**CUSTOMER CONTRACT REQUIREMENTS**
**Proprietary**
**CUSTOMER CONTRACT Milton**

CUSTOMER CONTRACT REQUIREMENTS

The following customer contract requirements apply to this Contract to the extent indicated below. Please note, the requirements below are developed in accordance with Buyer's prime contract and are not modified by Buyer for each individual Seller or statement of work. Seller will remain at all times responsible for providing to any government agency, Buyer, or Buyer's customer, evidence of compliance with the requirements herein or that such requirements are not applicable to the extent satisfactory to the requesting party.

**1. Prime Contract Special Provisions** The following prime contract special provisions apply to this purchase order

**Milton Special Provisions** .
**FOREIGN OWNERSHIP, CONTROL, INFLUENCE, ACCESS TO TECHNOLOGY & EXPORT CONTROL**

(a) Definitions. As used in this Article-

Effectively Owned or Controlled: A foreign Government or any entity controlled by a foreign Government has the power, either directly or indirectly, whether exercised or exercisable, to control the election, appointment, or tenure of the Seller's officers or a majority of the Seller's board of directors by any means, e.g., ownership, contract, or operation of law (or equivalent power for unincorporated organizations).

Entity Controlled by a Foreign Government: Any domestic or foreign organization or corporation that is effectively owned or controlled by a foreign Government, or any individual acting on behalf of a foreign Government. It does not include an organization or corporation that is owned, but is not controlled, directly or indirectly, by a foreign Government if the ownership of that organization or corporation by that foreign Government was effective before 23 October 1992.

Foreign Firm or Institution: A firm or institution organized or existing under the laws of a country other than the United States, its territories, or possessions. The term includes, for purposes of this Contract, any agency or instrumentality of a foreign Government; and firms, institutions, or business organizations which are owned or substantially controlled by foreign Governments, firms, institutions, or individuals.

Foreign Government: The state and the Government of any country (other than the United States and its outlying areas) as well as any political subdivision, agency, or instrumentality thereof.

Know-How: All information including, but not limited to, discoveries, formulas, materials, inventions, processes, ideas, approaches, concepts, techniques, methods, software, programs, documentation, procedures, firmware, hardware, technical data, specifications, devices, apparatus, and machines.

Proscribed Information:

(1) Top Secret (TS) information:

(2) Communications Security (COMSEC) material, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys;

(3) Restricted Data as defined in the U.S. Atomic Energy Act of 1954, as amended;

(4) Special Access Program (SAP) information; or

(5) Sensitive Compartmented Information (SCI).

Technology: Discoveries, innovations, Know-How and inventions, whether patentable or not, including computer software, recognized under U.S. Law as intellectual creations to which rights of ownership accrue, including, but not limited to, patents, trade secrets, mask works, and copyrights developed under this Contract.

(b) General

The Parties agree that research findings and technology developments arising under this Contract may constitute a significant enhancement to the national defense, and to the economic vitality of the U.S. Accordingly, access to important technology developments under this Contract by Foreign Firms or Institutions must be carefully controlled. The controls contemplated in this Article are in addition to, and are not intended to change or supersede, the provisions of the International Traffic in Arms Regulation (ITAR) (22 CFR Part 121 et seq.), the Department of Commerce Export Regulation (15 CFR Part 770 et seq.

If this Contract requires access to proscribed information to perform the Contract, the Seller shall disclose any interests a foreign Government has in itself, its immediate parent, intermediate parent, and any ultimate parent corporation to the Buyer. This Contract shall not be performed by entities controlled by a foreign Government, unless the Government has waived application of 10 U.S.C. §2536(a).

(c) Disclosure of Foreign Government Control

The Seller shall disclose any interest a foreign Government has in the Seller when that interest constitutes control by a foreign Government as defined in this Article. If the Seller is a subsidiary, it shall also disclose any reportable interest a foreign Government has in any entity that owns or controls the subsidiary, including reportable interest concerning the Seller's immediate parent, intermediate parent, and the ultimate parent.

