DATA PROTECTION EXHIBIT

This Data Protection Exhibit ("DPE"), dated as of _____, 20__ (the "Effective Date"), is incorporated by reference into the Contract Agreement by and between Leidos, Inc. ("Leidos") and _____ ("Supplier") (collectively, the "Parties"). The Parties agree that this DPE sets out the Parties' obligations with respect to the processing of Personal Information.

In the event of any conflict between the terms of the DPE and the Contract Agreement, the terms of the DPE will prevail. If the Standard Contractual Clauses are appended to the Contract Agreement, the terms of the Standard Contractual Clauses will prevail with respect to any conflict with the terms of the DPE.

1. Definitions

1.1. **"Contract Agreement(s)"** means the current agreement(s) between the parties entitled [Name(s) of the Agreement(s)], dated [Date(s) of named Agreement(s]. For purposes of this DPE, Contract Agreements include all associated statements of work, task orders, and purchase orders.

1.2. **"Data Protection Law(s)"** means any law, rule, regulation, or other legal requirement, applicable to the Processing, confidentiality, or security of Personal Information.

1.3. **"Data Subject Rights Request"** means any request by an individual to exercise rights provided under one or more applicable Data Protection Laws, such as the right to access or delete Personal Information.

1.4. **"Industry Standards"** means generally accepted security best practices as codified by standards setting bodies, such as the International Organization for Standardization, or by government authorities, such as the National Institute of Standards and Technology.

1.5. **"Personal Information"** means (1) information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual and (2) any other information concerning an identified or identifiable natural person that is protected under one or more Data Protection Laws. For purposes of this DPE, Personal Information refers to the Personal Information Supplier Processes in providing the Products or Services to Leidos.

1.6. **"Processing"** or any variation thereof, means any operation or set of operations performed on Personal Information or sets of Personal Information, whether or not by automated means. Processing includes, but is not limited to, collecting, recording, organizing, structuring, storing, retaining, adapting or altering, retrieving, consulting, using, disclosing, disseminating, combining, erasing, or destroying Personal Information.

1.7. **"Product(s)"** means any software, applications, cloud offerings, or other solutions provided by the Supplier under the Contract Agreement(s).

1.8. **"Security Incident"** means any actual or suspected (1) unauthorized access to or acquisition of Personal Information, (2) unauthorized use or disclosure of Personal Information, (3) unauthorized access to Supplier's systems that Process Personal Information or (4) theft or loss of any computing device, documents, or storage media containing Personal Information. A Security Incident does not include any pings, port

scans, denial of service attacks, or other unsuccessful attempts to access an information system containing Personal Information.

1.9. **"Sell"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating (orally, in writing, or by electronic or other means), Personal Information to a third party for monetary or other valuable consideration.

1.10. **"Services"** means the services provided by the Supplier under the Contract Agreement(s).

1.11. **"Subcontractor"** means any vendor, agent, independent contractor, or other third party, which provide products or services to Supplier involving the Processing of Personal Information.

1.12. **"Supplier"** means [Name of Supplier], including all affiliates and subsidiaries of Supplier which have or will have access to Personal Information.

2. Compliance with Data Protection Laws and Industry Standards

2.1. **Compliance with Data Protection Laws.** Supplier agrees to Process Personal Information in full compliance with all applicable Data Protection Laws and to protect the privacy and confidentiality of Personal Information to the same extent as is required of Leidos under applicable Data Protection Law(s). In the event Supplier determines that it can no longer comply with its obligations under applicable Data Protection Law(s), Supplier will promptly notify Leidos in writing.

2.2. **Information Security Program.** Supplier agrees to maintain an information security program that aligns with applicable Industry Standards and applies to all devices, systems, and networks owned by Supplier that Process Personal Information and any facilities at which Supplier Processes Personal Information.

3. Limits on Processing Personal Information

3.1. **Processing Roles.** The Parties agree that Supplier Processes Personal Information as a service provider and/or data processor to Leidos. Supplier agrees to Process Personal Information pursuant to Leidos' instructions, as set out in this DPE and the Contract Agreement(s).

3.2. **Processing Details.** Supplier agrees that it processes Personal Information for the purpose of providing the Products or Services as set out in the Contract Agreement. In connection with providing the Products or Services, Supplier may process [LIST SPECIFIC TYPES OF PERSONAL INFORMATION: e.g., name, business email address, personal email address, other contact information, employment-related information, health-related information, medical diagnosis and/or treatment information, government-issued identifiers, financial information, payment card information, biometric information, date of birth, employee identifiers, location information, payroll information]. Further, Supplier will Process Personal Information for no longer than necessary to provide the Products or Services and comply with applicable law(s).

