiving Party will ensure that the arrangement with the Sub-processor is governed by a written contract including the terms in the Contract Agreement, the DPA, and this Exhibit B (or terms that at least offer the same level of protection for Leidos Data). Receiving Party will provide Leidos

with copies of such agreements within five (5) days of Leidos' request.

3.5. By contract or other legal act, Receiving Party will ensure that each Sub-processor Processes Personal Information and/or EU Personal Data on behalf of Leidos under the same data protection obligations under this Exhibit B, including but not limited to Sections 2.1, 4, 5, 6, and 7.

3.6. In the event the Sub-processor violates or fails to fulfill its data protection obligations, Receiving Party will be liable for such violations and will remain liable to Leidos for the performance of the Sub-processor's obligations.

4. **Data Subject Rights**.

4.1. Taking into account the nature of Processing, Receiving Party will implement appropriate administrative, physical, organizational, and technical measures to assist Leidos without undue delay in complying with Leidos' obligations under the Applicable Laws to respond to requests to exercise Data Subject's rights.

4.2. Receiving Party will: (i) promptly notify Leidos if it receives a request from a Data Subject regarding Personal Information and/or EU Personal Data Receiving Party is Processing on behalf of Leidos; and (ii) not respond to a request from a Data Subject without documented instructions from Leidos or as required by Applicable Laws, in which case Receiving Party will information Leidos of the legal requirement before Receiving Party responds to the request to the extent Receiving Party is permitted by Applicable Laws.

5. **Data Security Requirements and Security Incidents**.

5.1. Receiving Party will comply, and ensure any applicable Sub-processors comply, with the requirements in the DPA and this Exhibit B when Processing Personal Information and/or EU Personal Data on behalf of Leidos, including any applicable data security and confidentiality requirements.

5.2. Taking into account generally accepted industry standards, the costs of implementation, and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Receiving Party will implement, and ensure any applicable Sub-processors implement, appropriate administrative, technical, physical, and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, any measures referred to in the EU Data Protection Legislation, including but not limited to: (i) the pseudonymization and encryption of Personal Information; (ii) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident and/or Security Incident; (iv) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing; and (v) the implementation of a written security policy with respect to the Processing of Personal Information.

5.3. Receiving Party will comply, and ensure any applicable Sub-processors comply, with the requirements in the DPA and this Exhibit B, in the event there has been, or it is reasonable to believe that there has been, a Security Incident.

6. **Deletion or Return of Personal Information and/or EU Personal Data.** Within ten (10) days of Leidos' request or completion of the Services relating to Processing set out in the Contract Agreement, at Leidos' sole option, Receiving Party will: (i) return all (or in part) originals, copies, reproductions and summaries of Leidos Data (including Personal Information) and all other tangible materials and devices provided to Receiving Party as Leidos Data; or (ii) certify disposal of the same, except as necessary to comply with Applicable Laws. Both parties will agree to an acceptable transfer or disposal methodology as applicable. Receiving Party will maintain appropriate administrative, physical, organizational, and technical safeguards to ensure the security, confidentiality, and integrity of Leidos Data during such transfer or disposal.

7. **Audit Rights**. Receiving Party will allow for and contribute to audits, including inspections, conducted by Leidos or another auditor mandated by Leidos. Receiving Party will comply, and ensure any applicable Sub-processors comply, with the audit requirements in the DPA. Receiving Party will also make available to Leidos all information necessary to demonstrate compliance with Receiving Party's obligations under Applicable Laws and this Exhibit B.

8. **Restricted Transfers**. Receiving Party may transfer or otherwise Process Personal Information outside the EEA. Should such a transfer be required, Receiving Party will immediately notify Leidos, and Receiving Party and Leidos will enter into the appropriate Standard Contractual Clauses (Exhibit C) with respect to any transfer of Leidos Data.

9. **Limitation of Liability**. RECEIVING PARTY WILL COMPLY, AND ENSURE ANY APPLICABLE SUB-PROCESSORS COMPLY, WITH THE "LIMITATION OF LIABILITY" SECTION IN THE CONTRACT AGREEMENT AND/OR THE DPA.