The Seller shall submit a current SF 328, Certificate Pertaining to Foreign Interests to the Buyer, prior to Contract award. The SF 328 must include the following information:

(1) Seller's point of contact for questions about disclosure (name and phone number with country/city/area codes, as applicable);

(2) Name and address of the Seller;

(3) Name and address of entity controlled by a foreign Government; and

(4) Description of interest, ownership percentage, and identification of foreign Government.

If during performance of the Contract, foreign Government ownership or control status of the Seller changes, the Seller shall submit an updated SF 328 to the Buyer, within one (1) week of the change.

(d) Restrictions on Sale or Transfer of Technology to Foreign Firms or Institutions

In order to promote the national security interests of the U.S. and to effectuate the policies that underlie the regulations cited above, the procedures stated in paragraphs (d)(2), (d)(3), and (d)(4) below shall apply to any transfer of technology. For purposes of this paragraph, a transfer includes a sale of the company, and sales or licensing of technology. Transfers do not include:

(1) Sales of products or components, or

(2) Licenses of software or documentation related to sales of products or components, or

(3) Transfer to foreign subsidiaries of the Seller member entities for purposes related to this Contract, or

(4) Transfer which provides access to technology to a foreign firm or institution which is an approved source of supply or source for the conduct of research under this Subcontract if such transfer shall be limited to that necessary to allow the firm or institution to perform its approved role under this Subcontract, or

(5) Publication or Publicity

The Seller shall provide timely notice to the Government, via the Buyer, of any proposed transfers of technology developed under this Contract to foreign firms or institutions. If the Government determines that the transfer may have adverse consequences to the national security interests of the U.S., the Seller and the Government shall jointly endeavor to find alternatives to the proposed transfer which obviate or mitigate potential adverse consequences of the transfer but which provide substantially equivalent benefits to the Seller.

In any event, the Seller shall provide written notice to the Government, via the Buyer, of any

proposed transfer to a foreign firm or institution at least sixty (60) calendar days prior to the proposed date of transfer. Such notice shall cite this Article and shall state specifically what is to be transferred and the general terms of the transfer. Within thirty (30) calendar days of receipt of the Seller's written notification, the Buyer shall advise the Seller whether it consents to the proposed transfer. No transfer shall take place until a decision is rendered.

In the event a transfer of technology to foreign firms or institutions which is NOT approved by the Government takes place, the Seller shall:

(1) Refund to the Government, via the Buyer, those funds paid under this Contract for the development of the technology; and

(2) Provide to the Government a non-exclusive, nontransferable, irrevocable, paid-up license to practice or have practiced on behalf of the U.S. the technology throughout the world for Government and any and all other purposes, particularly to effectuate the intent of this Contract.

Upon request of the Government, the Seller shall obtain and provide written confirmation of such licenses described in paragraph (d).

(e) Export Compliance

Information subject to the Arms Export Control Act, 22 U.S.C. §§ 2751, et seq., the ITAR**,** 22 C.F.R. §§ 120, et seq., and the Export Administration Act, 50 U.S.C. app. §§ 2401, et seq., requires that all unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license under Executive Order (E.O.) 12470 or the Arms Export Control Act, and that such data requires an approval, authorization, or license under E.O. 12470 or the Arms Export Control Act. The Seller shall not export, directly or indirectly, any products and/or technology, confidential information, trade secrets, or classified and unclassified technical data in violation of any U.S. export laws or regulations. All documents determined to contain export-controlled technical data shall be marked with the following notice:

WARNING - this document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., and Sec 275 1, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provision of DOD Directive 5230.25.

(f) Lower Tier Agreements

The Seller shall include this Article, suitably modified to identify all Parties, in all lower tier Agreements. This Article shall, in turn, be included in all sub-tier subcontracts or other forms of lower tier Agreements, regardless of tier.

**ENABLING PRIME AND SUPPORT CONTRACTOR RELATIONSHIPS**

*The term "support contractor" retains its original meaning. The term "contractor" shall mean "Seller".*

(a) The Government currently has, or may enter into, contracts with one or more companies, the primary purpose of which is to furnish independent and impartial advice or technical assistance directly to the Government in support of the Government's management and oversight of a program or effort. These companies (hereafter referred to as support contractors), are obligated to safeguard the sensitive and proprietary information of other contractors, subcontractors, suppliers, and vendors to which they have access. Contact Buyer for the list of support contractors.