3.3. **Processing Limitation.** Supplier will not Process Personal Information except (1) to provide the Products or Services in accordance with the terms of the Contract Agreement(s), and (2) as required to comply with applicable law.

3.4. **Responding to Judicial or Governmental Orders.** If Supplier is subject to a judicial or governmental order requiring Supplier to disclose Personal Information, Supplier will provide Leidos with prompt written notice of such order, unless prohibited from doing so by applicable law. Supplier agrees to provide such notice to Leidos far enough in advance of disclosing any Personal Information to allow Leidos an opportunity to seek a court protective order or its equivalent. If applicable law does not permit Supplier to notify Leidos of such judicial or other governmental order, Supplier shall request that the judicial or governmental entity requesting the disclosure of such Personal Information provide written assurance that it will afford such Personal Information the highest level of protection possible. Supplier agrees to abide by a "minimum necessary" standard and disclose only the portion of Personal Information required to be disclosed under such order.

3.5. **Prohibition on Selling Personal Information and Marketing.** Supplier shall not Sell any Personal Information. Supplier further agrees that it will not use Personal Information to send direct marketing communications, or for targeted advertising purposes, except to the extent such communications are part of the Services to be provided under the Contract Agreement.

3.6. **Aggregate Information.** Supplier may use Personal Information to create aggregate information only if such aggregate information: (1) does not identify and cannot be associated with any individual and (2) does not identify and cannot be associated with Leidos.

3.7. **De-Identified Information**. Supplier represents and warrants that it will not use, disclose, or otherwise process any Personal Information which has been de-identified (via the use of any technology, standard for de-identification, or by any other means) but which does not meet the requirements for aggregate information as set out in the prior section.

3.8. **Certification.** Supplier certifies that it understands the requirements set out in this Section 3 and will comply with such requirements when Processing Personal Information.

4. Information Security Policy (or Policies) and Associated Procedures

4.1. **Information Security Policy (or Policies) and Procedures.** Supplier shall maintain at least one comprehensive written information security policy that applies across its entire organization and associated procedures. Supplier shall evaluate the effectiveness of its primary information security policy and associated procedures at least annually and promptly adjust and/or update such policy and procedures as reasonably necessary to address the findings of any such evaluation.

4.2. **Incident Response Plan.** Supplier shall maintain a written incident response plan that sets out response procedures Supplier will follow in the event of a Security Incident. Supplier shall evaluate and test its incident response plan no less than once per year and shall promptly adjust and/or update its incident response plan as necessary to address the findings and any data security-related risks identified by any such evaluation.

4.3. **Business Continuity/Disaster Recovery Plan.** Supplier shall maintain a written business continuity and disaster recovery plan covering any systems or networks that Process Personal Information.

5. Security Measures

5.1. Reasonable and Appropriate Security Measures. Supplier agrees to maintain reasonable and appropriate administrative, physical, organizational, and technical safeguards designed to maintain the confidentiality, availability, and integrity of Personal Information.

5.2. Access Controls

5.2.1. Least Privilege. Supplier agrees to limit access to Personal Information to only its employees and Subcontractors who require such access for Supplier to provide the Products or Services under the Contract Agreement(s) or to comply with applicable law.

5.2.2. Administrative Accounts. Supplier shall provide administrative rights only to its employees who require such elevated access to perform their assigned duties.

5.2.3. Access Termination. Supplier shall terminate each of its employee's or Subcontractor's access to Personal Information within twenty-four (24) hours (or by no later than the next business day) of such employee's termination of employment or the termination of Subcontractor's contract with Supplier or within twenty-four (24) hours of such employee or Subcontractor's change in job duties such that the employee or Subcontractor no longer needs such access for Supplier to provide the Products or Services.

5.2.4. Password Requirements. Supplier shall ensure that any systems or devices used to Process Personal Information can be accessed only by employees or Subcontractors using passwords that meet applicable Industry Standards with respect to uniqueness, complexity, and expiration.

5.2.5. Access Logging. Supplier shall log access to any of its servers or systems that Process Personal Information. Supplier shall retain such logs for at least 180 days and shall adhere to a procedure for reviewing access logs on a regular basis.

