AFLCMC Armament Directorate Rapid Response (ADRR) Commercial Solutions Opening (CSO) for Innovative Execution

The Air Force Life Cycle Management Center (AFLCMC) Armament Directorate at Eglin AFB, FL will utilize this CSO for specific future requirements. All specific requirements and submissions will be posted as Spirals with specific calls to action. This CSO may lead to FAR Part 12 or Other Transactions. This posting of the CSO does not commit the Government to contract for any supply or service whatsoever. Further, the Government is not seeking proposals at this time and will not accept unsolicited proposals. No funding is currently available for the CSO.

Table of Contents

SECTION I: INTRODUCTION, BACKGROUND, & SCOPE.....2

SECTION II: GUIDELINES FOR SOLUTION BRIEFS 8

SECTION III: SUBMISSION INFORMATION 10

SECTION IV: EVALUATION CRITERIA 11

SECTION V: ARTICLES.....11

SECTION VI: ATTACHMENTS 50

SECTION VII: CSO CONTACT INFORMATION 50

SECTION I: INTRODUCTION, BACKGROUND, & SCOPE

A. Background

The AFLCMC Armament Directorate Rapid Response (ADRR) Commercial Solutions Opening (CSO) is an umbrella CSO solicitation that contains the basic information but does not request solution briefs with its initial issuance. This is a competitive solicitation posted on this Government Point of Entry (GPE) www.sam.gov and/or Eglin CSO (https://eglincsoportal.us) through **04 June 2027**. The CSO authority is 10 U.S.C. 3458, implemented by DFARS Subpart 212.70, for the acquisition of innovative commercial products or commercial services.

Per 10 U.S.C. 3458, innovative products/services competitively selected by peer review of proposals resulting from a general solicitation (e.g., this ADRR CSO) are considered commercial notwithstanding the definition under FAR Subpart 2.101. The use of a CSO is permanently authorized by section 803 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 (Pub. L. 117-81) codified at 10 U.S.C. 3458.

The Armament Directorate (AFLCMC/EB) at Eglin AFB, FL is seeking to apply unique solutions and innovative ideas to:

- Rapidly develop technologies of novel weapons capabilities; and characterize new technologies and system concepts that provide evolutionary, revolutionary, and disruptive capabilities for the United States Air Force through weapons systems requirements development, studies, and demonstrations.

The overall objective is to exploit commercial items and services, or minimally modified commercial items and services, to provide rapid response to shifting requirements in all areas and lifecycle phases of weapons execution. These include weapons concepts, hardware prototypes, concept development, concept demonstrations, and weapons system procurement, production, fielding, operations, and sustainment. Potential customers include AFLCMC/EB divisions, SOCOM Det-1, Air Force Research Lab (AFRL), and the Air Force Nuclear Warfare Center (AFNWC), as well as 96th Test Wing units.

B. Objectives:

- Deliver innovative capabilities to the warfighter with increased speed and agility
- Incorporate digital acquisition and sustainment practices to include digital engineering (DE), agile processes, open system architecture (OSA), and Weapons Open System Architecture (WOSA)

C. Definitions:

Agile Processes – Project management processes, mainly used for software development, where demands and solutions evolve through the collaborative effort of self-organizing and cross-functional teams and their customers.

Agile Software – Software development methodologies centered around the idea of iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams and their customers.

Agreement – The body of the agreement and any attachments, which are expressly incorporated in and made a part of the agreement; signed by both the offeror and the Department of the Air Force (DAF) Agreements Officer (AO).

Agreements Officer – Title given to a Government representative with the authority to enter into, administer, and/or terminate agreements.

Agreements Officer Representative (AOR)– A Government representative designated and authorized in writing by the agreements officer to perform specific technical or administrative functions.

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at https://www.sam.gov (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

Authoritative Source of Truth (AsoT) – The central reference point for models and data across the lifecycle. The AsoT provides traceability as a system evolves, capturing historical knowledge and connecting authoritative versions of the models and associated data. Types of models include management, design, manufacturing, product support, verification and validation, and specialty engineering.

Behavior Modeling – A model that shows the interactions between objects to produce some particular system behavior that is specified as a use-case. Sequence diagrams (or collaboration diagrams) are used to model interaction between objects.

Business Intelligence (BI) – Strategies and technologies used by enterprises for data analysis of business information. BI technologies provide historical, current, and predictive views of business operations.

Commercial Solution Brief (CSB) – a brief to provide additional information to further elaborate and discuss proposed concept/technology/solution.

Commercial Solutions Opening (CSO) – is a competitive procedure contracting officers may use to acquire innovative commercial items, technologies, or services, as provided in section 803 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 (Pub. L. 117-81), 10 U.S.C. 3458, and DFARS Subpart 212.70.

Commercial Solutions Proposal (CSP) – Technical and price proposal prepared by offerors.

Covered Foreign Entity – for American Security Drone Act of 2023 purposes, an entity included on a list developed and maintained by the Federal Acquisition Security Council (FASC) published in the

System for Award Management (SAM) at https://www.sam.gov.

Digital Ecosystem – A group of interconnected information technology resources that can function as a unit. Digital ecosystems are made up of suppliers, customers, trading partners, applications, third-party data service providers, and all respective technologies. Interoperability is the key to the ecosystem's success.

Digital Engineering (DE) – An integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support lifecycle activities from concept through disposal.

Digital Trinity – The complete approach to digital acquisition of incorporating digital engineering and manufacturing, agile software, and open system architecture into weapon systems by enabling design, assembly, testing, and sustainment in the virtual/digital realm before real-world production begins.

Digital Twin – One-to-one system models, conjoined with their individual real-world systems in data feedback loops, which may or may not be governed by a full digital thread.

Digital Thread – An extensible analytic framework to connect models, and all associated data, software, and functional support, governing more than one system lifecycle phase with one-to-one real-word traceability.

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 Agreement, 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.

Form, Fit, and Function Data – Technical data that describes the required overall physical, functional, and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items. Form, Fit, and Function Data is to be delivered with Unlimited Rights.

Government – The United States of America, as represented by the Department of the Air Force.

Government Purpose – Any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations, or sales or transfers by the United States Government to foreign governments or international organizations. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data for commercial purposes or authorize others to do so.

Government Purpose Rights – the rights to—

(i) Use, modify, reproduce, release, perform, display, or disclose technical data within the

Government without restriction; and
(ii) Release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for United States government purposes.

Government Reference Architecture (GRA) – A model-based, authoritative source of information to guide and constrain mission architectures and solutions. It integrates data, information, boundary conditions, and rules that describe the mission capability needed by the warfighter in sufficient detail to allow for transition of technology-based solutions.

Integrated Digital Environment (IDE) – A compilation of data, models, and tools for collaboration, analysis, and visualization across all functional domains. IDE includes the methodology and specification for data, models, and tools arrangement with processes and procedures to exploit informational results. One note of importance is that the IDE includes the integration of programmatic (program manager, financial manager, logistics manager, etc.) information with the engineering models and data so that the environment is truly integrated.

Integrated Trade Space Analyses – Analyses that address criteria relevant to decision making that can be traded off against one another to achieve specific outcomes to reflect specific alternative solutions. Typical criteria include performance/benefits, schedule, risk, and cost.

Invention – Any invention or discovery which is or may be patentable or otherwise protectable under Title 35 of the United States Code.

Innovative – IAW section 803 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 (Pub. L. 117-81) and 10 U.S.C. 3458(e).

(1) any new technology, process, or method, including research and development that is new as of the date of submission of a proposal; or

(2) any new application that is new as of the date of submission of a proposal of a technology, process, or method existing as of such date.

Machine Learning and Artificial Intelligence – Machine learning enables a computer system to make predictions using historical data without being explicitly programmed. It is a subset of Artificial Intelligence, a technology with which systems can be created to simulate human intelligence (do not require pre-programming).

Milestone Payment – Milestone schedule based on key observable events in the critical path to accomplish program objectives and successful performance. Payments are triggered by successful performance of an observable technical event. Each spiral will outline any milestone schedule for payment.

Model Based Systems Engineering (MBSE) – The formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.

Modeling and Simulation (M&S) – The use of a physical or logical representation of a given system

to generate data and make predictions and support decision making.

Nontraditional Defense Contractor – IAW 10 U.S.C. 3014 means an entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by the Department of Defense for the procurement or transaction, any contract or subcontract for the Department of Defense that is subject to full coverage under the cost accounting standards prescribed pursuant to Section 1502 of Title 41 and the regulations implementing such section.

Nonprofit Research Institution – IAW 15 U.S.C. 3703(3) means an organization owned and operated exclusively for scientific or educational purposes, no part of the net earnings of which inures to the benefit of any private shareholder or individual.

Open System Architecture (OSA) – A system design approach which aims to produce systems that are inherently interoperable and connectable without recourse to retrofit and redesign.

Other Transaction (OT) – Refers to the type of Other Transaction Agreement (OTA) that may be placed as a result of this CSO and associated Area of Interest (AOI) This type of OT is authorized by 10 U.S.C. 4022 prototype projects directly relevant to enhancing the mission effectiveness of military personnel and the supporting platforms, systems, components, or materials proposed to be acquired or developed by the DoD, or for the improvement of platforms, systems, components, or materials in use by the armed forces. This type of OTA is treated by DoD as an acquisition instrument, commonly referred to as an "other transaction" for a prototype project or a 10 U.S.C 4022"other transaction".

Prototype Project – IAW 10 U.S.C. 4022 the term includes a project that addresses –

(1) a proof of concept, model, or process, including a business process;
(2) reverse engineering to address obsolescence;
(3) a pilot or novel application of commercial technologies for defense purposes;
(4) agile development activity;
(5) the creation, design, development, or demonstration of operational utility; or
(6) any combination of subparagraphs (1) through (5).

Such project can generally be described as a proof of concept, model, reverse engineering to address obsolescence, pilot, novel application of commercial technologies for defense purposes, agile development activity, creation, design, development, demonstration of technical or operational utility, or combinations of the foregoing. A process, including a business process, may also be the subject of a prototype project. Although assistance terms are generally not appropriate in OT agreements in 10 U.S.C. 4022 ancillary work efforts that are necessary for completion of the prototype project, such as test site training or limited logistics support, may be included in prototype projects. A prototype may be physical, virtual, or conceptual in nature. The quantity of prototypes/commercial solutions should generally be limited to that needed to prove technical or manufacturing feasibility or evaluate military utility, and pilot authority for installation and facility prototyping.

Restrictions on Obtaining and Disclosing Certain Information – IAW 41 U.S.C. 2101, *et seq*.

Small Business Concerns – Defined in the Small Business Act (15 U.S.C. 632) and 13 CFR Part 121.

Spiral – The Government will publish spirals periodically that outline the specific request (e.g., whitepaper/proposal), the deadlines for submission, the specific ask for the AOI being addressed, and any additional terms/conditions to be incorporated in the resulting award/OT.

Statement of Need – Prototype Solution Statement means the Government problem statement that forms the basis for the Request for Solution Briefs.

Successful Completion of the OT – The appropriate approving official determines in writing that the Prototype OT meets the technical goals, satisfies established Agreement success metrics, or accomplishes a particularly favorable or unexpected result that justifies transition. Each spiral will have a provision describing conditions of successful completion.

Technical Stack or "Tech Stack" – The collection of data, models, software, and associated infrastructure needed to create and optimize the digital representation of a system over its lifecycle.

Unlimited Rights – Rights to use, modify, reproduce, release, perform, display, or disclose data in whole or in part, in any manner and for any purpose whatsoever, and to have or authorize others to do so.

Virtual Twin – The integration of all digital system models, simulation software and environments, and other digital artifacts that are associated and sufficiently representative to describe the design, performance, manufacturing, or sustainment of the system.

WOSA X - extends the concept of WOSA (internal technical standard interface messages for internal weapon communications) to all other aspects of integration details for WOSA hardware assemblies. For example, WOSA compliant weapons will typically delivery all integration details for a WOSA domain in the Domain Implementation Package. The hardware integration details in the Domain Implementation Package may be used to define WOSA-X hardware integration details that become requirements for a given weapon system and or the WOSA domain. The intent is to provide for all integration details needed to integrate a WOSA domain to all prime integrators and supply chain vendors of WOSA domains (e.g. seekers, warheads, turbine engines, and solid rocket motors).