(b) In the performance of this contract, the contractor agrees to cooperate with companies as directed by Buyer. Cooperation includes, but is not limited to, allowing the listed support contractors to attend meetings; observe technical activities; discuss with the contractor technical matters related to this program at meetings or otherwise; and access contractor integrated data environments and facilities used in the performance of the contract.

(c) The contractor must provide the support contractors access to data such as, but not limited to, design and development analyses; test data, procedures, and results; research, development, and planning data; parts, equipment, and process specifications; testing and test equipment specifications; quality control procedures; manufacturing and assembly procedures; schedule and milestone data; and other contract data. To fulfill contractual requirements to the Government, support contractors engaged in general systems engineering and integration efforts and technical support are normally authorized access to information pertaining to this contract. Exceptions, such as when the contractor seeks to restrict access to contractor trade secrets, will be handled on a case-by-case basis. If the contractor seeks to limit distribution of data to Government personnel only, the contractor must submit this request in writing to the Contracting Officer through Buyer.

(d) The contractor further agrees to include in all subcontracts, except for those to provide only commercial and/or non-developmental items, a clause requiring the subcontractor and succeeding levels of subcontractors to comply with the response and access provisions of paragraph (b) above, subject to coordination with the contractor. This clause does not relieve the contractor of the responsibility to manage the subcontracts effectively and efficiently, nor is it intended to establish privity of contract between the Government or support contractors and such subcontractors. The contractor and its subcontractors are not required to take contractual direction from support contractors.

(e) The contractor and its subcontractors are not required to take contractual direction from support contractors.

(f) Support contractors are required to protect data and software related to this contract, and are prohibited from using such data for any purpose other than performance of the support contract.

(g) Support contractors shall protect the proprietary information of disclosing contractors, subcontractors, teammates, suppliers, and vendors. Because such entities are intended to be third-party beneficiaries, all such disclosing parties agree that these terms satisfy the non-disclosure agreement requirements set forth in 10 U.S.C. §2320(f)(2)(B). Accordingly, the contractor may only enter into a separate non- disclosure, confidentiality, proprietary information, or similar agreement with a disclosing party on an exception basis, and only after notifying the Contracting Officer through the Buyer. The Government and the disclosing contractors, subcontractors, suppliers, and vendors agree to cooperate to ensure that the execution of any non-disclosure agreement does not delay or inhibit performance of this contract, and the Government shall require support contractors to do the same. Such agreements shall not otherwise restrict any rights due the Government or Buyer under this contract. Separate non-disclosure agreements may be executed only in the following exceptional circumstances:

(1) The support contractor is a direct competitor of the disclosing party in furnishing end items or services of the type developed or produced for the program or effort;

(2) The support contractor will require access to extremely sensitive business data; or

(3) Other unique business situations exist in which the disclosing party can clearly demonstrate that clause CI 209-8 does not adequately protect their competitive interests.

(h) Any proprietary information furnished to support contractors shall be:

(1) Disclosed in writing and clearly marked "proprietary" or with other words of similar meaning;

or

(2) Disclosed orally or visually for instance, during a plant tour, briefing, or demonstration) and identified as proprietary information at the time of the oral or visual disclosure by the Government or a disclosing party. The support contractors shall treat all such information as proprietary unless within ten (10) days the support contractor coordinates with Buyer or disclosing party to obtain a written version of the proprietary information and determine the extent of the proprietary claims; or

(3) Disclosed by electronic transmission (e.g., facsimile, electronic mail, etc.) in either human readable form or machine-readable form, and the contractor marks it electronically as proprietary within the electronic transmissions, such marking to be displayed in human readable form along with any display of the proprietary information; or

(4) Disclosed by delivery of an electronic storage medium or memory device, and the contractor marks the storage medium or memory device itself as containing proprietary information and electronically marks the stored information as proprietary, such marking to be displayed in human readable form along with any display of the proprietary information.