5.3. Firewalls. Supplier shall maintain firewalls that meet all applicable Industry Standards on any of its systems or networks that Process Personal Information.

5.4. Malware.

5.4.1. Anti-Virus Solution(s). Supplier shall maintain and frequently update at least one anti-virus software program which meets applicable Industry Standards on all of its computers, workstations, mobile devices and servers that Process Personal Information. Supplier shall promptly apply all updates made available by the provider of its anti-virus software program.

5.5. Encryption

5.5.1. Encryption in Transit. Supplier will use TLS 1.2 or above to encrypt Personal Information transmitted outside of Supplier's network.

5.5.2. Encryption at Rest. Supplier will use AES 256 or above to encrypt Personal Information Processed on its network.

5.6. Intrusion Detection. Supplier shall maintain at least one intrusion detection solution on all of its networks used to Process Personal Information. Supplier's intrusion detection solution(s) shall meet applicable Industry Standards and enable Supplier to identify suspicious network traffic.

5.7. Data Loss Prevention. Supplier shall maintain at least one data loss prevention solution on all of its networks used to Process Personal Information. Supplier's data loss prevention solution shall meet applicable Industry Standards and enable Supplier to identify and block suspicious network traffic.

5.8. Physical Security. Supplier shall maintain physical security measures that comply with applicable Industry Standards at any facility at which Supplier Processes Personal Information. Supplier agrees that such physical security measures will include, but are not limited to, reasonable measures to restrict and monitor access to such facilities and those areas within those facilities where Personal Information is Processed.

5.9. Vulnerability Assessments. Supplier shall retain an independent third party to conduct quarterly vulnerability assessments of any systems or networks that Process Personal Information. Supplier shall promptly remediate any critical or high-risk vulnerabilities identified in connection with any such vulnerability assessment. If Supplier cannot remediate a critical vulnerability within three (3) calendar days, Supplier shall notify Leidos of the vulnerability. Supplier shall remediate all other identified vulnerabilities in accordance with its information security policy (or policies) and associated procedures.

5.10. Penetration Testing. Supplier will retain an independent third party to perform penetration tests at least once annually. Supplier shall promptly remediate any critical or high-risk vulnerabilities identified through such penetration tests. If Supplier cannot remediate a critical vulnerability within three (3) calendar days, Supplier shall notify Leidos of the vulnerability. Supplier shall remediate all other identified vulnerabilities in accordance with its information security policy.

6. Security Incidents

6.1. Investigation. Upon discovering a Security Incident, Supplier shall immediately investigate the cause and extent of the Security Incident. Supplier shall preserve a record of its investigation and maintain any evidence it discovers in the course of its investigation.

6.2. **Notice to Leidos.** Supplier shall notify Leidos in writing within forty-eight (48) hours of discovering a Security Incident that could affect Personal Information. Supplier will provide such notice via email to Supplier's point of contact at Leidos and copy to SupplierIncident@leidos.com. Such notice will, at a minimum, (1) describe the Security Incident and its effect on Leidos, (2) identify any Personal Information potentially compromised or impacted by the Security Incident, and (3) describe Supplier's efforts to investigate and mitigate the Security Incident. Supplier agrees to update this notice during the course of Supplier's investigation until such investigation and Supplier's mitigation activities have concluded. Further, at Leidos' request, Supplier agrees to share a final summary of the findings of such investigation with Leidos and to provide Leidos with any information Leidos requires for Leidos to independently assess the impact of the Security Incident and, when legally required or appropriate in Leidos' discretion, notify affected individuals and government regulators.

6.3. **Notice to Affected Individuals.** Supplier will notify Leidos at least five (5) business days in advance of making any public statements about or notifying any individuals impacted by a Security Incident involving Personal Information. If Supplier makes any public statements about a Security Incident or provides notice to affected individuals or government regulators, Supplier will not mention Leidos without obtaining Leidos' prior written consent.

6.4. **Mitigation.** Supplier shall take all necessary steps, at Supplier's expense, to prevent any further unauthorized access to, or use or disclosure of, Personal Information potentially impacted by a Security Incident.

7. Return or Deletion of Personal Information

7.1. **Return or Deletion.** Supplier shall, at Leidos' request and discretion, either return or securely destroy the Personal Information, at no additional cost to Leidos and within ten (10) days of receiving such a request. Supplier shall dispose of Personal Information in a manner that renders Personal Information unreadable, indecipherable, and unusable and complies with all applicable Data Protection Laws and Industry Standards. Upon securely destroying Personal Information, Supplier shall promptly provide Leidos with written certification of such disposal.

