EXHIBIT 1: DATA PROTECTION AND SECURITY

ARTICLE 1. DATA PROTECTION AND PRIVACY

a. Definitions. The following definitions shall apply for purposes of this Exhibit:

- **Agreement** means the agreement, purchase order or contract that this Exhibit is attached hereto.
- **CCPA** – the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this Exhibit.
- **Data Privacy Laws** – (a) any state or international, national law or regulation protecting the privacy, confidentiality, or security of Personal Data or any specific categories of Personal Data, including any European Union (EU) or Member State laws with respect to any GDIT Personal Data in respect of which GDIT is subject to EU Data Protection Laws.
- **GDPR** – EU General Data Protection Regulation 2016/679.
- **EEA** – the European Economic Area.
- **EU Data Protection Laws** – EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
- **EU Personal Data** means Personal Data the sharing of which pursuant to this Exhibit is regulated by the GDPR.
- **Personal Data** is defined as any individually identifiable information about GDIT customers, clients, employees (including employees or customers of GDIT customers or clients) or any other individuals about whom Seller receives identifiable information from or on behalf of GDIT in connection with the provision of Services under the Agreement or this Exhibit including but not limited to PHI (as defined below) and sensitive personal information.
- **Sensitive Information** – all non-public information about an individual considered Sensitive Personal Information (SPI) (i.e., social security numbers, driver's license number, birth date, mother's maiden name, passport, personal bank information, etc.) or GDIT Sensitive Information, Confidential information, Deliverables or Work Product and Personal Data.
- **Confidential Information** – all non-public information about a government, company or person that is restricted from disclosure by another party because of the harm it may cause to the government, company or person if it was disclosed to unauthorized recipients or became public knowledge.
- **Controller -** has the meaning given to it in the GDPR
- **Controller-to Processor Clauses -** the standard contractual clauses between controllers and processors for data transfers as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located https://assets.ctfassets.net/szx3os6exj55/3IKuHf747N0ajyuI4tjMzX/d99bfd00154f55c02f23bf4615dd5003/Data_Protection_and_Security_Schedule_1_-_Standard_Contractual_Clauses__Controller_to_Processor_.pdf
- **Processor -** has the meaning given to it in the GDPR
- **Process** or **Processing** or **Processed** is as defined in the relevant Data Privacy Laws or, where not defined, means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, encrypting, or disclosing by transmission, dissemination or otherwise making available, aligning or combining, blocking, erasing, or destroying.
- **Processor-to Processor Clauses** - the standard contractual clauses between processors and processors for data transfers as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://assets.ctfassets.net/szx3os6exj55/1Gnt4KNWMh8n1MWzxPn47m/cba47dc7c6c24cc4c3975ed87d8389b3/Data_Protection_and_Security_Schedule_1_-_Standard_Contractual_Clauses__Processor_to_Processor_.pdf
- **Protected Health Information or PHI -** as that term is defined in the HIPAA Privacy and Security Rules (45 CFR, Part 160-164) issued pursuant to the Health Insurance Portability and Accountability Act of 1996 **HIPAA**.
- **Standard Contractual Clauses -** the standard contractual clauses as officially published by the European Commission Implementing Decision 2021/914, dated 4 June 2021, as updated or replaced by the European Commission from time to time.

b. Applicability of Data Privacy Protections. In the event that Personal Data will be processed by Supplier in connection with the performance of Services under the Agreement or any SOW, then and only then shall the provisions of this Exhibit be applicable. In any such event, all Personal Data obtained from or on behalf of GDIT or in connection with the provision of Services to GDIT pursuant to this Exhibit shall be protected pursuant to this Article 1 and any other sections of this Exhibit or overarching Agreement that address personal data. Notwithstanding the foregoing, Section 1.j below shall apply only if the personal data processed pursuant to the Agreement, this Exhibit or any SOW meets the definition of PHI.