(i) The contractor agrees not to hold the support contractor liable for unauthorized disclosure of proprietary information if it can be demonstrated in written documentation or other competent evidence that the information was:

(1) Already known to the support contractor without restriction on its use or disclosure at the time of its disclosure by the disclosing party;

(2) In the public domain or becomes publicly known through no wrongful act of the support contractor;

(3) Proprietary information disclosed by the support contractor with the contractor's prior written permission;

(4) Independently developed by the support contractor, subsequent to its receipt, without the use of any proprietary information;

(5) Disclosed to the support contractor by a third party who was legally entitled to disclose the same and who did not acquire the proprietary information from the disclosing party;

(6) Specifically provided in writing by the U.S. Government to the support contractor with an unlimited rights license; or

(7) Disclosed by the support contractor as required by law, regulatory or legislative authority, including subpoenas, criminal or civil investigative demands, or similar processes, provided the support contractor provides the disclosing party that originated the proprietary information with prompt written notice so that the disclosing party may seek a protective order or other appropriate remedy, and provided that, in the absence of a timely protective order, the support contractor furnishes only that minimum portion of the proprietary information that is legally required.

(j) Any notice to the support contractor(s) required or contemplated under the provisions of this article shall be in writing and shall be deemed to have been given on:

(1) The date received if delivered personally or by overnight courier;

(2) The third day after being deposited in the U.S. mail, postage prepaid; or

(3) The date sent if sent by facsimile transmission or e-mail with a digital copy.

(k) Buyer and contractor agree to cooperate in resolving any unauthorized disclosure or misuse of proprietary information by a support contractor. This shall not be construed as requiring the contractor to conduct an inquiry into an unauthorized disclosure or misuse, or as authorizing the allocation of costs for such an inquiry directly to this contract. Any costs incurred by the contractor in said fact-finding efforts may be allowable and allocable upon determination of Buyer after adjudicating the circumstances related to any unauthorized disclosures or misuse.

**SUPPLY CHAIN RISK MANAGEMENT**

*The term "Performer" shall mean "Buyer."*

*The requirements of this article do not apply to Commercial Services and Commercial Off-the- Shelf (COTS) items, that are not on the Performer's government-approved Critical Component List.*

(a) Definitions. As used in this article-

*Covered System* means all DoD critical information systems and weapons systems, which includes major systems as defined by 10 U.S.C. 3041; national security systems as defined by 44 U.S.C. 3542; and all DoD information systems, categorized as Mission Assurance Category (MAC) I, and select DoD information systems categorized as MAC II, in accordance with DoDI.

*Criticality Analysis and Assessment (CAA)* means an end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. CAA includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. The criticality assessment determines the potential harm; i.e., mission loss or degradation, caused by the probable loss, damage, or compromise of a product, material (hardware, software or firmware components) or service.

*Critical Component* means hardware, software, and firmware, whether custom, commercial, or otherwise developed, which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

*Critical Program Information (CPI)* means a U.S. information capability element that contributes to the warfighters' unique technical advantage when employed in its operational environment, which if compromised, undermines U.S. military or intelligence community capabilities, by degradation in mission effectiveness; shortens the expected effective life of the system; reduces technological advantage; significantly alters program direction; or enables an adversary to defeat, counter, copy, or reverse engineer the technology or capability. U.S. information capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

*Due Diligence* means reasonable steps taken to gather publicly or commercially available information about a prospective supplier and comprehensively evaluate said supplier within the twelve risk areas described in the DoD Supply Chain Risk Management Taxonomy- Version 1.0, dated 28 November 2022.

*Enterprise Products List (EPL)* means the single source at the GOVERNMENT for approved information technology (IT) Products.

*Information and Communications Technology (ICT)* means the IT integration of telecommunications and computers, software, or firmware that enable users to access, store, transmit, and process information.

*Original Component Manufacturer (OCM)* means an organization that designs and/or engineers an item and is entitled to any intellectual property rights to that item, or for the purposes of this article, an OCM authorized reseller or distributor.

*Original Equipment Manufacturer (OEM)* means a company that manufactures products that it has designed from purchased components and sells those products under the company's brand name, or for the purposes of this article, an OEM authorized reseller or distributor.

*Program Protection Plan (PPP)* means a risk-based, comprehensive, living plan to guide efforts for managing the risks to CPI and mission-critical functions, components and technologies associated with a research, development, and acquisition program. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI protection activities.