7.2. **Retention of Backup Tapes.** If Personal Information is maintained on backup tapes and the destruction of Personal Information maintained on such backup tapes would require commercially unreasonable time and expense, Supplier may retain Personal Information on such backup tapes until the backup tapes are destroyed in accordance with Supplier's reasonable and appropriate record retention policies. If Supplier maintains Personal Information on backup tapes pursuant to this provision, Supplier may not further Process Personal Information for any purpose other than to destroy such Personal Information, unless otherwise requested by Leidos or as expressly required by applicable law.

7.3. **Retention for Compliance with Applicable Laws.** Notwithstanding any other provision in this section, Supplier may retain Personal Information where necessary to comply with applicable laws. Supplier may not Process any Personal Information retained to comply with applicable laws for any purpose other than meeting its obligations under such applicable laws. Once Supplier is no longer required by applicable laws to retain Personal

Information, Supplier shall promptly and securely destroy such Personal Information as required by this DPE.

8. Data Subject Rights

8.1. Notice of Data Subject Rights Requests. If Supplier receives a Data Subject Rights Request from an individual identified by Personal Information Processed by Supplier and/or one or more of its Subcontractors, Supplier shall notify Leidos in writing within forty-eight (48) hours of receiving such request.

8.2. Responding to a Data Subject Rights Request. If Leidos receives a Data Subject Rights Request from an individual whose Personal Information is Processed by Supplier and/or one or more of its Subcontractors, Supplier shall provide reasonable assistance to Leidos in responding to such Data Subject Rights Request, including notifying any Subcontractors that Process Personal Information of the Data Subject Rights Request, at no additional cost to Leidos. If Leidos does not have access to the Personal Information that is the subject of the Data Subject Rights Request, Supplier shall respond to the individual on behalf of and at Leidos' direction. Supplier's response to the individual shall comply with any requirements under applicable Data Protection Law(s).

8.3. Notice to Subcontractors. If Supplier receives a Data Subject Rights Request, Supplier agrees to direct any Subcontractors who Process or have access to Personal Information to process the Data Subject Rights Request to the extent required by applicable Data Protection Law(s).

9. Responsibility for Employees

9.1. Employee Data Processing Obligations. Prior to providing an employee of Supplier with access to Personal Information or otherwise disclosing Personal Information to one or more of its employees, Supplier must advise (whether via training or otherwise) such employee(s) of Supplier's obligations under this DPE. Supplier shall also require its employees who Process Personal Information to comply with obligations materially similar to Supplier's obligations under this DPE.

9.2. Employee Privacy and Security Training. Prior to being provided with access to Personal Information, Supplier shall ensure that its employees with access to Personal Information have completed privacy and cybersecurity training which meets the requirements of applicable Data Protection Laws and at a minimum meets applicable Industry Standards. Such training shall include, for example, information about how to identify phishing attacks. Supplier shall ensure its employees receive such training on an annual basis thereafter.

9.3. Employee Oversight. Supplier shall implement and maintain policies and procedures that set out reasonable and appropriate disciplinary measures for employees who fail to comply with their obligations with respect to the Processing of Personal Information.

9.4. Personnel Security Checks. Supplier shall implement appropriate measures to verify the reliability of any employee with access to Personal Information, including conducting background investigations, consistent with applicable law, prior to providing any such employee with access to Personal Information.

10. Subcontractors

10.1. Due Diligence. To ensure that its Subcontractors are capable of complying with all applicable Data Protection Laws as well as the contractual obligations referenced in Section 10.2 below, Supplier shall carry out reasonable due diligence on any Subcontractor which will have access to Personal Information, before such access is granted.

10.2. Agreements with Subcontractors. Prior to providing a Subcontractor with access to Personal Information or disclosing Personal Information to a Subcontractor, Supplier will execute a written agreement with the Subcontractor which "flows down" obligations and responsibilities materially similar to those imposed on the Supplier under this DPE.

10.3. Adding New Subcontractors. Supplier may not disclose Personal Information to a new Subcontractor or provide a new Subcontractor with access to Personal Information unless Supplier provides Leidos with at least thirty (30) days advance written notice of its intent to add a new Subcontractor, either through updates to a mailing list to which Leidos can subscribe or by direct notice to Supplier's point of contact at Leidos, and unless Leidos does not object to the use of the new Subcontractor within such thirty (30) day period. Such notice shall identify the new Subcontractor and provide sufficient details of the Processing activities engaged in by the Subcontractor, so that Leidos can evaluate the Subcontractor's use of the Personal Information.