c. Compliance with Data Privacy Laws. Supplier agrees that it will process any Personal Data to which it has access in connection with its performance of the Services under any Agreement or SOW only on behalf of and for the benefit of GDIT in accordance with this Exhibit and GDIT'S prior written instructions, if any, and as otherwise required by all applicable data privacy laws including the requirements of Article 28(3) of the GDPR. Supplier agrees that it will not process any Personal Data for any other purpose absent specific written instructions from GDIT. In addition, to the extent applicable, Supplier agrees to comply with any requirements of any applicable data privacy law regarding the collection, storage, use, transfer, security, or processing of Personal Data.

d. Transfer of Personal Data outside of the EEA. To the extent that Supplier will process or access EU Personal Data that is subject to GDPR outside of the EEA, Supplier shall (i) enter into applicable arrangements to put in place adequate protection for such Personal Data to enable compliance by the GDIT and Supplier with their obligations under the GDPR and (ii) be subject to the Controller-to Processor Clauses to the extent that GDIT is a Controller of the data transfer (direct cost contracts with the government customer) or the Processor-to- Processor Clauses to the extent that GDIT is a Processor (indirect cost contracts with the government customer). The parties further agree that the Controller-to Processor Clauses or Processor-to Processor Clauses (as applicable will apply to personal data that is transferred via the Services under any SOW from the EEA and/or Switzerland to outside the EEA, United Kingdom, and Switzerland, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive). The Supplier's signature on the shall be deemed to constitute signature and acceptance of the Controller-to Processor Clauses or Processor to Processor Clauses (as applicable) incorporated herein, including their Annexes. Article 3 of this Exhibit shall apply as Annex II of such Clauses.

e. Security Incidents. Supplier will immediately, and in no event more than one (1) business day following the Incident, give written notice to GDIT of any privacy or security Incident of which it becomes aware. A privacy or security "Incident" is an unauthorized access, use, disclosure, modification, exfiltration, destruction of information or interference with access, or any other breach of privacy or security, in connection with any Confidential Data or Personal Data. Supplier will make a written report to the designated contact indicated in the Agreement as soon as possible

and in no event more than five (5) business days after Supplier learns of such Incident or any non-permitted or violating use or disclosure that contains all then known information concerning the nature and impact of the Incident, including but not limited to identifying the Confidential Data or Personal Data relating, directly or indirectly, to the Incident and all governmental and agency reporting or disclosing relating to the Incident that has occurred, is required, or is being contemplated, and Supplier's steps to mitigate the impact of the Incident. Further, Supplier shall cooperate as reasonably requested by GDIT in order to further investigate and resolve the Incident. In the event of an Incident, Supplier agrees to pay all costs and expenses associated with the Incident, including but not limited to notification costs and costs relating to credit monitoring.

Supplier agrees to secure and preserve all evidence and logs pertaining to such Incident, to take no action that would impair evidence or the tracking and tracing of the Incident, to make no public statements to the press regarding the Incident without approval from GDIT, and to inform GDIT without delay of any and all interactions with any federal, state, or local government department, agency or law enforcement in connection with such Incident. In addition, Supplier agrees to take all actions necessary to comply with applicable Data Privacy Laws, which compliance will be deemed to expand and supplement any obligation set forth in this Section 1.f.

f. Contact with Third Parties. In the event that Supplier receives a request from a third party (including an individual) to access any Confidential Data or Personal Data in Supplier's possession, Supplier will promptly forward a copy of such request to GDIT and will cooperate with GDIT in responding to any such request. Upon GDIT's request, Supplier will make Confidential Data or Personal Data in its possession available to GDIT or any third party designated in writing by GDIT and will update Confidential Data Personal Data in Supplier's possession in accordance with GDIT's written instructions. If any government or competent authority requests Supplier to disclose or allow access to GDIT Personal Data, Supplier shall immediately notify GDIT of such request and shall not disclose or allow access to such GDIT Personal Data without first giving GDIT an opportunity to consult with such government or authority to seek to prevent such disclosure or accessing. The Parties shall discuss and agree to any lawful actions or steps which may be taken to avoid or prevent such disclosure or accessing.