*Software Bill of Materials (SBOM)* means a formal record containing the products used to assemble the software capability to include open source and commercial software components. The minimum elements for an SBOM are identified in Executive Order 14028, Improving the Nation 's Cybersecurity, 12 July 2021.

*Supply Chain Risk* is any risk that has the potential to-

(1) Jeopardize the integrity of products, services, people, and technologies;

(2) Compromise intellectual property;

(3) Disrupt the flow of product, material, information, and finances needed for continued SCRM process; or

(4) Drive material cost increases to the program.

Risk categories include-

(1) Compliance;

(2) Environmental;

(3) Infrastructure;

(4) Economics;

(5) Financial;

(6) Foreign Ownership Control or Influence (FOCI);

(7) Foreign Dependence;

(8) Human Capital;

(9) Manufacturing & Supply;

(10) Transportation & Distribution;

(11) Political & Regulatory;

(12) Product Quality & Design; and

(13) Technology & Cybersecurity.

*Supply Chain Risk Assessment (SCRA)* means the collective results of the criticality analysis and assessment, supply chain threat analysis, supply chain vulnerability assessment, and culmination of the supply chain risk mitigation strategies applicable to the covered system.

*Supply Chain Risk Management (SCRM)* means a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats to covered acquisitions, CCs or systems throughout a program's or agreement's supply chain, and developing mitigation strategies to combat or address those threats whether presented by the supplier, the supplied product and its subcomponents, or any other place within the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

*Supply Chain Risk Management System (SCRMS)* means a corporate set of tools, processes, policies, practices, procedures, programs and IT infrastructure integrated together to prevent the purchase of any item, or use of any service provider within its supply chain, that poses a potential product availability or integrity risk, including those with national security consequence, and provides for conformance with the requirements specified in paragraph (b) below.

*Supply Chain Threat Assessment* is the government's evaluation and characterization of threats to the availability, integrity, trustworthiness, and authenticity of the acquisition item.

*Technology Readiness Level (TRL)* is a method for estimating the maturity of technologies during the acquisition phase of a program. TRLs enable consistent and uniform discussions of technical maturity across different types of technology.

*Vulnerability* means an attribute or characteristic that may be inherent or introduced into a system's components (i.e., system, component, hardware, software, firmware), or service's design, implementation, or operation and management that could be exploited by an adversary at any stage of the acquisition lifecycle.

*Vulnerability Assessment* is the government process of formally and systematically evaluating and documenting information on vulnerabilities of a critical component applicable to the acquisition item throughout the item's lifecycle, from design to disposal.

*Original Equipment Manufacturer (OEM)* means a company that manufactures products that it

has designed from purchased components and sells those products under the company's brand name, or for the purposes of this article, an OEM authorized reseller or distributor.

*Program Protection Plan (PPP)* means a risk-based, comprehensive, living plan to guide efforts for managing the risks to CPI and mission-critical functions, components and technologies associated with a research, development, and acquisition program. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI protection activities.

*Software Bill of Materials (SBOM)* means a formal record containing the products used to assemble the software capability to include open source and commercial software components. The minimum elements for an SBOM are identified in Executive Order 14028, Improving the Nation 's Cybersecurity, 12 July 2021.

*Supply Chain Risk* is any risk that has the potential to-

(1) Jeopardize the integrity of products, services, people, and technologies;

(2) Compromise intellectual property;

(3) Disrupt the flow of product, material, information, and finances needed for continued SCRM process; or

(4) Drive material cost increases to the program.

Risk categories include-

(1) Compliance;

(2) Environmental;

(3) Infrastructure;

(4) Economics;

(5) Financial;

(6) Foreign Ownership Control or Influence (FOCI);

(7) Foreign Dependence;

(8) Human Capital;

(9) Manufacturing & Supply;

(10) Transportation & Distribution;

(11) Political & Regulatory;

(12) Product Quality & Design; and

(13) Technology & Cybersecurity.

*Supply Chain Risk Assessment (SCRA)* means the collective results of the criticality analysis and assessment, supply chain threat analysis, supply chain vulnerability assessment, and culmination of the supply chain risk mitigation strategies applicable to the covered system.