D. Scope (Potential Areas of Interest)

Potential agreements or awards issued under the AFLCMC ADRR CSO may include new technologies, processes, or methods applicable to the following areas of interest (AOI):

- Seeker Science and Technology (S&T) and Prototyping
- Warhead Energetics, Prototyping, and Modeling
- Software Defined Radio Prototyping; weapon to weapon communications network standards, long range kill chain communication standards

- Prototype integration, WOSA modeling, WOSA MOATEL testing, testing of prototype hardware/software with WOSA models
- Initial prototype procurement, prototype production activities to include early manufacturing process verifications
- Advanced system reprogramming concepts
- Modernization
- Prototyping
- Experimentation
- Procurement of Prototypes
- Studies, Demonstrations, Testing of Prototypes
- Cloud Architecting and Software Containerization
- Artificial Intelligence and Machine Learning Implementation
- Infrastructure as Code (IaC)
- Hardware and Software Modifications
- Hardware Design, Test, and Qualification
- Weapon Design
- System Modeling
- Data Mining, Collection, Analysis
- Computer Networks and Networking
- Software & Tools (to include software licenses)
- IT, IDE, and Hardware
- MBSE Related Software Development Kits (SDKs)
- WOSA Domain Software Design & Architecture
- Third Party Software Development
- Software DevSecOps Factory and/or Pipelines
- Munitions Open Architecture Test and Evaluation Lab (MOATEL) Testing Capability and associated hardware, software, and documentation
- Software Lab with Processor In the Loop (SWIL) or Hardware In The Loop (HWIL)
- HWIL Test capabilities with infrared (IR) wall or radio frequency (RF) wall capabilities within Guided Weapons Evaluation Facility (GWEF)
- Platform integration, weapon to weapon datalink testing, NCA Autonomy testing with Golden Horde Colosseum, System testing with HWIL GWEF facility
- Mission Planning Software
- Mission Data
- Weapons Reprogramming Software
- Software Tool Training
- Analytic and Visualization Tool Development
- Red/Blue Target Generation

SECTION II: GUIDELINES FOR SOLUTION BRIEFS

The AFLCMC ADRR CSO for Innovative Execution will be open continuously for a 12-month period and may be extended upon internal review prior to the end of the term. No solution briefs will be accepted under this CSO. Rather, solution briefs are to be submitted in response to the publication of "spirals". The issuing

office, AFLCMC/EBI (DoDAAC FA8659) will amend the CSO to solicit for solution briefs in response to "spirals". Each spiral will include specific information regarding the AOI being solicited, period of performance, technical evaluation criteria, etc.

All definitions and articles included in the ADRR CSO will be applicable and flow down to spirals and potential awards. In addition, spirals and awards will include additional information specific to the AOI and needs of the user.

The Government reserves the right to award an OT under 10 U.S.C. 4022 agreement, or award a FAR Part 12 contract, or award no contract/agreement instrument at all, as a result of this solicitation. Interested parties are encouraged to review 10 U.S.C. 4022, to include 10 U.S.C. 4022(f), regarding award of transactions for prototype projects and possible follow-on production transactions or contracts subject to successful completion of prototype projects awarded using competitive procedures.

The Government may post a Closed or Open Spiral

A. Closed Spiral – Submissions by date/time specified with all evaluations occurring after submission deadline.
    1. Commercial Solution Briefs (CSB) – The Government will evaluate a CSB against the criteria stated in the CSO. Offerors responding to this CSO may be invited to provide additional information to further elaborate and discuss their proposed concept/technology/solution. If the Government requires a virtual demonstration, additional instructions will be provided within the subject AOI.
    2. Commercial Solution Proposal (CSP) - Request for (CSP) Technical and price proposals are requested.

The Government will not be obligated to pay offerors for responding to the CSO or follow-on Spiral proposal activity.

The Government reserves the right to award all, part, or none of the proposals received if requested.

B. Open Spiral – Submissions accepted any time during specified period with evaluations occurring upon receipt.

The Government may add any number of AOIs against this CSO's AOIs at any time within the fiscal year. Interested offerors are encouraged to frequently check this CSO Solicitation on sam.gov and/or https://eglincsoportal.us for new AOI or Spiral postings.

**If in the event the Government chooses to award a FAR 12 contract, the spiral will describe the general guidelines, submission information, clauses, evaluations, and T&C.*

General Guidelines

1. Unnecessarily elaborate brochures or proposals are not desired.
2. Use of diagram(s) or figure(s) to depict the essence of the proposed solution is strongly encouraged.
3. Offerors may submit multiple solution briefs (as required by the specific spiral) to any single AOI if each submission represents a separate and distinct concept. Individual Solution Briefs may only address one concept based on the stated AFLCMC ADRR CSO AOI.

4. Technical data with military application may require approval, authorization, or license for lawful exportation.
5. All Solution Briefs and Proposals shall be unclassified. Solution Briefs and Proposals containing proprietary information that is not to be disclosed to the public for any purpose or used by the Government except for evaluation purposes shall include the following general disclaimer on the cover page:

   "This [select one: Solution Brief or Proposal] includes proprietary information that shall not be disclosed outside the Government, except to non-Government personnel for evaluation purposes, and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this submission. If, however, an agreement is awarded to this Offeror as a result of -- or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent agreed upon by both parties in the resulting agreement. This restriction does not limit the Government's right to use information contained in this proprietary information if it is legally obtained from another source without restriction. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]"

6. Submissions shall be submitted electronically as prescribed in the spiral.
7. Submissions sent through other mediums, channels, and/or after the prescribed spiral open period has ended will not be considered, reviewed nor evaluated.
8. Submission deadlines, instructions, steps, and specific requirements will be published as an amendment to the AFLCMC ADRR CSO – called "spirals".

SECTION III: SUBMISSION INFORMATION

A. Term of the Opening

The term of an award made under this CSO announcement will be identified in the spiral which will be published as an amendment to the AFLCMC ADRR CSO. The AFLCMC ADRR CSO was initially opened for a 12-month period ending on 04 June 2025. Following a subsequent review, it was extended for an additional 12-month period ending on 04 June 2026. This CSO is now validated for an additional 12-month extension, establishing a new closing date of **04 June 2027**, with the option for subsequent extensions subject to review by the AO.

B. Extending the Term

The term of the CSO may be amended by the program office at any point following an internal review of the CSO. Agreements issued off of this CSO will have a standard set of term(s) and conditions as provided here and also may include specific terms and conditions based on need and as agreed between the Agreements Officer (AO) and the Vendor Administrator.

C. CSO Provision-Subject to Availability of Funds.

Funds are not presently available for this CSO. The Government's obligation under this CSO is contingent upon the availability of appropriated funds from which payment for CSO purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Agreement/Contracting Officer for subsequent AOIs until the contractor or awardee(s) receives notice of such availability, to be confirmed in writing by the Agreement/Contracting Officer.

D. Submission Sensitive Information:

Restrictive notices notwithstanding, during the evaluation process, submissions may be handled by Government-contracted Non-Government advisors for administrative purposes and/or to assist with technical evaluation(s) (i.e., government support contractors). These government support contractors are expressly prohibited from business lines competing in the CSO AOI and are bound by appropriate NDA submissions. The original of each submission received will be retained and all other non-required copies destroyed. A certification of destruction may be requested, provided the formal request is received by the contracting office within 5 days after notification that the proposal was not selected.

E. In order to receive an award, offerors must:

- Have a Unique Entity Identifier (UEI) number and must register in the System for Award Management (SAM) prior to receiving an award or agreement.
- Register in the prescribed Government invoicing system (Wide Area Work Flow): https://piee.eb.mil/xhtml/unauth/help/newuser.xhtml
- Represent their small business size and status as required in the solicitation.
- Be determined to be responsible by the Contracting/Agreements Officer and must not be suspended or debarred from award by the Federal Government nor be prohibited by Presidential Executive Order and/or law from receiving an award.

SECTION IV: EVALUATION CRITERIA

The primary evaluation factors for selecting proposals for award shall be technical merit, importance to agency programs, and funds availability. Price will be considered to the extent appropriate, but at a minimum, to determine that the price is fair and reasonable.

Each proposal will be evaluated by the Government and the proposal must stand on its own technical merit. Proposals received as a result of the AFLCMC ADRR CSO will be evaluated in accordance with the specific evaluation criteria stated in the spiral.

SECTION V: ARTICLES

Articles under this section are applicable to all awards made off of the AFLCMC ADRR CSO. The articles may be tailored for specific awards and awards may incorporate additional articles depending on the program requirements.

Some articles, like Article V and Article VI, require fill-ins to be provided by the offeror and the Government. Instructions on how to complete will be provided at the spiral level.

Article I: Ombudsman

(a) Before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommendations to the Agreements officer for resolution. Consulting an ombudsman does not alter or postpone the timelines for any other processes.

(b) If resolution cannot be made by the Agreements Officer, the interested party may contact the ombudsman.

Phone 310-710-2734
Email cecilia.montes_de_oca@us.af.mil

Concerns, issues, disagreements, and recommendations that cannot be resolved at the Center/MAJCOM/DRU/SMC ombudsman level, may be brought by the interested party for further consideration to the Department of the Air Force ombudsman, Associate Deputy Assistant Secretary (ADAS) (Contracting), SAF/AQC, 1060 Air Force Pentagon, Washington DC 20330-1060, phone number (571) 256-2395, facsimile number (571) 256-2431.

(c) The ombudsman has no authority to render a decision that binds the agency.

(d) Do not contact the ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries shall be directed to the Agreements Officer.

Article II: Debrief/Notification of Award

The Government will conduct post-award debriefings upon request only. Debriefings to unsuccessful offerors shall be provided upon request in accordance with provisions and timelines of 10 U.S.C. 2305 and Section 818 of National Defense Authorization Act for 2018.

Article III: Patent Rights

A. Allocation of Principal Rights
    1. Unless the Vendor shall have notified The Department of the Air Force (DAF), in accordance with subparagraph B.2 below, that the Vendor does not intend to retain title, the Vendor shall retain the entire right, title, and interest throughout the world to each Subject Invention consistent with the provisions of this Article.
    2. With respect to any Subject Invention in which the Vendor retains title, DAF shall have a nonexclusive, nontransferable, irrevocable, paid-up license to practice or have practiced on behalf of the United States the Subject Invention throughout the world.

B. Invention Disclosure, Election of Title, and Filing of Patent Application
    1. The Vendor shall disclose each Subject Invention to DAF within four (4) months after the inventor discloses it in writing to his Vendor personnel responsible for patent matters. The disclosure to DAF shall be in the form of a written report and shall identify the Agreement and circumstances under which the Invention was made and the identity of the inventor(s). It shall be sufficiently complete in technical detail to convey a clear understanding, to the extent known at the time of the disclosure, of the nature, purpose, operation, and the physical, chemical, biological, or electrical characteristics of the Invention. The disclosure shall also identify any publication, sale, or public use of the invention and whether a manuscript describing the Invention has been submitted and/or accepted for publication at the time of disclosure.
    2. If the Vendor determines that it does not intend to retain title to any such Invention, the Vendor shall notify DAF, in writing, within eight (8) months of disclosure to DAF. However, in any case where publication, sale, or public use has initiated the one-year statutory period wherein valid patent protection can still be obtained in the United States, the period for such notice may be shortened by DAF to a date that is no more than sixty (60) calendar days prior to the end of the statutory period.
    3. The Vendor shall file its initial patent application on a Subject Invention to which it elects

to retain title within one (1) year after election of title or, if earlier, prior to the end of the statutory period wherein valid patent protection can be obtained in the United States after a publication, or sale, or public use. The Vendor may elect to file patent applications in additional countries, including the European Patent Office and the Patent Cooperation Treaty, within either ten (10) months of the corresponding initial patent application or six (6) months after the date permission is granted by the Commissioner for Patents to file foreign patent applications, where such filing had previously been prohibited by a Secrecy Order.