Supplier shall promptly notify GDIT if any complaints are received from third parties about its Processing of Personal Data, and Supplier shall not make any admissions or take any action that may be prejudicial to the defense or settlement of any such complaint. Supplier shall provide GDIT with such reasonable assistance as it may require in connection with resolving any such complaint.

g. CCPA Personal Information Processing. Supplier shall comply with all applicable requirements of the CCPA. Supplier shall not retain, use or disclose CCPA Personal Information (as defined in the CCPA) for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by the CCPA. Processing CCPA Personal Information outside the scope of the Agreement or this Exhibit will require prior written agreement between GDIT and the Supplier. The Supplier shall not disclose, release, transfer, make available or otherwise communicate any CCPA Personal Information to another business or third party without the prior written consent of GDIT. Notwithstanding the foregoing, nothing in this Exhibit or the Agreement shall restrict the Supplier's ability to disclose CCPA Personal Information to comply with applicable laws or as otherwise permitted by the CCPA. The Supplier shall promptly notify GDIT of any request received by the Supplier from a CCPA Consumer (as defined in the CCPA) in respect of the CCPA Personal Information of the CCPA Consumer and shall not respond to the CCPA Consumer except to direct such CCPA Consumer to GDIT.

h. Access to Personal Data by Suppliers. Supplier will require any Suppliers or agents to which it discloses Personal Data hereunder or under any SOW to provide reasonable assurance, evidenced by written contract (terms which meet the requirements of Article 28(3) of the GDPR shall be included where applicable), that it will comply with the same confidentiality, privacy and security obligations with respect to such Personal Data as apply to Supplier hereunder (hereinafter **"Personal Data Related Obligations"**). Supplier shall not subcontract any portion of its work without prior written consent from GDIT. In the event consent is granted, Supplier must ensure all applicable requirements are flowed down within lower tier Supplier agreements. Supplier shall ensure that any failure on the part of any Supplier or agent to comply with the Personal Data Related Obligations shall be grounds to promptly terminate such Supplier or agent. If during the term of the Agreement or any SOW GDIT determines, in its exclusive discretion, that any Supplier or agent cannot comply with the Personal Data Related Obligations, then GDIT may terminate the Agreement in whole or in part (with respect to any SOW for which such Supplier or agent is providing services).

i. HIPAA. To the extent (if any) that GDIT discloses protected health information to Supplier or Supplier accesses, maintains, uses, or discloses protected health information, Supplier agrees as follows: Supplier agrees that with respect to any PHI to which it has access in connection with the performance of Services under the Agreement or any SOW, that it will: (a) not use or further disclose PHI other than as permitted or required by this Agreement or as required by law; (b) use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement and that these safeguards will meet the requirements of the HIPAA Security Rule as of the applicable compliance date forth HIPAA Security Rule; (c) report to GDIT any use or disclosure of PHI not provided for under this Agreement of which Supplier becomes aware; (d) ensure that any agents, including a Supplier to whom Supplier provides PHI received from GDIT, or created or received by Supplier on GDIT's behalf, agree to the same restrictions and conditions that apply to Supplier with respect of such PHI; (e) make available PHI in a Designated Record Set (if any is maintained by Supplier) in accordance with 45 CFR section 164.526; (f) make available PHI for amendment and incorporate any amendments to PHI in a Designated Record Set in accordance 45 CFR section 164.526; (g) make available PHI required to provide an accounting of disclosures in accordance with 45 CFR section 164.528; and (h) make Supplier's internal practices, applicable documentation and records related to the use and disclosure of PHI Processed hereunder, available to the Secretary of Health and Human Services for the purpose of determining GDIT's compliance with the HIPAA Privacy and Security Rules.

j. Audit rights. Supplier shall make available to GDIT on request all information necessary to demonstrate compliance with this Exhibit, and shall allow for and contribute to audits, including inspections, by GDIT or an auditor mandated by GDIT in relation to the processing of the GDIT Personal Data by the Supplier or any Suppliers. Information and audit rights of the Company only arise to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of GDPR.