*Supply Chain Risk Management (SCRM)* means a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats to covered acquisitions, CCs or systems throughout a program's or agreement's supply chain, and developing mitigation strategies to combat or address those threats whether presented by the supplier, the supplied product and its subcomponents, or any other place within the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

*Supply Chain Risk Management System (SCRMS)* means a corporate set of tools, processes, policies, practices, procedures, programs and IT infrastructure integrated together to prevent the purchase of any item, or use of any service provider within its supply chain, that poses a potential product availability or integrity risk, including those with national security consequence, and provides for conformance with the requirements specified in paragraph (b) below.

*Supply Chain Threat Assessment* is the government's evaluation and characterization of threats to the availability, integrity, trustworthiness, and authenticity of the acquisition item.

*Technology Readiness Level (TRL)* is a method for estimating the maturity of technologies during the acquisition phase of a program. TRLs enable consistent and uniform discussions of technical maturity across different types of technology.

*Vulnerability* means an attribute or characteristic that may be inherent or introduced into a system's components (i.e., system, component, hardware, software, firmware), or service's design, implementation, or operation and management that could be exploited by an adversary at any stage of the acquisition lifecycle.

*Vulnerability Assessment* is the government process of formally and systematically evaluating and documenting information on vulnerabilities of a critical component applicable to the acquisition item throughout the item's lifecycle, from design to disposal.

(b) Compliance Requirements.

(1) The Performer shall procure, to the maximum extent practicable, products, systems and critical components of those systems, which are OEM/OCM and competitively sourced. Procurement of products, systems and critical components must be compliant with the Buy American Act and Government Information Technology (IT) procurement policies.

(2) The Government may waive or tailor SCRM requirements for Advanced Research and Development projects involving experimental or demonstration projects that meet any of the following-

(i) Projects/systems in Technology Readiness Level 1-3 with limited domestic-only supply chain exposure or without utilization of Government networks or supply chain exposure.

(ii) Projects/systems that will have no physical or virtual connection with operational mission systems.

(iii) Projects/systems without identified Critical Components or Information and Communications Technology (ICT).

(c) Supply Chain Risk Management Plan.

(1) The Performer shall submit a comprehensive Supply Chain Risk Management Plan to the AOR and Agreements Officer in accordance with the TDD guidance.

(2) Contents of the plan shall include at a minimum-

(i) A complete Supply Chain List (SCL) of ICT components and of subcontractors, hardware and software component suppliers, and vendors (including delivery, packaging, and warehousing vendors) used for the performance of the agreement. The SCL shall be updated and accessible to the Government. This list shall be maintained as current throughout the acquisition lifecycle.

(ii) Performer's confirmation of compliance with the Government's policy requirements for purchases, components, CPI, ICT, materials, instruments, hardware, software or firmware regarding-

(A) OEM/OCMs;

(B) US-made, US-only Suppliers/Vendors;

(C) Trade Agreement Act (TAA) compliance for parent level IT, (e.g., Router, Switch, Server, Desktop);

(Note: Component level IT does not require TAA compliance (e.g., Motherboards, RAM, internal hard drives, video card); and

(D) Competitively-awarded suppliers.

(iii) All information available (e.g., Supplier Name, Address, Mission Assurance (MA) Points-of-Contact (POCs), Program and Agreements POCs, Contact Information, CAGE Code, Website Address, etc.) on suppliers the Performer has already purchased from and/or used under this agreement, together with rationale for purchasing from sources, that are-

(A) Non-OEM/OCM;

(B) Foreign-owned, operated, and/or controlled;

(C) Unknown, or first-time use; and/or

(D) Sole source.

(iv) A complete description of its Supply Chain Risk Management System (SCRMS) as defined herein.

(v) A description of the Performer's purchasing process or system, including security and vetting controls used in the selection and award of subcontractors, vendors and suppliers to comply with paragraphs (c)(2)(ii) - (iv).

(vi) The status of purchasing system review conducted by the Defense Agreement Management Agency (DCMA) or other Government agency, to include Government POCs, dates of assessments and any outstanding corrective actions.

(vii) Subcontractor purchasing systems shall be compliant with the Performer's SCRM.

(d) SCRMS Requirements.