10. **Indemnification**. Receiving Party will comply, and ensure any applicable Sub-processors comply, with the "Indemnification" section in the Contract Agreement and/or the DPA.

11. **Termination.** This Exhibit B will continue in full force and effect until the later of: (i) termination of the Contract Agreement; or (ii) when Receiving Party and any applicable Sub-processors stop Processing Personal Information on behalf of Leidos. Leidos may terminate the Contract Agreement immediately without providing an opportunity to cure upon written notice to Receiving Party if Receiving Party and/or any applicable Sub-processor breaches its obligations under this Exhibit B.

APPENDIX 1 TO EXHIBIT B

DETAILS OF PROCESSING OF PERSONAL INFORMATION AND/OR EU PERSONAL DATA

This Appendix 1 includes details of the Processing of Personal Information and/or EU Personal Data.

1. Subject Matters and Duration.

   The subject matter and duration of Processing Personal Information and/or EU Personal Data on behalf of Leidos are set out in the Contract Agreement [*and/or other documents such as Statements of Work*]

2. Nature and Purpose of Processing Personal Information and/or EU Personal Data

3. Types of Personal Information and/or EU Personal Data to be Processed

4. Categories of Data Subject to whom the Personal Information and/or EU Personal Data Relate

APPENDIX 2 TO EXHIBIT B

PROPOSED SUB-PROCESSORS

This Appendix 2 includes information regarding the proposed Sub-processors.

1. Name of Sub-processor:

    a. Point of Contact:

    b. Address:

    c. Telephone:

    d. Subject Matters and Duration of Processing:

    e. Nature and Purpose of Processing Personal Information and/or EU Personal Data:

    f. Types of Personal Information and/or EU Personal Data to be Processed:

    g. Categories of Data Subject to whom the Personal Information and/or EU Personal Data Relate:

2. Name of Sub-processor:

    a. Point of Contact:

    b. Address:

    c. Telephone:

    d. Subject Matters and Duration of Processing:

    e. Nature and Purpose of Processing Personal Information and/or EU Personal Data:

    f. Types of Personal Information and/or EU Personal Data to be Processed:

    g. Categories of Data Subject to whom the Personal Information and/or EU Personal Data Relate:

EXHIBIT C

STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR)

Standard Contractual Clauses (Controller to Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the Data Exporter:

Leidos, Inc. on behalf of and for the benefit of its Affiliate(s) (as defined in Appendix 3) located in the European Union and identified by Customer on Appendix 1 to the Clauses, who each are entitled to enforce the Clauses as independent data exporters (each such Affiliate, a 'Customer Affiliate')

and

Name of the Data Importer:.....

Address:.....

Tel.: ……; fax: .....; e-mail: .....

Other information needed to identify the organization:

……
(the Data Importer)

each a "party;" together "the parties;"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his

instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the Sub-processor'* means any processor engaged by the data importer or by any other Sub-processor of the data importer who agrees to receive from the data importer or from any other Sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the Sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any Sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for Sub -processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of Sub-processing, the processing activity is carried out in accordance with Clause 11 by a Sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for Sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of Sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the Sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any Sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a Sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the Sub-processor agrees that the data subject may issue a claim against the data Sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any Sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any Sub-processor preventing the conduct of an audit of the data importer, or any Sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Law of England and Wales (processing of employee data in the UK).

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the data importer under the Clauses. Where the Sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the Sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the Sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal

obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for Sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Law of England and Wales (processing of employee data in the UK).

4. The data exporter shall keep a list of Sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the Sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the Sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the Data Exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organization)

On behalf of the Data Importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organization)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES (EXHIBIT C)

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
……
……
Data importer
The data importer is (please specify briefly activities relevant to the transfer):
……
……
Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
……
……
Categories of data
The personal data transferred concern the following categories of data (please specify):
……
……
Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
……
……
Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
……
……

DATA EXPORTER
The data exporters are the entities listed in Appendix 3 to this Exhibit C.

Name:……
Authorized Signature ……

DATA IMPORTER
Name:……
Authorized Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES (EXHIBIT C)

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

……
……
……

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES (EXHIBIT C)

PARTIES

[PARTY NAMES TO BE INSERTED]