k. Breach of Agreement. Supplier agrees that any Processing, of Personal Data or PHI in violation of this Exhibit shall constitute a material breach of this Agreement and may cause immediate and irreparable harm to GDIT for which monetary damages may not constitute an adequate remedy. Therefore, the Parties agree that GDIT may seek specific performance and/or injunctive or other equitable relief for such violation, in addition to its remedies at law, without proof of actual damages or for the security or posting of any bond in connection with such remedy. In addition to all other legal and contractual rights, if GDIT determines that Supplier has breached this Exhibit, GDIT may terminate the Agreement, in whole or in part with respect to any affected SOW, effective immediately upon notice of termination (or such other time as stated in such notice).

l. Compliance with Laws. Supplier agrees and warrants that Supplier's performance of all Services under the Agreement or this Exhibit shall comply with all applicable laws, orders, rules, regulations, ordinances, directives, permits, and licenses that govern or apply to the Services including without limitation NDAA Section 889 as well as all Child Labor and Combating Trafficking in Persons regulations (collectively "Applicable Laws"). Supplier shall procure all licenses/permits, pay all fees, and other required charges and shall comply with all Applicable Laws of any local, state, and/or federal governmental authority. Supplier shall immediately report to GDIT and provide any information concerning any violation of Applicable Laws pertaining to the performance of this Exhibit and shall provide GDIT any information and/or certifications requested by GDIT

related to its compliance with Applicable Laws. Supplier agrees that in connection with all services performed under the Agreement or this Exhibit it shall not make or promise to make any improper payments, or provide or offer to provide anything of value, directly or indirectly, to government officials or other parties in violation of the Foreign Corrupt Practices Act or other applicable anti-bribery laws. Upon GDIT's request, Supplier shall provide GDIT with signed written representations and warranties regarding its compliance with Applicable Laws including, without limitation, providing any third party certifications regarding its compliance with Applicable Laws including, without limitation, any certification pursuant to the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC).

m. Export Controls.

1. Supplier shall comply with the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and the regulations issued by the Office of Foreign Assets Control, as well all other laws, regulations, and orders that control the export of commercial and dual-use items, defense articles and associated technology and technical data. Supplier shall not export, directly or indirectly, any hardware, software, technology, information, or technical data disclosed under the Agreement, this Exhibit or any associated Order to any individual or country for which the U.S. Government requires an export license or other governmental approval, without first obtaining all required export licenses and approvals.
2. Supplier acknowledges that GDIT is a U.S. Defense Contractor, and as such, is under certain mandatory security obligations with regard to access to its facilities and technology. Supplier agrees that if access to GDIT facilities or technology is necessary to the performance of the services, it will not assign any employee to perform services under this Exhibit, the Agreement or any associated Order unless such employee qualifies as a "U.S. Person," as defined under Applicable Laws (e.g. 22 CFR §120.15).
3. Supplier shall abide by all U.S. security laws and regulations and controls related to safeguarding information that is "Classified," "Secret" or "Top Secret" Supplier agrees that while working at GDIT's facilities, Supplier and its employees will comply with all applicable facility rules and procedures, including without limitation, any security requirements set forth in the Department of Defense Industrial Security Manual. Unless otherwise agreed in writing by GDIT, Supplier and its employees shall be granted access to GDIT facilities only during normally scheduled business hours. To the extent the Services required under this Exhibit, the Agreement or any associated Order result in Supplier or its employees having access to information relating to a U.S. Government classified program, or other information regulated by the National Industrial Security Program Operating Manual, Supplier shall not assign any employees to such work unless the individuals are citizens or nationals of the United States, and in the case of a classified program, unless the individuals are properly cleared to receive access to such information.
4. In the event that an exchange of technical data is required, GDIT will require the Supplier to certify that its employees are U.S. Persons (as defined under Applicable Laws). If required, the Supplier shall perform the necessary due diligence to ensure that only U.S. Persons have access to such technical data.
5. In addition to the foregoing requirements, Supplier will comply with the Immigration Reform and Control Act of 1986 and in particular, have all of its workers fill out an I-9 form, verifying their authorization to work in the United States.