4. The Vendor shall notify DAF of any decisions not to continue the prosecution of a patent application, pay maintenance fees, or defend in a reexamination or opposition proceedings on a patent, in any country, not less than thirty (30) calendar days before the expiration of the response period required by the relevant patent office.
5. Requests for extension of the time for disclosure election, and filing under this Article, may be granted at DAF's discretion after considering the circumstances of the Vendor and the overall effect of the extension.
6. The Vendor shall submit to DAF annual listings of Subject Inventions. At the completion of the Agreement, the Vendor shall submit a comprehensive listing of all subject inventions identified during the course of the Agreement and the current status of each.

C. Conditions When the Government May Obtain Title

Upon Department of the Air Force's written request, the Vendor shall convey title to any Subject Invention to The Department of the Air Force under any of the following conditions:

1. If the Vendor fails to disclose or elects not to retain title to the Subject Invention within the times specified in Paragraph B of this Article; however, DAF may only request title within sixty (60) calendar days after learning of the failure of the Vendor to disclose or elect within the specified times;
2. In those countries in which the Vendor fails to file patent applications within the times specified in Paragraph B of this Article; however, if the Vendor has filed a patent application in a country after the times specified in Paragraph B of this Article, but prior to its receipt of the written request by DAF, the Vendor shall continue to retain title in that country; or
3. In any country in which the Vendor decides not to continue the prosecution of any application for, to pay the maintenance fees on, or defend in reexamination or opposition proceedings on, a patent on a Subject Invention.

D. Minimum Rights to the Vendor and Protection of the Vendor's Right to File

1. The Vendor shall retain a nonexclusive, royalty-free license throughout the world in each subject invention to which the Government obtains title, except if the Vendor fails to disclose the Subject Invention within the times specified in Paragraph B of this Article.

   The Vendor's license extends to its domestic subsidiaries and affiliates, including Canada, if any, and includes the right to grant licenses of the same scope to the extent that the Vendor was legally obligated to do so at the time the Agreement was awarded. The license is transferable only with the approval of DAF, except when transferred to the successor of that part of the business to which the Subject Invention pertains. DAF approval for license transfer shall not be unreasonably withheld.

2. The Vendor's domestic license may be revoked or modified by DAF to the extent necessary to achieve expeditious practical application of the Subject Invention pursuant to an application for an exclusive license submitted consistent with appropriate provisions at 37 C.F.R. Part 404. This license shall not be revoked in that field of use or the geographical areas in which the Vendor has achieved practical application and continues to make the benefits of the Subject Invention reasonably accessible to the public. The license in any foreign country may be revoked or modified at the discretion of DAF to the extent the Vendor, its licensees, or the subsidiaries or affiliates have failed to achieve practical application in that foreign country.
3. Before revocation or modification of the license, DAF shall furnish the Vendor a written notice of its intention to revoke or modify the license, and the Vendor shall be allowed thirty (30) calendar days (or such other time as may be authorized for good cause shown) after the notice to show cause why the license should not be revoked or modified.

E. Action to Protect the Government's Interest

1. The Vendor agrees to execute or to have executed and promptly deliver to DAF all instruments necessary to (i) establish or confirm the rights the Government has throughout the world in those Subject Inventions to which the Vendor elects to retain title, and (ii) convey title to DAF when requested under Paragraph C of this Article and to enable the Government to obtain patent protection throughout the world in that Subject Invention
2. The Vendor agrees to require by written agreement with its employees, other than clerical and non-technical employees, to disclose promptly in writing to personnel identified as responsible for the administration of patent matters and in a format suggested by the Vendor each Subject Invention made under this Agreement in order that the Vendor can comply with the disclosure provisions of Paragraph B of this Article. The Vendor shall instruct employees, through employee agreements or other suitable educational programs, on the importance of reporting inventions in sufficient time to permit the filing of patent applications prior to United States or foreign statutory bars.
3. The Vendor shall include, within the specification of any United States patent application and any patent issuing thereon covering a subject invention, the following statement:

   This invention was made with Government support under Agreement No. FAXXXX-XX-S-XXXX, awarded by DAF. The Government has certain rights in the invention. (This will be filled in IAW spiral instructions).

F. Lower Tier Agreements

The Vendor shall include this Article, suitably modified, in all subcontracts or lower tier agreements, regardless of tier, for experimental, developmental, or research work.

G. Reporting on Utilization of Subject Inventions

1. The Vendor agrees to submit, during the term of the Agreement, an annual report on the utilization of a Subject Invention or on efforts at obtaining such utilization that are being made by the Vendor or its licensees or assignees. Such reports shall include information regarding the status of development, date of first commercial sale or use, gross royalties received by the Vendor, and such other data and information as the agency may reasonably specify. The Vendor also agrees to provide additional reports as may be

requested by DAF in connection with any march-in proceedings undertaken by DAF in accordance with Paragraph I of this Article. DAF agrees it shall not disclose such information to persons outside the Government without permission of the Vendor, unless required by law.

2. All required reporting shall be accomplished, to the extent possible, using the i-Edison reporting website: https://www.nist.gov/iedison. To the extent any such reporting cannot be carried out by use of i-Edison, reports and communications shall be submitted to the AO and Administrative Agreements Officer (AAO), where one is appointed.

H. Preference for American Industry

Notwithstanding any other provision of this article the Vendor agrees that it shall not grant to any person the exclusive right to use or sell any Subject Invention in the United States unless such person agrees that any product embodying the Subject Invention or produced through the use of the subject invention shall be manufactured substantially in the United States. However, in individual cases, the requirements for such an agreement may be waived by DAF upon a showing by the Vendor that reasonable but unsuccessful efforts have been made to grant licenses on similar terms to potential licensees that would be likely to manufacture substantially in the United States or that, under the circumstances, domestic manufacture is not commercially feasible.

I. March-in Rights

The Vendor agrees that, with respect to any Subject Invention in which it has retained title, DAF has the right to require the Vendor, an assignee, or exclusive licensee of a Subject Invention to grant a non-exclusive license to a responsible applicant or applicants, upon terms that are reasonable under the circumstances, and if the Vendor, assignee, or exclusive licensee refuses such a request, DAF has the right to grant such a license itself if DAF determines that:

1. Such action is necessary because the Vendor or assignee has not taken effective steps, consistent with the intent of this Agreement, to achieve practical application of the Subject Invention;
2. Such action is necessary to alleviate health or safety needs which are not reasonably satisfied by the Vendor, assignee, or their licensees;
3. Such action is necessary to meet requirements for public use and such requirements are not reasonably satisfied by the Vendor, assignee, or licensees; or
4. Such action is necessary because the agreement required by Paragraph H of this Article has not been obtained or waived or because a licensee of the exclusive right to use or sell any Subject Invention in the United States is in breach of such Agreement.

Article IV: Termination

The Government may terminate this Agreement by written notice to the Vendor, provided that such written notice is preceded by consultation between the Parties. The Vendor may request Agreement termination by giving the Government sixty (60) days written notification of their intent to do so. If the Vendor decides to request termination of this Agreement, the Government may, at its discretion, agree to terminate. The Government and the Vendor should negotiate in good faith a reasonable and timely adjustment of all outstanding issues between the Parties as a result of termination, which may include non-cancelable commitments. In the event of a termination of the Agreement, the Government shall have

paid-up rights in Data as described in Article V, Data Rights. Failure of the Parties to agree to an equitable adjustment shall be resolved pursuant to Article VII, Disputes.

The Agreements Officer may also unilaterally terminate performance of work under this Agreement or a project funded under this Agreement, in whole or in part, based on a reasonable determination that the Agreement/Project will not produce beneficial results commensurate with the expenditure of resources. The USG may terminate this Agreement, in whole or in part, if the AO determines that a termination is in the USG's best interest. The AO shall terminate by delivering a Notice-of Termination specifying the extent of termination and the effective date.

After receipt of a Notice of Termination, and except as directed by the AO, the ACO shall immediately proceed with the following obligations, regardless of any delay in determining or adjusting any amounts due:

1. Stop work and direct Awardees to stop work as specified in the notice.
2. Place no further projects or orders for materials, services, or facilities, except as necessary to complete the continued portion of the Agreement or project.
3. Terminate all orders to the extent they relate to the work terminated.
4. With approval or ratification to the extent required by the AO, settle all outstanding liabilities and termination settlement proposals arising from the termination of orders. The approval or ratification will be final.
5. As directed by the AO, obtain from the Awardee under the terminated portion of the Agreement a transfer of title to the following. where applicable and deliver to the USG: The fabricated or unfabricated payments, work in process, completed work, supplies, other material produced or acquired for the work terminated, completed or partially completed plans, drawings, information, and other property that, if the order had been completed, would have been required to be furnished to the USG.
6. Complete performance of any work not terminated, if applicable.
7. Take any action that may be necessary, or that the AO may direct, for the protection and preservation of the property related to the Agreement or any projects hereunder that is in the possession of the Awardee(s) and in which the USG has or may acquire an interest.
8. Use its best efforts to sell, as directed or authorized by the AO, any property of the types referred to under Property Article, provided that the vendor or awardee(s)

   (A) Is not required to extend credit to any purchaser; and

   (B) May arrange for the Awardee(s) who were performing the terminated work to acquire the property under the conditions prescribed by, and at prices approved by the AO. The proceeds of any transfer or disposition of property will be applied to reduce any payments to be made to the USG under that particular project.

Termination Costs. The USG, and the Awardees will negotiate in good faith an equitable reimbursement for work performed toward accomplishment of the task(s) of Projects. The USG will allow full credit for the USG share of the obligations properly incurred by the contractor/vendor or the awardee(s) prior to termination. Costs incurred by Awardees during a suspension or after termination of a Project are not allowable unless the Agreements Officer expressly authorizes them in either the notices of suspension, termination, or subsequent notice. Other Awardee costs

incurred during a suspension or after termination which are necessary and reasonably unavoidable are allowed if:

1. The fees which result from obligations which were properly earned by the contractor/vendor or the awardee(s) or costs properly incurred by the Awardee before the effective date of the suspension or termination, are not in anticipation of it, and in the case of a termination, are noncancellable; and

2. The costs would be allowable if the Project was not suspended or the award expired normally at the end of the funding period in Which the termination takes effect.

Article V: Data Rights

A. Allocation of Principal Rights

1. The Parties agree that in consideration for Government funding, the Vendor intends to reduce to practical application items, components and processes developed under this Agreement.

2. With respect to Data developed or generated under this Agreement related to the

   (INSERT DELIVERABLE PROTOTYPE – to be inserted by the offeror IAW spiral instructions at the time of offer), the Government shall receive (INSERT APPLICABLE DATA RIGHTS), as defined in Section 1C.

3. With respect to Data delivered under the Agreement, the Government shall receive (INSERT APPLICABLE DATA RIGHTS – to be inserted by the offeror IAW spiral instructions at the time of offer). Notwithstanding the provision in A.4, the Vendor agrees, with respect to data generated or developed under this Agreement, the Government may, within (INSERT NUMBER OF YEARS to be inserted by the offeror IAW spiral instructions at the time of offer) after completion or termination of this Agreement, require delivery of data and receive (INSERT APPLICABLE DATA RIGHTS – to be inserted by the offeror IAW spiral instructions at the time of offer).

4. March-In Rights

   (a) In the event the Government chooses to exercise its March-in Rights, as defined in Article III, sub paragraph I of this Agreement, the Vendor agrees, upon written request from the Government, to deliver at no additional cost to the Government, all Data necessary to achieve practical application within sixty (60) calendar days from the date of the written request. The Government shall retain Unlimited Rights, as defined in Article I, Section B of this Agreement, to this delivered Data.

   (b) To facilitate any potential deliveries, the Vendor agrees to retain and maintain in good condition until (INSERT NUMBER OF YEARS - be inserted by the offeror IAW spiral instructions at the time of offer) after completion or termination of this Agreement, all Data necessary to achieve practical application of any Subject Invention as defined in Article V of this Agreement.

B. Marking of Data

Pursuant to Paragraph A above, any Data delivered under this Agreement shall be marked with the following legend:

Use, duplication, or disclosure is subject to the restrictions and will be pursuant to an agreement issued off of this CSO as stated in Agreement [INSERT AGREEMENT NUMBER FAXXXX-XX-S-XXXX] between the Government and the Vendor.

C. Lower Tier Agreements

The Vendor shall include this Article, suitably modified to identify the Parties, in all subcontracts or lower tier agreements, regardless of tier, for experimental, developmental, or research work.