10.4. Objections to New Subcontractors. If Leidos objects to a new Subcontractor, Supplier shall enter into good faith discussions with Leidos to agree upon an alternative method of providing the Products or Services as set forth in the Contract Agreement(s) without using the new Subcontractor. If at the end of such good faith discussions, the Parties are unable to agree on an alternative method of providing the Products or Services, the Parties may each terminate the Contract Agreement(s) without penalty.

10.5. Responsibility for Subcontractor. Supplier shall remain fully liable to Leidos for all of the acts and omissions of its Subcontractors with respect to any Processing of Personal Information.

11. Due Diligence and Audits

11.1. Privacy and Data Security Questionnaire(s).

11.1.1. Frequency and Accuracy of Supplier Responses. From time to time, Supplier may be asked to respond to Leidos' written questions relating to Supplier's privacy and data security-related policies and practices. Unless otherwise provided in the Contract Agreement, Leidos may also request that Supplier respond to a formal privacy and data security questionnaire no more frequently than once per year. Supplier represents and warrants that its responses to any such questions will be true and accurate and that it will notify Leidos if there are any material changes to its prior responses.

11.2. **Certifications and Reports.** Upon Leidos' written request, and as applicable, Supplier shall provide Leidos with a copy of its most recent SOC 2 Type 2 report, ISO/IEC 27001 certification, and any other reports demonstrating compliance with Industry Standards.

11.3. **Paper Audit.** Upon Leidos' request, Supplier will make available to Leidos, or a third-party auditor as directed by Leidos, reasonable documentation demonstrating Supplier's compliance with its obligations under this DPE. Any third-party auditor designated by Leidos shall not be a competitor of Supplier.

11.4. **Facility Audit.** If Leidos is unable to determine whether Supplier is compliant with its obligations under this DPE following an audit pursuant to Section 11.3or if Leidos determines that an audit under Section 11.3will not provide Leidos with the information it needs to determine Supplier's compliance with this DPE, Leidos may initiate an audit of Supplier's facilities that Process Personal Information. Leidos shall provide Supplier with at least thirty (30) days prior notice of any facility audit. Supplier shall provide Leidos or Leidos' third-party auditor with sufficient access to Supplier's facilities and systems to permit Leidos to determine whether Supplier has complied with its obligations under this DPE.

11.5. **Government Audit**. Supplier shall provide Leidos with such information and assistance as Leidos reasonably requires to respond to a request for information or order from a government regulator or data protection authority, at no additional cost to Leidos.

11.6. **Audit Assistance.** If Leidos exercises its audit rights under Sections 11.4 or 11.5, Supplier will provide reasonable assistance, at no additional cost to Leidos, including providing appropriate management and other personnel to engage with Leidos, respond to questions, and supervise any audit, if needed.

11.7. **Audit Timing.** If Leidos exercises an audit right under Section 11.4 (Facility Audit), such audit will be conducted at a mutually agreed-upon time.

11.8. **Remediation.** If Leidos identifies any unauthorized use of Personal Information or Supplier notifies Leidos of any unauthorized use of Personal Information, Leidos may, upon providing written notice to Supplier, take reasonable and appropriate steps to stop and remediate such unauthorized use of Personal Information.

12. Survival. The terms of this DPE shall survive the termination of the Contract Agreement and shall remain in effect for so long as Supplier or its Subcontractors Process Personal Information for any purpose.

13. Indemnity. Supplier agrees to indemnify, defend, and hold harmless Leidos, its affiliates, and their respective officers, directors, employees, agents, successors, and assigns (collectively "Leidos Indemnitees") from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs (including attorneys' fees), and expenses (including the cost of enforcing any indemnification right) arising out of or resulting from: (1) any Security Incident involving Personal Information; (2) Supplier's failure to comply with its obligations in this DPE, any Business Associate Agreement or Data Transfer Addendum between the Parties; (3) Supplier's failure to comply with any applicable Data Protection Law; (4) Supplier's Processing of aggregate information created using any Personal Information, or (5) Supplier's gross negligence or willful misconduct relating to the Processing of Personal Information.

14. **Limitation of Liability.** Supplier agrees that its obligation to indemnify Leidos per this DPE shall not be subject to any limitation of liability in the Contract Agreement.

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