ARTICLE 2. ENCRYPTION

a. Supplier shall encrypt its laptops and other portable devices and media capable of data storage and transmissions that contain Confidential Information, Deliverables or Work Product, and Personal Data (collectively, **"GDIT Sensitive Information"**), utilizing, at a minimum, industry standard 256-bit encryption techniques. GDIT Sensitive Information includes electronic information obtained from GDIT personnel and notes typed by Supplier's Personnel on a laptop during or after a conversation with GDIT personnel.

b. Where GDIT Sensitive Information is stored on non-portable devices and media capable of data storage and transmissions, Supplier shall ensure that such devices and media are protected to prevent unauthorized logical and physical access. When such data storage mediums are destroyed or repurposed, any GDIT Sensitive Information contained therein is to be deleted or destroyed to industry standards that render it unreadable.

ARTICLE 3. DATA SECURITY

a. Security of GDIT Data. Without superseding or limiting the specificity of Article 1 of this Exhibit as it relates to Personal Data, Supplier shall implement organizational, operational, and technical security measures, to protect the integrity, availability, confidentiality of its networks, applications, and all data provided by GDIT to Supplier of any type, including but not limited to GDIT Sensitive Information, Confidential Information, Personal Data, and PHI (collectively, **"GDIT Data").** In the event of any unauthorized access to or exfiltration of GDIT Data that is in the possession or control of Supplier or is accessed by or stored in Supplier's computer or information systems or networks which was not in compliance with this Exhibit, the Agreement including, without limitation, in the event of any breach of Supplier's data security measures and systems, Supplier shall promptly notify GDIT of any such unauthorized access or exfiltration and shall fully cooperate with GDIT to report, identify, and confirm the details of any such Incident including, without limitation, as may be required pursuant to Applicable Laws. In addition, Supplier shall immediately implement effective remediation measures to prevent future non-compliant access and exfiltration of any GDIT Data or, at GDIT's written request, shall return or destroy all GDIT Data.

b. Safeguards. Supplier will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to preserve the security, integrity, and confidentiality of, and to prevent intentional or unintentional non-permitted or violating use or disclosure of, and to protect against unauthorized access to or accidental or unlawful destruction, loss, or alteration of, the GDIT Data created for or received from or on behalf of GDIT in connection with the Services. Such safeguards shall meet all applicable legal standards (including any encryption requirements imposed by law) and shall meet or exceed accepted security standards in the industry (including as applicable the measures referred to in Article 32(1) of the GDPR). Supplier will document and keep these safeguards current and shall make them available to GDIT upon request and shall meet, where applicable, the requirements of Article 28(3)(h) of the GDPR. Supplier shall ensure that only such of Supplier's employees or representatives who may be required to assist it in meeting its obligations under any Agreement or SOW shall have access to the GDIT Data.

c. Access to GDIT Data by Supplier Personnel. Supplier shall ensure that only such of Supplier Personnel who may be required to assist it in meeting its obligations under this Agreement or any SOW shall have access to the GDIT Data. Supplier shall take all reasonable steps to ensure that all Supplier Personnel used to provide the Services under this Exhibit, any SOW, or the Agreement have undergone security checks and have been deemed trustworthy, experienced, and of suitable character and integrity to handle GDIT Data, especially GDIT Sensitive Information, and have undergone training in information security, privacy and data protection, and the care and handling of GDIT Sensitive Information. Supplier will advise GDIT in advance if a security check of the type required hereunder cannot be performed by Supplier because of any legal or regulatory

restraints on investigating personnel in the local venue.