Article VI: Obligation and Payment

The publication of the AFLCMC ADRR CSO is not authorization to begin performance for any effort and in no way obligates the Government for any costs incurred by the Offeror associated with developing a solution brief. Funds are not presently available for this effort. No award or agreement will be made until funds are available. The Government reserves the right to cancel the AFLCMC ADRR CSO and any subsequent spirals at any time.

A. Obligation

The Government's liability to make payments to the Vendor is limited to only those funds obligated under an agreement or modification to an agreement made as a result of this CSO. The Department of the Air Force may obligate funds in full or incrementally as determined in each specific spiral.

B. Payments

1. The Parties agree that fixed payments will be made for the completion of milestones. These payments reflect value received by the Government toward the accomplishment of the research goals of this Agreement.

2. The Vendor shall document the accomplishments of each milestone by submitting or otherwise providing the Milestones Report required by Attachment X. The Vendor shall submit one (1) copy of all invoices to the AO or appointee for payment approval. After written verification of the accomplishment of the milestone by the DAF AOR, and approval by the AO/appointee, the Vendor will submit their invoice through Wide Area Work Flow (WAWF), as detailed in this Article.

3. Limitation of Funds: In no case shall the Government's financial liability exceed the amount obligated under this Agreement.

4. Limitation of the Government Obligations: In no event shall the Government's financial liability exceed the amount obligated under any agreement. Awardee's liability shall not exceed committed funding on agreement or per milestone. Nothing in this Article shall be construed to create the basis of a claim or suit where none would otherwise exist. The Government does not contemplate any unusually hazardous risks being associated with the awarded projects.

5. Payments will be made by the Defense Finance and Accounting Services office, as indicated below, within thirty (30) calendar days of an accepted invoice in WAWF. WAWF is a secure web-based system for electronic invoicing, receipt and acceptance. The WAWF application enables electronic form submission of invoices, government inspection, and acceptance documents in order to support DoD's goal of moving to a paperless acquisition process. Authorized DoD users are notified of pending actions by e-mail and are presented with a collection of documents required to process the contracting or financial action. It uses Public Key Infrastructure (PKI) to electronically bind the digital signature to provide non-refutable proof that the user electronically signed the document with the contents. Benefits include online access and full spectrum view of document status, minimized re-keying and improving data accuracy, eliminating unmatched disbursements and making all documentation required for payment easily accessible.

6. The Vendor is required to utilize the WAWF system when processing invoices and receiving reports under this Agreement. The Vendor shall (i) ensure an Electronic Business Point of Contact is designated in System for Award Management (SAM) at http://www.sam.gov and (ii) register to use WAWF–RA at the https://wawf.eb.mil site, within ten (10) calendar days after award of this Agreement. Step-by-step procedures to register are available at the https://wawf.eb.mil site. The Vendor is directed to use the 2-in-1 format when processing invoices. The Vendor shall maintain an active registration for "All Awards" in System for Award Management (SAM) throughout the life of the award. The Vendor should submit a copy of the AOR approval of the milestone, as well as a copy of the milestone report, with each invoice. For WAWF Payment and Invoicing Support, email DAFInvoices@DAF.mil or contact WAWF help desk at 866-618- 5988 or email disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil.

*Below fill-ins will be completed by the requesting Government activity and will be specific for each spiral.

a. For the "Issue By" DoDAAC, enter FAXXXX, Extension *(INSERT AO'S EXTENSION)*.
b. For the "Admin DoDAAC, enter FAXXXX.
c. For the "Service Acceptor AOR" fields, enter the Service Acceptor AOR DoDAAC.
d. Leave the "Inspect by" DoDAAC, "Ship From Code" DoDAAC, "Service Approver", and "LPO" DoDAAC fields blank unless otherwise directed by the Agreements Officer.
e. The following guidance is provided for invoicing processed under this Agreement through WAWF:
   - The AOR identified in Article IV, "Agreement Administration" shall continue to formally inspect and accept the deliverables/ milestones. To the maximum extent practicable, the AOR shall review the deliverable(s)/ milestone report(s) and either: 1) provide a written notice of rejection to the Vendor which includes feedback regarding deficiencies requiring correction, or 2) written notice of acceptance to the DAF PM and Agreements Officer.
   - Acceptance within the WAWF system shall be performed by the AOR upon receipt of a confirmation email, or other form of transmittal, from the AOR.
   - The Vendor shall send an email notice to the AOR and upload the AOR approval as an attachment upon submission of an invoice in WAWF (this can be done from within WAWF).
   - Payments shall be made by DFAS (*INSERT APPROPRIATE DFAS OFFICE NAME AND*

DODAAC).

- The Vendor agrees, when entering invoices entered in WAWF to utilize the agreement line-item number (ALIN) and accounting classification reference number (ACRN) associated with each milestone as delineated at Attachment 3. The description of the CLIN shall include reference to the associated milestone number along with other necessary descriptive information. The Vendor agrees that the Government may reject invoices not submitted in accordance with this provision.

Note for DFAS: The Agreement shall be entered into the DFAS system by ALIN – Milestone association (MS)/ACRN as delineated at Attachment X. The Agreement is to be paid out by ALIN (MS)/ACRN. Payments shall be made using the ALIN (MS)/ACRN association as delineated at Attachment X.

f. Payee Information: As identified at SAM.
   - Cage Code:
   - SAM UEI:
   - TIN:

7. Payments shall be made in the amounts set forth in Attachment X, provided the DAF AOR has verified the accomplishment of the milestones.

C. Financial Records and Reports:

1. The Vendor shall maintain adequate records to account for all funding under this Agreement. Upon completion or termination of this Agreement, whichever occurs earlier, the Vendor shall furnish to the AO a copy of the Final Report to the AO required by the spiral. The Vendor's relevant financial records are subject to examination or audit on behalf of DAF by the Government for a period not to exceed three (3) years after expiration of the term of this Agreement. The AO or designee shall have direct access to sufficient records and information of the Vendor, to ensure full accountability for all funding under this Agreement. Such audit, examination, or access shall be performed during business hours on business days upon prior written notice and shall be subject to the security requirements of the audited party.
2. To the extent that the total government payments under the Agreement exceed $5,000,000, the Comptroller General of the United States, in its discretion, shall have access to and the right to examine records of any party to the Agreement or any entity that participates in the performance of this Agreement that directly pertain, to and involve transactions relating to, the Agreement for a period of three (3) years after final payment is made. This requirement shall not apply with respect to any party to this Agreement or any entity that participates in the performance of the Agreement, or any subordinate element of such party or entity, that, in the year prior to the date of the Agreement, has not entered into any other contract, grant, cooperative agreement, or other transaction agreement that provides for audit access to its records by a government entity in the year prior to the date of this Agreement. This paragraph only applies to any record that is created or maintained in the ordinary course of business or pursuant to a provision of law. The terms of this paragraph shall be included in all sub-agreements/contracts to the Agreement.

Article VII: Disputes

A. General

The Parties shall communicate with one another in good faith and in a timely and cooperative manner when raising issues under this Article.

B. Dispute Resolution Procedures

1. Any disagreement, claim or dispute between The Government and the Vendor concerning questions of fact or law arising from or in connection with this Agreement, and, whether or not involving an alleged breach of this Agreement, may be raised only under this Article.

2. Whenever disputes, disagreements, or misunderstandings arise, the Parties shall attempt to resolve the issue(s) involved by discussion and mutual agreement as soon as practicable. In no event shall a dispute, disagreement or misunderstanding which arose more than three (3) months prior to the notification made under subparagraph B.3 of this article constitute the basis for relief under this article unless the Director of Contracting, Air Force Life Cycle Management Center in the interests of justice waives this requirement.

3. Failing resolution by mutual agreement, the aggrieved Party shall document the dispute, disagreement, or misunderstanding by notifying the other Party in writing of the relevant facts, identify unresolved issues, and specify the clarification or remedy sought. Within five (5) working days after providing notice to the other Party, the aggrieved Party may, in writing, request a joint decision by the AFLCMC Senior Procurement Executive and senior executive, no lower than (INSERT A LEVEL OF EXECUTIVE FAR ENOUGH REMOVED FROM THE PROGRAM TO MAINTAIN A GREATER LEVEL OF IMPARTIALITY – THIS IS TO BE COMPLETED BY THE OFFEROR AT THE TIME OF SUBMISSION IAW SPIRAL INSTRUCTIONS) level, appointed by the Vendor. The other Party shall submit a written position on the matter(s) in dispute within thirty (30) calendar days after being notified that a decision has been requested. The AFLCMC Senior Procurement Executive and the senior executive shall conduct a review of the matter(s) in dispute and render a decision in writing within thirty (30) calendar days of receipt of such written position. Any such joint decision is final and binding.

4. In the absence of a joint decision, upon written request to the Deputy Director of Contracting, Air Force Life Cycle Management Center, made within thirty (30) calendar days of the expiration of the time for a decision under subparagraph B.3 above, the dispute shall be further reviewed. The Deputy Director of DAF may elect to conduct this review personally or through a designee or jointly with a senior executive, no lower than (INSERT A LEVEL OF EXECUTIVE FAR ENOUGH REMOVED FROM THE PROGRAM TO MAINTAIN A GREATER LEVEL OF IMPARTIALITY THIS IS TO BE COMPLETED BY THE OFFEROR AT THE TIME OF SUBMISSION IAW SPIRAL INSTRUCTIONS) level, appointed by the Vendor. Following the review, the Deputy Director of DAF or designee will resolve the issue(s) and notify the Parties in writing. Such resolution is not subject to further administrative review and, to the extent permitted by law shall be final and binding.

D. Limitation of Damages

Claims for damages of any nature whatsoever pursued under this Agreement shall be limited to direct damages only up to the aggregate amount of DAF funding disbursed as of the time the dispute arises. In no event shall DAF be liable for claims for consequential, punitive, special and

incidental damages, claims for lost profits, or other indirect damages.

Article VIII: Safeguarding Covered Defense Information and Cyber Incident Reporting

A. Adequate Security

The VENDOR shall provide adequate security on all Covered VENDOR information systems. To provide adequate security, the VENDOR shall implement, at a minimum, the following information security protections:

1. For covered VENDOR information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

   a. Cloud computing services shall be subject to the security requirements specified:

      i. The VENDOR shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) found at https://public.cyber.mil/dccs unless notified by the Agreements Officer Representative (AOR) that this requirement has been waived by the DoW Chief Information Officer (CIO).

      ii. The VENDOR shall maintain within the U.S. or outlying areas all Government data that is not physically located on Government premises, unless the VENDOR receives written notification from the AOR to use another location.

   b. Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this agreement.

2. For covered VENDOR information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph A.1. of this Article, the following security requirements apply:

   a. Except as provided in paragraph A.2.b. of this Article, the covered VENDOR information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, Revision 2" (available at https://www.acq.osd.mil/dpap/policy/policyvault/USA001074-24-DPC.pdf).

   b. The NIST Considerations:

      i. The VENDOR shall implement NIST SP 800-171, as soon as practical.

      ii. The VENDOR shall submit requests to vary from NIST SP 800-171 in writing to the Agreements Officer (AO), for consideration by the DoW CIO. The VENDOR need not implement any security requirement adjudicated by an authorized representative of the DoW CIO to be non-applicable or to have an alternative, but equally effective, security measures that may be implemented in its place.

      iii. If the DoW CIO has previously adjudicated the VENDOR's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the AO or AOR when requesting its recognition under this agreement.

      iv. If the VENDOR intends to use an external cloud service provider to store, process, or transmit any Covered Defense Information in performance of this agreement, the VENDOR shall require and ensure that the cloud service provider meets security requirements equivalent to those

established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements in paragraphs C through F of this Article for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

3. Apply other information systems security measures when the VENDOR reasonably determines that information systems security measures, in addition to those identified in paragraphs A.1 and A.2 of this Article, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

4. The Vendor shall provide access, on a mutually agreeable basis, to its facilities, systems, and personnel necessary for the Government to conduct a NIST SP 800-171 DoW Assessment, using the methodology described at 32 CFR 170.24, if necessary.