(1) The Performer shall establish and maintain an acceptable SCRMS. Failure to maintain an acceptable SCRMS, as defined in this article, may result in: disapproval of the Performer's purchasing system; Agreements Officer determination of Non-Responsibility; negative past performance assessment; and/or termination of this agreement.

(2) The Performer's SCRMS shall comply with the following-

(i) The Performer shall have adequate systems in place to contribute to supply chain threat assessments to support its SCRMS in documenting, assessing, and dispositioning vulnerabilities in its supply chain, and that enable data exchange with the private and public sector. Performers will share data collected with Program Managers in accordance with section 2(ii), including the Government-Industry Data Exchange Program (GIDEP).

(ii) The Performer shall provide input to the Government SCRA and component assessments-Criticality Analysis, Supply Chain Threat Assessment, and Vulnerability Assessment-including due diligence research performed in selecting a supplier. Performer shall propose risk mitigation strategies for Government consideration.

(iii) The Performer shall provide a description of its Supply Chain Risk, defined in section (a), of process or system, addressing how risks are identified and mitigated to the supply chain relative to products, systems and/or critical components of those systems, or otherwise, to service providers to all levels in the supply chain of the agreement.

(iv) The Performer shall receive and ship all equipment, software and hardware assets for final delivery using DoD approved carriers in accordance with the Defense Transportation Regulation (DTR).

(v) The Performer shall track property from date of procurement or date of Government Furnished Equipment (GFE) transfer to disposal (if applicable) and shall make available, at the Government's request, an audit trail of such purchases and transfers. The Performer shall obtain and track Destruction Certificates for serial numbered items when permanently removed from service.

(vi) The Performer shall provide notification to the AOR and the Agreements Officer, within 72 hours, if any items are already purchased, and reflected in the Performer's Supply Chain List (SCL) that are: not OEM/OCM; not US-made; not known suppliers (Government SCRA is nonexistent or older than 2 years), or sole source suppliers, including full information available to the Performer (Supplier Name, Address, POCs, Contact Info, CAGE Code, Website Address, etc.) regarding the items purchased and their source.

(vii) The Performer shall notify the AOR and the Agreements Officer within 72 hours of the Performer's knowledge of any changes to the Performer's supply chain, or to information on the SCL that was initially provided to the government and reflected in its Supply Chain Surveillance Plan (SCSP), under this agreement.

(viii) The Performer shall notify the AOR and the Government Agreements Officer within 72 hours, when discovering a supply chain compromise or anomaly, whether verified or suspected, and anomalies associated with NIST SP 800-53 compliance. The Performer shall conduct a comprehensive investigation of the compromise and keep the AOR informed throughout the process.

(ix)The Performer shall select all parts, materials and process for use in Space Systems

(qualification, proto-qualification and/or acceptance tested) to meet the program's Statement of Work.

(x) The Performer shall develop and deliver its "Software Bill of Materials" or "SBOM." The SBOM will be used to perform vulnerability or license analysis, both of which can be used to evaluate risk in the developed software capability. The SBOM shall be delivered in one of the data formats conformant to Software Package Data eXchange (SPDX), CycloneDX, Software Identification (SWID) tags (ISO 19770-2) is acceptable.

(xi) The Performer shall identify CPI and document CPI measures in support of the PPP to address supply chain risks.

(e) Subcontracts. The Performer shall insert the substance of this article, including this paragraph (e), into all agreements/subcontracts except for Commercial Services and Commercial Off-the-Shelf (COTS) items, that are not on the Performer's government approved Critical Component List.

(f) Government sources. The Performer and its subcontracts are required to comply with the requirements of this article, as applicable, even when: purchasing item(s) from the Federal Supply Schedule; purchasing electronic parts from suppliers accredited by the Defense Microelectronics Activity; or requisitioning electronic parts from Government inventory/stock under the authority of FAR Clause 52.251-1, Government Supply Sources.

(g) Reporting Requirements. The reporting requirements of this article shall be effective at the point in time when the Performer has identified Critical Components on its Critical Component List through the end of agreement performance.

(h) Exceptions. The requirements of this article do not apply to Commercial Services and Commercial Off-the- Shelf (COTS) items, that are not on the Performer's government-approved Critical Component List.