d. **Return or Destruction of GDIT Data.** In the event Supplier acquires GDIT Data of any type, and notwithstanding any provisions to the contrary regarding Confidential Information, at any time and upon expiration or termination of the Agreement, howsoever caused, Supplier shall immediately cease accessing, using, and processing GDIT Data and, at GDIT's election: (i) return all GDIT Data (in electronic, paper, and any other format) to GDIT, within ten (10) business days of request, or (ii) if the GDIT Data is no longer needed, securely destroy and dispose of any copies of the GDIT Data in its possession and provide a certificate signed by an officer of Supplier attesting to such secure destruction and disposition

e. **Network Security and Compliance** The Supplier will comply with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance for safeguarding government customer data or GDIT Data (e.g., including but not limited to the Federal Information Security Management Act; E-Government Act of 2002 (Public Law 107-347); OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources; The Privacy Act of 1974, 5 USC § 552a; Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503); Health Insurance Portability and Accountability Act; The Health Information Technology for Economic and Clinical Health Act; HR 2868: The Chemical Facility Anti-Terrorism Standards Regulation; Sarbanes-Oxley Act; Customs-Trade Partnership Against Terrorism; Free and Secure Trade Program; Children's Online Privacy Protection Act; Federal Rules of Civil Procedure Chapter 5, Rules 26-37, etc.); Patient Safety and Quality Improvement Act, Patient Safety Rule); Payment Card Industry Data Security Standard; Gramm-Leach-Bliley Act; Electronic Fund Transfer Act, Regulation E; Fair and Accurate Credit Transaction Act, including Red Flags Rule; and Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records. The Supplier's devices to be connected to the GDIT network shall at all times be maintained in a current status with respect to all operating system patches, updates, service packs, and critical updates, where "current status" shall include all patches, updates, service packs, and critical updates that have been available for download for seven (7) calendar days or more the Supplier and its personnel connecting to the GDIT network must have the latest/up-to-date antivirus protection whether it comes from their own selected commercial vendor (except as noted below) or from a GDIT approved vendor. If the choice is not the GDIT approved vendor, then the Supplier's antivirus product selection must be a commercial-grade product with a current antivirus engine and real-time protection enabled that uses definitions not more than two (2) days old. Any Supplier devices that are expected to be connected to the GDIT network for a period exceeding seven (7) calendar days must install the GDIT standard; i.e., they must have and run the GDIT approved antivirus package (e.g., Symantec Antivirus software, and/or eTrust Identity and Access Management software).The Supplier and its personnel acknowledge that GDIT's computer software and information processing facilities may be vulnerable to the introduction of Malicious Software/Code, (often referred to as "Malware" or "computer contaminant"). Malware is any software or program that is designed to disrupt the normal operation of a computer by allowing an unauthorized process to occur or unauthorized access to be granted and is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware can find its way into an information system through e-mail channels, infected disks, thumb drives, fake videos, pictures, or just by clicking on a link to a Web site when connected to a network. Malware includes but is not limited to computer viruses, network worms, Trojan horses, Adware and Spyware. The Supplier and its personnel must be made aware of the dangers of unauthorized or malicious software; and managers should, where appropriate, introduce special controls to detect or prevent its introduction into GDIT's or GDIT's customer's information processing networks or systems. Precautions must be taken by Supplier to detect and prevent computer viruses on Supplier personal computers if used in support for the performance of the Agreement or any SOW. The Supplier will have antivirus software on all devices connecting to the GDIT network unless the Supplier has been given an explicit written exemption from GDIT. Failure of the Supplier's personnel who have access to GDIT's or GDIT's government customer network to comply with this network security clause are subject to temporary or permanent removal from GDIT's network. Suppliers may also be found to be in default of the Agreement and this Exhibit and shall defend, indemnify and hold GDIT and its affiliates and customers harmless from any damages, fines, fees, expenses, or costs caused by, arising from, or related to any such non-compliance.

GENERAL DYNAMICS INFORMATION TECHNOLOGY INC.	<INSERT SUPPLIER NAME>

SIGNATURE		SIGNATURE	
NAME		NAME	
TITLE / POSITION		TITLE / POSITION	
ADDRESS		ADDRESS	
DATE		DATE	