B. Cyber Incident Reporting

1. When the VENDOR discovers a cyber incident that affects a covered VENDOR information system or the Covered Defense Information residing therein, or that affects the VENDOR's ability to perform the requirements of the Agreement that are designated as Operationally Critical Support and identified in the agreement, the VENDOR shall—

   b. Conduct a review for evidence of compromise of Covered Defense Information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered VENDOR information system(s) that were part of the cyber incident, as well as other information systems on the VENDOR's network(s), that may have been accessed as a result of the incident in order to identify compromised Covered Defense Information, or that affect the VENDOR's ability to provide Operationally Critical Support; and

   c. Rapidly report (within 72-hours of discovery) cyber incidents to DoW at https://dibnet.dod.mil.

2. Cyber Incident report. The Cyber Incident Report shall be treated as information created by or for DoW and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

C. Malicious Software

When the VENDOR or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoW Cyber Crime Center (DC3) at this website: https://www.dc3.mil/ or in accordance with additional instructions provided by DC3 or the AO or the AOR. Do not send the malicious software to the AO or AOR.

D. Media Preservation and Protection

When a VENDOR discovers a cyber incident has occurred, the VENDOR shall preserve and protect images of all known affected information systems identified in paragraph B.1.a. of this Article and all relevant monitoring/packet capture data for at least 90 calendar days from the submission of the Cyber Incident Report to allow DoW to request the media or decline interest.

E. Access to Additional Information or Equipment Necessary for Forensic Analysis

Upon request by DoW, the VENDOR shall provide DoW with access to additional information or equipment that is necessary to conduct a forensic analysis.

F. Cyber Incident damage assessment activities

If DoW elects to conduct a damage assessment, the AO will request that the VENDOR provide all of the damage assessment information gathered in accordance with paragraph D of this Article.

G. DoW safeguarding and use of VENDOR attributional/proprietary information

The Government shall protect against the unauthorized use or release of information obtained from the VENDOR (or derived from information obtained from the VENDOR) under this Article that includes VENDOR attributional/proprietary information, including such information submitted in accordance with paragraph B. To the maximum extent practicable, the VENDOR shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the VENDOR attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

H. Use and release of Vendor attributional/proprietary information not created by or for DoW

Information that is obtained from the VENDOR (or derived from information obtained from the VENDOR) under this Article that is not created by or for the DoW is authorized to be released outside of the DoW -

1. To entities with missions that may be affected by such information;
2. To entities that may be called upon to assist in the diagnosis, detection, or mitigation of Cyber Incidents;
3. To Government entities that conduct counterintelligence or law enforcement investigations;
4. For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 C.F.R. Part 236).
5. To a support services vendor that is directly supporting Government activities under a federal procurement contract subject to the Defense Federal Acquisition Regulation Supplement (DFARS) that includes the clause at 252.204-7009, *Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.*

I. Use and release of VENDOR attributional/proprietary information created by or for DoW

Information that is obtained from the VENDOR (or derived from information obtained from the VENDOR) under this Article that is created by or for the DoW (including the information submitted pursuant to paragraph B of this Article) is authorized to be used and released outside of the DoW for purposes and activities authorized by paragraph H of this Article, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

J. Other safeguarding or reporting requirements

The safeguarding and cyber incident reporting required by this Article in no way abrogates the VENDOR's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable Articles of this agreement, or as a result of other applicable U.S. Government statutory or regulatory requirements.

K. Lower Tier Agreements

The VENDOR shall include this Article, suitably modified to identify the Parties, in all subcontracts or lower tier agreements entered into solely in connection with this Agreement.

Definitions

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Covered VENDOR information system" means an unclassified information system that is owned, or operated by or for, a VENDOR and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is—

a. Marked or otherwise identified in the agreement, task order, or delivery order and provided to the VENDOR by or on behalf of DoW in support of the performance of the agreement; or

b. Collected, developed, received, transmitted, used, or stored by or on behalf of the VENDOR in support of the performance of the Agreement.

"Controlled Unclassified Information (CUI)" means unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. Instructions for the use, marking, dissemination, and storage of CUI can be found in DoW Instruction 5200.48, "Controlled Unclassified Information (CUI)."

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to agreement administration, such as financial, administrative, cost or pricing, or management information.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Government" means the U.S. Government.

"Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which

covered defense information is recorded, stored, or printed within a covered VENDOR information system.

"Operationally critical support'' means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Article IX: Follow-on Production Contracts or Other Transactions

In accordance with 10 U.S.C. 4022(f), the Government may award a follow-on production contract or Other Transaction (OT) to the Vendor, or a recognized successor in interest to the OT, following the successful completion of this entire Agreement, as modified.

Article X: Title to and Disposition of Property (if the Vendor will be acquiring property valued at more than $5K, use a tailored version)

A. Title to Property (USE THIS PARAGRAPH IF NO PROPERTY BEING ACQUIRED OVER $5,000.)

No significant items of property are expected to be acquired under this Agreement. Title to each item of property acquired under this Agreement with an acquisition value of $5,000 or less shall vest in the Vendor upon acquisition with no further obligation of the Parties unless otherwise determined by the AO. Should any item of property with an acquisition value greater than $5,000 be required, the Vendor shall obtain prior written approval of the AO. Title to the property shall also vest in the Vendor upon acquisition. The Vendor shall be responsible for the maintenance, repair, protection, and preservation of all property at its own expense. The Vendor's deliverable prototype shall not be classified as property.

A. Title to Property (USE THIS PARAGRAPH IF THERE WILL BE PROPERTY ACQUIRED OVER $5,000.)

The Vendor will acquire property with an acquisition value greater than $5,000 under this Agreement as set forth in Attachment 4, which is necessary to further the research and development goals of this Program and is not for the direct benefit of the Government. Title to any other items of property acquired under this Agreement with an acquisition value of $5,000 or less shall vest in the Vendor upon acquisition with no further obligation of the Parties unless otherwise determined by the AO. Should any other item of property with an acquisition value greater than $5,000 be required, the Vendor shall obtain prior written approval of the AO. The Vendor shall be responsible for the maintenance, repair, protection, and preservation of all property at its own expense.

B. Disposition of Property

At the completion of the term of this Agreement, items of property with an acquisition value greater than $5,000 shall be disposed of in the following manner, subject to review and approval by the AO:

1. Purchased by the Vendor at an agreed-upon price, the price to represent fair market value, with the proceeds of the sale being returned to DAF; or
2. Transferred to a Government research facility with title and ownership being transferred to the Government; or
3. Donated to a mutually agreed University or technical learning center for research purposes; or
4. Any other DAF-approved disposition procedure.

Article XI: Civil Rights Act

This Agreement is subject to the compliance requirements of Title VI of the Civil Rights Act of 1964 as amended (42 U.S.C. 2000d) relating to nondiscrimination in Federally assisted programs. The Vendor has signed an Assurance of Compliance with the nondiscriminatory provisions of the Act.

Article XII: Execution

This Agreement constitutes the entire agreement of the Parties and supersedes all prior and contemporaneous agreements, understandings, negotiations, and discussions among the Parties, whether oral or written, with respect to the subject matter hereof. This Agreement may be revised only by written consent of the Vendor and the DAF AO. This Agreement, or modifications thereto, may be executed in counterparts each of which shall be deemed as original, but all of which taken together shall constitute one and the same instrument.

Article XIII: Security Prohibitions and Exclusions

Prohibition
Unless a waiver or exception applies, the Vendor is prohibited from providing any products or services to the Government or using in the performance of the agreement any of the following:

(a) Covered Applications and Articles
(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Vendor under this agreement, including equipment provided by the Vendor's employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328)).
(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91)).

(b) Covered Telecommunications
(1) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).
(2) This does not prohibit the Vendor from providing:
(i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(ii) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Prohibition on Unmanned Aircraft Systems (UAS)
(1) Prohibition. The Vendor is prohibited from:
(i) Delivering any FASC-prohibited unmanned aircraft system (including drones and associated elements) manufactured or assembled by American Security Drone Act—covered foreign entities (sections 1823 and 1826 of American Security Drone Act of 2023, within the NDAA for FY 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.).
(ii) On or after December 22, 2025, operating a FASC-prohibited UAS in the performance of the agreement (section 1824 of Pub. L. 118-31).
(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited UAS (section 1825 of Pub. L. 118-31).
(2) Procedures. The Vendor shall search SAM.gov for the FASC-maintained list of covered foreign entities

before proposing or using any UAS in agreement performance. Any expenditure associated with a FASC-prohibited UAS must align with an express exemption, exception, or waiver determination in the agreement.

(3) Exemptions/Waivers. The prohibitions in paragraph (c) do not apply if the agency has determined an exemption, exception, or waiver applies, and the agreement indicates such a determination (See sections 1823–1825 and 1832 of Pub. L. 118-31).

(d) Prohibition on Specific Transactions Regardless of Connection to Agreement

(1) Telecommunications & Video Surveillance: Unless waived, the Vendor cannot use equipment, systems, or services utilizing covered telecommunications as a substantial/essential component or critical technology (paragraph (a)(1)(B) of section 889, Pub. L. 115-232). This prohibition applies regardless of whether the use is in performance of a Federal agreement. It does not prohibit third-party connecting services or non-routing/non-visible telecommunications equipment.

(2) OFAC Restrictions: Except as authorized by the Office of Foreign Assets Control (OFAC), the Vendor shall not acquire supplies/services for this agreement if OFAC statutes, executive orders, or regulations (31 CFR chapter V) would prohibit such a transaction. Most transactions involving Cuba, Iran, and Sudan, and imports from Burma or North Korea, are prohibited. See OFAC's Specially Designated Nationals List and the Consolidated Screening List.

(3) Sudan: The Vendor is prohibited from conducting restricted business operations in Sudan (Accountability and Divestment Act of 2007, Pub. L. 110-174).

(4) Iran Prohibitions: Unless an exception or waiver applies, the Vendor is prohibited from:

(i) Engaging in certain activities/transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(ii) Exporting certain sensitive technology to Iran (22 U.S.C. 8515).

(iii) Note: Prohibitions (i) and (ii) do not apply if the acquisition involves designated country end products under trade agreements.

(iv) Knowingly engaging in significant transactions (over $15,000) with Iran's Revolutionary Guard Corps or affiliates (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) Governmentwide Exclusion and Removal Orders

Unless waived, the Vendor shall not provide or use any covered article, product, or service if the source or article is prohibited by an applicable FASCSA order (DoW FASCSA orders for DoW agreements; DHS orders for others). The Vendor must search SAM.gov for "FASCSA order" to locate applicable restrictions. Orders issued post-solicitation apply only if added via agreement modification.

(f) Reasonable Inquiry

The Vendor shall conduct a reasonable inquiry (reviewing possessed information, without requiring an internal or third-party audit) to determine if there are any prohibited products or services.

(g) Removal of Prohibited Products and Services

Upon notification from the Agreements Officer during agreement performance, the Vendor shall promptly make necessary modifications to remove any product or service that this article prohibits.

(h) General Reporting Requirements

(1) If the Vendor discovers that any provided or used product/service does not comply with any prohibition in this article, it must report the following to the Agreements Officer (or via https://dibnet.dod.mil for DoW agreements) within 72 hours:

- Agreement and order number;
- The specific prohibition violated;

- Description of the prohibited item (brand, model, OEM, part number);
- Producer details (entity name, CAGE code, manufacturer/distributor codes);
- Impact of the item's functionality on risk;
- Justification for any requested waiver/exception;
- Availability of compliant alternatives;
- Details of maintained items (if applicable) and mitigation actions.

(2) If new information is discovered later, subsequent reports must be submitted within 72 hours.

(i) New FASCSA Orders Report

(1) The Vendor shall review SAM.gov at least every three months to check for new FASCSA orders.

(2) If a new order impacts the supply chain, the Vendor must conduct a reasonable inquiry to determine if a newly prohibited article was provided or used during agreement performance.

(3) The Vendor must report identified violations to the Agreements Officer within 72 hours, including agreement number, order details, and item/source specifics as outlined in paragraph (h)(1).

Subcontracts

The Vendor shall insert the substance of this article, including this paragraph, in all subcontracts.

Definitions:

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Covered article, as defined in 41 U.S.C. 4713(k), means:

(1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;

(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or

(4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

Covered foreign country means The People’s Republic of China.

Covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies Vendor or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Vendor, or Dahua Technology Vendor (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.

FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):

(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.

(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD), also referenced as the Department of War (DoW) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoW FASCSA order.

(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a Vendor under a contract or transaction with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor/vendor incidental to a Federal contract or transaction.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;

(9) The Bureau of Intelligence and Research of the Department of State;

(10) The Office of Intelligence and Analysis of the Department of the Treasury;

(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

(12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connecting a customer of telephone provider A to a customer of telephone Vendor B) or sharing data and other information resources.

Kaspersky Lab-covered article means any hardware, software, or service that—

(1) Is developed or provided by a Kaspersky Lab-covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab-covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab-covered entity.

Kaspersky Lab-covered entity means—

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor/vendor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or

intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).

Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).

Article XIV: Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies:

(a) Prohibition. In accordance with Section 1211 of the National Defense Authorization Act for Fiscal Year 2006 (Pub. L. 109-163), Section 1243 of the NDAA for FY 2012 (Pub. L. 112-81), and Section 1296 of the NDAA for FY 2017 (Pub. L. 114-328), the Vendor shall not acquire or utilize any items covered by the USML from any Communist Chinese military Vendor in the performance of this Agreement.

(b) Lower Tier Agreements. The Vendor shall insert the substance of this article, including this paragraph (b), in all subcontracts or lower-tier agreements that involve the delivery or procurement of items covered by the USML.

Article XV: Export Control

Vendors or awardee(s) and their subcontractors shall comply with U.S. Export regulations including, but not limited to, the requirements of the Arms Export Control Act, 22 U.S.C. § § 2751-2794, including the International Traffic in Arms Regulation (ITAR), 22 C.F.R. § 120 et seq.; and the Export Administration Act, 50. U.S.C. app. §2401-2420. Each party is responsible for obtaining from the Government export licenses or other authorizations/approvals, if required, for information or materials provided from one party to

another under this Agreement. Accordingly, vendors or awardees and their subcontractors 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.

Article XVI: Non-Government Advisors

Non-Government advisors may participate, as non-scoring members, in the evaluation of all Spirals and shall have signed a non-disclosure agreement (NDA) with the Government. Non-government advisors may also serve in administrative & assistance support capacities. If non-Government advisor(s) are used, offerors will be notified of the name and corporate affiliation of these advisors. Offerors will be afforded the opportunity to enter into a specific NDA with the corporate entity prior to submission of their solution brief, spiral, or proposal. The Government understands that information provided in response to this CSO is presented in confidence and may contain trade secrets or commercial or financial information, and it agrees to protect such information from unauthorized disclosure to the maximum extent permitted or required by Law, to include:

➔ 18 U.S.C. 1905 (Trade Secrets Act);
➔ 18 U.S.C. 1831 et seq. (Economic Espionage Act);
➔ 5 U.S.C. 552(b)(4) (Freedom of Information Act);
➔ Executive Order 12600 (Pre-disclosure Notification Procedures for Confidential Commercial Information); and,
➔ Any other statute, regulation, or requirement applicable to Government employees

Article XVII: Security Requirements

1. General Agreement Level

The overall security level for this Agreement is UNCLASSIFIED. However, work performed under this Agreement and subsequent Spirals may involve access to Controlled Unclassified Information (CUI) as well as information classified as CONFIDENTIAL, SECRET, or TOP SECRET.

2. Classified Information

To the extent that work performed involves classified information, the Vendor shall comply with the National Industrial Security Program Operating Manual (NISPOM) as outlined in Part 117 of Title 32, Code of Federal Regulations (formerly DoD 5220.22-M), and DD Form 441. The Government will provide a Security Classification Specification (DD Form 254) for the overarching Agreement and/or each individual Spiral as required.

3. Controlled Unclassified Information (CUI)

If the work involves DoD Controlled Unclassified Information (CUI), the Vendor shall ensure all information is safeguarded and handled in accordance with DoDI 5200.48, Controlled Unclassified Information. Furthermore, the Vendor shall comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, to ensure adequate safeguarding of the Vendor's unclassified internal information systems that process, store, or transmit CUI.

Article XVIII: FOIA Exemption

In accordance with 10 U.S.C. 4021 information submitted during the award process (competitive or noncompetitive) is exempt from FOIA for 5 years from receipt.

Article XIX: Foreign Entities

Foreign participation at the prime level is prohibited. Subcontracting arrangements will be handled in accordance with the International Traffic and Arms Regulation. In addition, foreign national participation will be limited to public domain information only.

Foreign disclosure reviews shall be performed before the release of information to the public on all acquisitions requiring disclosure of classified or export-controlled unclassified, including sensitive unclassified information.

Article XX: Weapons Open System Architecture (WOSA)

WOSA Technical Specification – The WOSA Reference Architecture (Attachment 1) defines all functions of a weapon system into a series of hardware and software domains. For each of these domains, conformance to the WOSA technical specification requires the use of the WOSA domain specific interface message structures and formats. Industry partners are encouraged to request changes to the WOSA technical specification if the current baseline is not able to provide the functionality required for contemplated designs to meet system performance requirements. Within each weapon system, the WOSA messaging design specifies the rate of message transmission from each domain, and the Munition Data Bus defines the transmission paths of messages to all other recipient domains. There is flexibility in the specification to allow for variations of design approaches to meet requirements. The WOSA technical specification itself does not require the use of any hardware or other standard interfaces for the transmission of WOSA messages.

Article XXI: Domain Integration Packages

Domain Integration Packages – Weapon Open Systems Architecture (WOSA) Domain interface data items are deemed Form, Fit, Function technical data that describes the required overall physical, functional, and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items, which shall be delivered with Unlimited Data Rights.

Article XXII: WOSA X

WOSA X – Once a weapon has established the initial design for WOSA domains, the Domain Integration Package will be used to determine the WOSA X integration and interface attributes for key aspects of each domain for a given weapon system. The intent of this evolution from WOSA to WOSA X is to document the interface requirements, accelerate the integration of future hardware within a given WOSA compliant weapon system design from the supply chain of key hardware and software, and to facilitate potential cross-weapon use of key hardware and software domains.

Article XXIII: Weapons GRA

Weapons GRA – Developed by the Digital Acquisition and Sustainment Office (DASO) as a series of Systems Markup Language (SysML) models. The Weapons GRA Government Issued Framework (GIF) contains tailored program office and program information, the Statement of Objectives (SOO), the System Requirements Document (SRD), System Performance Specification (SPS), Contract Data Requirements List (CDRL), WOSA Technical Specification, Universal Armament Interface (UAI) Interface Control Document (ICD), the Common Flexible Weapons ICD (CFWICD), as well as other general reference data. The Weapons GRA also contains the Information Hub (iHUB), which has a series of functional landing pages for Industry to insert artifacts or links to artifacts which fulfill requirements of systems engineering processes, certification requirements, authorization requirements, and flight clearance requirements. The Government and Industry will evaluate when to update program implementation models to new releases of the Weapons GRA based on the DASO Weapons GRA release notes and content of additional capabilities. Weapons GRA Quick Start Guide (Attachment 2); use of Weapons GRA is a requirement of this CSO.

Article XXIV: Non-Traditional Vendors

Vendors receiving prototype OT project awards under this ADRR agreement will be required to share the cost/contribute one-third of the cost of the OTA project award unless one of the following applies:

(a) Awardee is a non-traditional defense contractor/vendor, small business, or a team consisting entirely of small businesses and non-traditional defense contractors/vendors.
(b) Team receiving the award, which may include traditional defense contractors/vendors, includes at least one non-traditional defense contractor/vendor, who will contribute significantly to the prototype OT project objectives.
(c) Significant participation includes, but not limited to:
    1. The participation causes a material reduction in the cost or schedule
    2. The participation causes an increase in the performance of prototype
    3. The Vendor is responsible for a new key component, technology, or process on the critical path
    4. The Vendor is accomplishing a significant amount of the effort

Article XXV: Government Furnished Property

The Government will provide [INSERT VENDOR NAME], with the Government Furnished Property (GFP) listed in the [SOO/SOW/PWS/etc.] and referenced in the GFP Property List that may be incorporated as an attachment to this Agreement to facilitate the performance of this OTA.

[INSERT VENDOR NAME] shall assume the risk of and be responsible for any loss or destruction of, or damage to, the GFP while it is in [INSERT VENDOR NAME'S] possession or control. The Government may, at its option, furnish property in an "as-is" condition. The vendor will be given the opportunity to inspect such property prior to the property being provided. In such cases, the Government makes no warranty with respect to the serviceability and/or suitability of the property for agreement performance. Any repairs, replacement, and/or refurbishment shall be at the vendor's expense. The GFP shall be returned at the end of the OTA period of performance in a condition that is as good as when it was received, or in accordance with the provisions of the OTA regarding its use. [INSERT VENDOR NAME] shall obtain explicit written authorization for any transfer

or disposition of the GFP.

(a) Definitions.

Government Furnished Property (GFP): is any property in the possession of, or directly acquired by, the Government and subsequently furnished to the vendor under this award. GFP includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul or modification.

The vendor's accountability extends from the initial acquisition and receipt of property, through stewardship, custody, and use until formally relieved of responsibility by authorized means, including delivery, consumption, expending, sale (as surplus property), or other disposition, or via a completed investigation, evaluation, and final determination for lost property. This requirement applies to all government property under the vendor's accountability, stewardship, possession or control, including its vendors or subcontractors.

As is: means that the Government makes no warranty with respect to the serviceability and/or suitability of the Government property for agreement performance and that the Government will not pay for any repairs, replacement, and/or refurbishment of the property.

(b) Government Furnished Property Transfer and Acceptance

Upon agreement award, the vendor shall gain access to and utilize the GFP Transfer Module within Procurement Integrated Enterprise Environment (PIEE) to accomplish an inventory and reconciliation of GFP. Discrepancies noted by the vendor shall be documented within the PIEE GFP Transfer Module. The vendor shall notify the Government of any discrepancies and annotate the discrepancies within the PIEE GFP Transfer Module. The Government will work with the vendor to resolve discrepancies noted during inventory. Once the inventory and reconciliation of GFP is complete, the Government will sign a DD1149 confirming the vendor received the equipment. This document is used so GFP can be moved from the Government's Unit Identification Code (UIC) to the vendor Storage Location (SLOC). The vendor documents acceptance of the property by using the GFP module of PIEE at https://piee.eb.mil/piee-landing/.

(c) Government Furnished Property Shipping

The vendor shall be responsible for the shipment of GFP. The vendor shall ship GFP from vendor facilities to and between various locations as necessary to support the execution of this agreement. Movement of all GFP shall be made via one of the following forms: Internal vendor shipping document, DD1149, DD1348, DD250, or a commercial shipping/tracking document. Signed shipping documentation shall be provided to the Agreement Officer's Representative (AOR).

(d) Government Furnished Property Maintenance

Scheduled Preventative Maintenance Checks and Services (PMCS) of GFP shall be the vendor's responsibility; however, unscheduled services will be completed using Contractor Logistics Support (CLS) provided by the Government. In the event unscheduled services are required, the vendor shall notify the Government AOR within 24 hours of discovery.

(e) Government Furnished Property Disposition

At award, completion, or termination the vendor shall account for all property furnished under this award. The vendor shall report GFP that is no longer required to perform a contract using the PIEE Plant Clearance Module. The Government will direct the vendor to prepare and ship the excess GFP. The vendor shall ensure GFP is restored to the condition it was received prior to returning GFP to the Government.

(f) Government Furnished Property Restrictions

GFP issued under this agreement shall only be utilized by the vendor in support of this agreement. Any other use is strictly prohibited.

Article XXVI: Tariffs

(a) Authority and scope. In accordance with 19 U.S. Code § 1321 - Administrative exemptions and 10 U.S. Code § 4864 - Authority to acquire property this article outlines the procedures for obtaining duty-free entry into the United States (US) for certain supplies acquired by the vendor for delivery to the US Government under this agreement.

(b) Definitions.

1. Component: Any item furnished to the Government as part of an end product or another component.
2. Customs Territory of the United States: The 50 States, the District of Columbia, and Puerto Rico.
3. Eligible Supplies: Supplies that are eligible for duty-free entry under 19 U.S.C. § 1321(a)(2) when imported for the U.S. Government. This generally includes:
    a. End items specifically designated under this agreement for duty-free entry.
    b. Components (including raw materials and intermediate assemblies) incorporated into U.S.-made end products to be delivered under this agreement.
    c. Other supplies for which the vendor estimates the duty will exceed $300 per shipment.
4. Fair Retail Value (Country of Shipment): The typical price at which an item would be sold to an end consumer in the country from which it is shipped. This value is used to determine whether the aggregate value of duty-free imports falls within the limits set by the Secretary of the Treasury.

(c) Vendor Responsibilities:

1. Duty Not Included in Price: The vendor's price for this agreement shall not include any amount for duty on Eligible Supplies unless those supplies were already imported into the Customs Territory of the United States before the effective date of this agreement.
2. Exclusive Government Use: The vendor shall claim duty-free entry only for supplies that are intended for delivery to the Government under this agreement, either as end items or as components of end items.
3. Duty Payment on Diversion: The vendor shall pay all applicable duties on supplies, or

any portion thereof, diverted to non-governmental use, with the exception of supplies that are:

- Scrapped or salvaged
- Sold in a competitive sale that is directed or authorized by the Agreements Officer

(d) Government Responsibilities:

The Government will provide assistance to the vendor in obtaining duty-free entry for Eligible Supplies by executing duty-free entry certificates, provided that:

1. No duty is included in the agreement price for those supplies, as specified in paragraph (c)(1).
2. The shipping documents bear the notation specified in paragraph (e).

(e) Shipping Documentation:

For foreign supplies for which the Government will issue duty-free entry certificates under this clause, shipping documents presented to Customs must:

1. Consign the shipments to the appropriate entity as follows:
   - The relevant Military Department in care of the vendor, including the vendor's delivery address; *or*
   - The appropriate Military Installation.
2. Include the following information:
   - Prime agreement number.
   - Identification of the carrier.
   - The applicable notation, based on the final consignee, as follows:
     - For Shipments to Military Installations: "UNITED STATES GOVERNMENT, DEPARTMENT OF DEFENSE Duty-Free Entry to be claimed pursuant to 19 U.S.C. § 1321(a)(2) and Section XXII, Chapter 98, Subchapter VIII, Item 9808.00.30 of the Harmonized Tariff Schedule of the United States. Upon arrival of shipment at the appropriate port of entry, District Director of Customs, please release shipment under 19 CFR Part 142 and notify [Designated Government Authority, e.g., DCMA] for execution of required forms."
     - For Shipments to Vendor: "UNITED STATES GOVERNMENT, DEPARTMENT OF DEFENSE Duty-Free Entry to be claimed pursuant to 19 U.S.C. § 1321(a)(2) and Section XXII, Chapter 98, Subchapter VIII, Item 9808.00.30 of the Harmonized Tariff Schedule of the United States. Upon arrival of shipment at the appropriate port of entry, District Director of Customs, please release shipment under 19 CFR Part 142 and notify [Designated Government Authority, e.g., DCMA] for execution of required forms."

- Gross weight in pounds (and cubic feet, if applicable).
- Estimated value in U.S. dollars.
- The activity address number of the agreement administration office.

(f) Customs Forms:

1. The vendor shall prepare all necessary customs forms for the entry of foreign supplies into the Customs Territory of the United States (except for shipments consigned directly to a military installation). The vendor will then submit these forms to the District Director of Customs and provide a copy to the Designated Government Authority for the execution of any required duty-free entry certificates.
2. For shipments containing both supplies that are eligible for duty-free entry and supplies that are not, the vendor must clearly identify the duty-free items on the customs forms.

(g) Other Shipping Requirements:

1. The vendor (or the foreign supplier, if the vendor is foreign) must prepare sufficient copies of the bill of lading (or other shipping document) to ensure that at least two copies accompany the shipment for use by the District Director of Customs.
2. The shipment must be consigned as specified in paragraph (e).
3. The exterior of all packages must be marked with:
   - "UNITED STATES GOVERNMENT, DEPARTMENT OF DEFENSE"
   - The activity address number of the agreement administration office.

(h) Notification to Administrative Agreements Officer (ACO):

The vendor shall notify the ACO in writing of any purchase of Eligible Supplies that are to be imported into the Customs Territory of the United States for delivery to the Government or for incorporation into end items. The notice must be provided immediately upon award to the supplier and must include the following information:

1. Vendor’s name, address, and CAGE code
2. Prime agreement number
3. Total dollar value of the agreement
4. Date of the last scheduled delivery under the agreement
5. Foreign supplier's name and address
6. List of items purchased
7. Agreement that the vendor will pay duty on supplies diverted to non-governmental use (except for scrap/salvage or authorized competitive sales)
8. Country of origin

9. Scheduled delivery date(s)

(i) Exceptions:

This article does not apply if:

1. The supplies are identical to supplies the vendor purchases for their commercial business; *and*

2. It is not economical or feasible to track the supplies separately to ensure that the duty-free amount does not exceed the amount purchased specifically for this agreement.

(j) Compliance with CBP Regulations:

All activities undertaken pursuant to this clause shall be conducted in full compliance with the regulations and guidelines issued by U.S. Customs and Border Protection (CBP) related to 19 U.S.C. § 1321. The vendor is responsible for staying informed about and adhering to all applicable CBP regulations.

Article XXVII: Common Access Cards (CACs) for Vendor Personnel

(a) Authority. 32 CFR 156.6, DoD Manual 1000.13 Volume 1

(b) Applicability. Vendors shall ensure Common Access Cards (CACs) are obtained by all personnel who meet one or both of the following criteria:

1. Require logical access to Department of Defense computer networks and systems in either:
   A. the unclassified environment; or
   B. the classified environment where authorized by governing security directives.

2. Perform work, which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

(c) Process of Obtaining CACs.

1. Vendors shall provide a listing of personnel who require a CAC to the Contracting Officer. The government will provide the vendor with instruction on how to complete the vendor Verification System (CVS) application and then notify the vendor when approved.

2. Vendor personnel shall obtain a CAC from the nearest Real Time Automated Personnel Identification Documentation System (RAPIDS) Issuing Facility (typically the local Military Personnel Flight (MPF)).

(d) Other Requirements.

1. While visiting or performing work on installation(s)/location(s), vendor personnel shall wear or prominently display the CAC as required by the governing local policy.

2. Within seven (7) working days of any changes to the listing of personnel authorized a CAC, provide an updated listing to the Contracting Officer who will provide the updated listing to the authorizing government official.

3. Return CACs in accordance with local policy/directives within seven (7) working days of a change in status for vendor personnel who no longer require logical or physical access.

4. Return CACs in accordance with local policy/directives within seven (7) working days following a CACs expiration date.

5. Report lost or stolen CACs in accordance with local policy/directives.

6. Within seven (7) working days following completion/termination of the agreement, the vendor shall return all CACs issued to their personnel to the issuing office or the location specified by local policy/directives.

7. Failure to comply with these requirements may result in the withholding of final payment.

Article XXVIII: Modifications

(1) As a result of meetings, annual reviews, or at any time during the term of the Agreement, progress or results may indicate that a change in the SOO and/or the Schedule of Milestones and Payments, would be beneficial to program objectives. Recommendations for modifications, including justifications to support any changes to the SOO and/or the Schedule of Milestones and Payments, will be documented in writing and submitted by the Vendor to the AOR with a copy to the AO. This documentation will detail the technical, chronological, and financial impact of the proposed modification to the research program. The Government is not obligated to pay for additional or revised milestones until the Schedule of Milestones and Payments is formally revised by the AO and made part of this Agreement.

(2) For minor or administrative Agreement modifications (e.g. changes in the paying office or appropriation data, changes to Government or the Vendor's personnel identified in the Agreement, etc.) no signature is required by the Vendor.

(3) The AO will be responsible for executing all modifications to this Agreement.

(4) (a) The Agreements Officer may at any time, by written order, and without notice to the sureties, if any, make changes within the general scope of this contract in any one or more of the following:

1. Drawings, designs, or specifications when the supplies to be furnished are to be specially manufactured for the Government in accordance with the drawings, designs, or specifications.
2. Method of shipment or packing.
3. Place of delivery.

(b) If any such change causes an increase or decrease in the estimated cost of, or the time required for, performance of any part of the work under this agreement, whether or not changed by the order, or otherwise affects any other terms and conditions of this agreement, the Agreements
Officer shall make an equitable adjustment in the-

1. Estimated cost, delivery or completion schedule, or both;
2. Amount of any fixed fee; and
3. Other affected terms and shall modify the contract accordingly.

(c) The vendor must assert its right to an adjustment under this clause within 30 days from the date of receipt of the written order. However, if the Agreements Officer decides that the facts justify it, the Agreements Officer may receive and act upon a proposal submitted before

final payment of the agreement.

(d) Failure to agree to any adjustment shall be a dispute under the Disputes article. However, nothing in this article shall excuse the vendor from proceeding with the agreement as changed.

Article XXIX: Preventing Conflicts of Interest

The vendor shall—

(1) Have procedures in place to screen covered employees for potential personal conflicts of interest, by-

(i) Obtaining and maintaining from each covered employee, when the employee is initially assigned to the task under the agreement, a disclosure of interests that might be affected by the task to which the employee has been assigned, as follows:

(A) Financial interests of the covered employee, of close family members, or of other members of the covered employee's household.
(B) Other employment or financial relationships of the covered employee (including seeking or negotiating for prospective employment or business).
(C) Gifts, including travel; and

(ii) Requiring each covered employee to update the disclosure statement whenever the employee's personal or financial circumstances change in such a way that a new personal conflict of interest might occur because of the task the covered employee is performing.

(2) For each covered employee—

(i) Prevent personal conflicts of interest, including not assigning or allowing a covered employee to perform any task under the agreement for which the vendor has identified a personal conflict of interest for the employee that the vendor or employee cannot satisfactorily prevent or mitigate in consultation with the contracting agency;

(ii) Prohibit use of non-public information accessed through performance of a Government agreement for personal gain; and

(iii) Obtain a signed non-disclosure agreement to prohibit disclosure of non-public information accessed through performance of a Government agreement.

(3) Inform covered employees of their obligation-

(i) To disclose and prevent personal conflicts of interest;

(ii) Not to use non-public information accessed through performance of a Government agreement for personal gain; and

(iii) To avoid even the appearance of personal conflicts of interest;

(4) Maintain effective oversight to verify compliance with personal conflict-of-interest safeguards;

(5) Take appropriate disciplinary action in the case of covered employees who fail to comply with policies established pursuant to this Article; and

(6) Report to the Agreements Officer any personal conflict-of-interest violation by a covered employee as soon as it is identified. This report shall include a description of the violation and the proposed actions to be taken by the vendor in response to the violation. Provide follow-up reports

of corrective actions taken, as necessary. Personal conflict-of-interest violations include-

(i) Failure by a covered employee to disclose a personal conflict of interest;

(ii) Use by a covered employee of non-public information accessed through performance of a Government agreement for personal gain; and

(iii) Failure of a covered employee to comply with the terms of a non-disclosure agreement.

(a) Mitigation or waiver.

(1) In exceptional circumstances, if the vendor cannot satisfactorily prevent a personal conflict of interest as required by paragraph (2)(i) of this Article, the vendor may submit a request through the Agreements Officer to the Head of the Contracting Activity for-

(i) Agreement to a plan to mitigate the personal conflict of interest; or

(ii) A waiver of the requirement.

(2) The vendor shall include in the request any proposed mitigation of the personal conflict of interest.

(3) The vendor shall-

(i) Comply, and require compliance by the covered employee, with any conditions imposed by the Government as necessary to mitigate the personal conflict of interest; or

(ii) Remove the vendor employee or subcontractor employee from performance of the agreement or terminate the applicable subcontract.

(b) *Subcontracts*. The vendor shall include the substance of this Article, including this paragraph (d), in subcontracts—

(1) That exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award; and

(2) In which subcontractor employees will perform acquisition functions closely associated with inherently governmental functions (*i.e.*, instead of performance only by a self-employed individual).

Article XXX: Delegation of Transportation Authority to DCMA

(a) Authority and Scope. The Agreements Officer hereby delegates to the Defense Contract Management Agency (DCMA) the authority to oversee, coordinate, and authorize transportation services related to the performance of this agreement.

(b) Specific Delegated Powers. DCMA is authorized to:

(1) Approve transportation methods, carriers, and routing for agreement deliverables;

(2) Utilize Transportation Account Code (TAC) provided by [INSERT GOVERNMENT OFFICE];

(3) Coordinate with the United States Transportation Command (USTRANSCOM) and commercial carriers;

(4) Apply transportation security services, as necessary;

(5) Resolve transportation-related disputes between the vendor and transportation providers IAW Defense Transportation Regulation 4500.9-R.

(c) Vendor Requirements for Coordination.

(1) Vendor shall contact DCMA Transportation on ALL "DCMA Administered" agreements prior to shipment and after material acceptance for shipping instructions using the DCMA Shipment Instruction Request (SIR) eTool System at Access to eTools SIR is projected to transition to the Procurement Integrated Enterprise Environment (PIEE) in CY26 at which time vendors will be required to request shipping instructions via that module, when the system goes live.

(2) for ALL FOB: Origin, Foreign Military Sales (FMS), and FOB: Destination OCONUS/Export movements to obtain the appropriate DOD regulatory clearances, shipping documentation and instructions from cognizant DCMA Transportation Office. If vendor is new to DCMA, and does not already have a SIR eTool account, request an account via DCMA External Web Access Management (EWAM) application which can be accessed at Access to eTools. If vendor needs additional assistance, email DCMA Transportation Group at: dcma.stlouis-mo.hq.mbx.transportation-inbox@mail.mil.

(3) Do not move any freight to a water or aerial port prior to coordinating with DCMA. Failure to contact DCMA may result in additional expenditures borne by the vendor.

(4) The vendor shall provide a completed DD Form 1149 for each shipment prior to DCMA notification. The DD Form 1149 will be included with each shipment. The DD Form 1149 will be finalized and signed by the authorized USG representative upon vendor notification of assets available for shipment from vendor designated integration location, [INSERT VENDOR ADDRESS], [INSERT VENDOR NAME].

(5) The vendor shall provide the following FMS information via SIR submission (in addition to USG signed DD Form 1149 and normally required shipping data) for each shipping request:

- FMS/BPC case ID
- MILSTRIP(s)
- Quantity (pieces, weight, and dims)
- Supplemental Address
- Ship-To/Mark For
- Transportation Account Code (TAC):

Article XXXI: Delegation of Inspect & Accept Authority to DCMA

(a) Authority and Scope. The Agreements Officer hereby delegates to the Defense Contract Management Agency (DCMA) the authority to inspect and accept all supplies furnished under the agreement.

(b) Specific Delegated Powers. DCMA is authorized to:

(1) Inspect and test all supplies called for by the agreement, to the extent practicable, at all places and times, including the period of manufacture, and in any event before acceptance;

inspections and test shall be performed in a manner that will not unduly delay work. Specific locations for inspection and acceptance shall be identified in the agreement.

(2) Either to reject or to require correction of nonconforming supplies. Supplies are nonconforming when they are defective in material or workmanship or are otherwise not in conformity with agreement requirements. The Government may reject nonconforming supplies with or without disposition instructions.

(3) Permit correction in place, promptly after notice, and at the expense of the vendor.

(4) Accept supplies furnished under this agreement via DD250 which shall be submitted through the WAWF system.

(5) Provide advance notice to the vendor to coordinate inspection/acceptance.

Article XXXII: NIST SP 800-171 DoD Assessment Requirements

A. Background
To ensure Vendors are adequately protecting Covered Defense Information (CDI) and Controlled Unclassified Information (CUI), the Department of Defense (DoD) requires verification of a Vendor's implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev. 2. This Article outlines the requirement for the Vendor to maintain a current NIST SP 800-171 DoD Assessment and post the resulting score in the Supplier Performance Risk System (SPRS).

B. Definitions

- "Basic Assessment" means a Vendor's self-assessment of the Vendor's implementation of NIST SP 800-171 Rev. 2 that results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

- "Medium Assessment" means an assessment conducted by the Government that results in a confidence level of "Medium" in the resulting score, based on a review of the Vendor's Basic Assessment, System Security Plan (SSP), and a thorough document review.

- "High Assessment" means an assessment conducted by the Government that results in a confidence level of "High" in the resulting score, based on a review of the Vendor's Basic Assessment, SSP, a thorough document review, and verification, examination, and demonstration of a Vendor's system security plan to validate that NIST SP 800-171 Rev. 2 security requirements have been implemented.

- "SPRS" means the Supplier Performance Risk System, the DoD enterprise application used to retrieve and store vendor assessment scores.

C. SPRS Assessment Requirement

1. The Vendor shall ensure that a current NIST SP 800-171 DoD Assessment (i.e., not more than three years old unless a lesser time is specified in the Agreement) for each covered Vendor information system that is relevant to this Agreement has been posted to SPRS.

2. The Vendor shall maintain this assessment within SPRS throughout the period of performance of this Agreement.

3. If the Vendor has conducted a Basic Assessment, but the score is not currently posted in SPRS, the Vendor shall submit the assessment score and the following required summary level data via

encrypted email to webptsmh@navy.mil:

- System Security Plan (SSP) name and version.
- System Architecture identifier (e.g., CAGE code or MAC address).
- Date of the assessment.
- Summary level score (e.g., 95 out of 110).
- Date that all requirements are expected to be implemented (if the score is less than 110).

D. DoD-Conducted Assessments

1. Access: The Government may choose to conduct a Medium or High Assessment of the Vendor's covered information systems. If the Government elects to conduct such an assessment, the Vendor shall provide the Government (including DoD assessors) access to its facilities, systems, and personnel necessary to conduct the assessment.

2. Rebuttals: The Government will provide the Vendor with the results of a Medium or High Assessment. The Vendor will have 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the Government assessment team. The Government will review any provided information and update the SPRS score accordingly.

E. Lower Tier Agreements (Flow-Down)
The Vendor shall include the substance of this Article in all subcontracts and lower-tier agreements, regardless of tier, that involve the processing, storing, or transmitting of CUI.

1. The Vendor shall not award a lower-tier agreement or subcontract until the Vendor has verified that the lower-tier Vendor has a current (not more than 3 years old) NIST SP 800-171 DoD Assessment score posted in SPRS for all relevant covered information systems.

2. The Vendor shall ensure that the lower-tier Vendor maintains their assessment score in SPRS for the duration of the lower-tier agreement.

<u>Article XXXIII: Supply Chain Risk Management and National Security Systems</u>

A. Scope and Applicability
This Article applies to all hardware, software, components, and services procured for or utilized in the performance of this Agreement where such performance involves National Security Systems (NSS) as defined at 44 U.S.C. § 3552(b) (and referenced in 10 U.S.C. § 3252).

B. Access to Restricted Supplier Information
The Vendor acknowledges that the National Security System (NSS) Restricted List is Controlled Unclassified Information (CUI). Access to this list is restricted to authorized personnel and is maintained within the Supplier Performance Risk System (SPRS) via the Procurement Integrated Enterprise Environment (PIEE).

C. Vendor Responsibility
Credentials: The Vendor is responsible for obtaining and maintaining the necessary PIEE credentials and SPRS access roles required to view the NSS Restricted List.

Safeguarding: The Vendor shall safeguard the NSS Restricted List in accordance with the CUI handling requirements established in Article VIII (Cybersecurity) and Article XIX (Security Requirements) of this Agreement.

Exclusion: The Vendor shall not procure or utilize any components, software, or services from suppliers listed on the NSS Restricted List for work involving National Security Systems. The Vendor shall verify compliance via SPRS (https://www.sprs.csd.disa.mil/) prior to procurement.

D. Lower Tier Flow-Down
The Vendor shall flow down the requirements of this Article to all subcontractors and suppliers at all tiers. If a subcontractor does not have access to SPRS, the Vendor is responsible for conducting the restricted list check on the subcontractor's behalf to ensure compliance with this Agreement.

Article XXXIV: Prohibition Regarding Russian Fossil Fuel and Fossil Fuel Business Operations

A. Definitions
For the purposes of this Article:

"Fossil fuel" means coal, petroleum, natural gas, or any derivative of coal, petroleum, or natural gas that is used for fuel.

"Fossil fuel business operations" means the extraction, recovery, refining, manufacturing, or transporting of fossil fuels.

B. Representation
By signing this Agreement, the Vendor represents that it does not have any fossil fuel business operations with the Government of the Russian Federation or the energy sector of the Russian Federation.

C. Prohibition
In accordance with Section 804 of the National Defense Authorization Act (NDAA) for Fiscal Year 2024 (Pub. L. 118-31) and related Department of Defense policy, the Vendor shall not provide to the Government any fossil fuel that was extracted, recovered, refined, manufactured, or transported by the Russian Federation or the energy sector of the Russian Federation. Furthermore, the Vendor shall not procure any such restricted fossil fuels in the performance of this Agreement.

D. Lower Tier Flow-Down
The Vendor shall include the substance of this Article, including this flow-down requirement, in all subcontracts or lower-tier agreements, regardless of tier, that involve the procurement or delivery of fossil fuels.

Article XXXV: Accounting System Requirements

(a) Applicability: This article applies only to Spirals or projects awarded under this Agreement that are structured as expenditure-based or require a Vendor resource share.

(b) Standard of Accounting: The Vendor shall maintain an accounting system capable of complying with Generally Accepted Accounting Principles (GAAP).

(c) Internal Controls: The Vendor's system must feature effective internal controls to ensure complete, accurate, and current records of all project funds. Specifically, the Vendor's system shall:

1. Maintain effective internal controls over all project funds, including Federal funds and any required Vendor resource share;

2. Maintain complete, accurate, and current records that document the sources of funds and the purposes for which they are disbursed; and

3. Ensure that Government and cost-share funds are used only for purposes permitted by the terms of this Agreement.

(d) Consistency and Commercial Practices: If the Vendor currently performs under other expenditure-based Federal awards, the Vendor shall apply those same approved financial management standards to this Agreement. However, provided the Vendor meets the baseline GAAP and internal control requirements stated herein, the Government will not require the Vendor to fundamentally revise or alter its existing commercial accounting system.

Article XXXVI: Nondiscrimination and Addressing DEI Discrimination

(a) Prohibition on Racially Discriminatory DEI Activities.
The Vendor agrees that it shall not engage in any racially discriminatory Diversity, Equity, and Inclusion (DEI) activities in connection with the performance of this Agreement. For the purposes of this Article, this means the Vendor shall not engage in disparate treatment based on race or ethnicity in recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or the allocation or deployment of the Vendor's resources. "Program participation" includes membership or participation in, or access or admission to, training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities sponsored or established by the Vendor.

(b) Materiality of Compliance.
The Vendor acknowledges and agrees that compliance with applicable anti-discrimination laws and the specific prohibitions contained in this Article is material to the Government's payment decisions under this Agreement.

(c) Information, Reports, and Access.
The Vendor shall furnish all information and reports, and provide the Government (including the Agreements Officer or authorized designees) access to books, records, and accounts, as required by the Agreements Officer for the sole purpose of ascertaining compliance with this Article.

(d) Subcontractor Oversight and Notification.
To ensure compliance throughout the supply chain, the Vendor shall:

1. Report to the Agreements Officer any subcontractor's known or reasonably knowable conduct that may violate the prohibitions in this Article;
2. Take any appropriate remedial actions regarding non-compliant subcontractors as directed by the Agreements Officer; and
3. Promptly inform the Agreements Officer if a subcontractor files a lawsuit against the Vendor that puts the validity or enforcement of this Article at issue in any way.

(e) Remedies for Noncompliance.
In the event of the Vendor's or a subcontractor's noncompliance with this Article, this Agreement may be canceled, terminated, or suspended in whole or in part, and the Vendor or subcontractor may be declared ineligible for further Government agreements or contracts.

(f) Lower Tier Agreements.
The Vendor shall insert the substance of this Article, including this paragraph (f), in all subcontracts or lower-tier agreements, regardless of tier, for work performed in support of this Agreement.

SECTION VI: ATTACHMENTS

Attachment 1 – (CUI) WOSA Reference Architecture
Attachment 2 – Weapons GRA Quick Start Guide
Attachment 3 – Milestones & Payment
Attachment 4 – Property & Equipment

SECTION VII: CSO CONTACT INFORMATION

CSO Administrative Contracting/Agreements Officer:

AFLCMC/EBIW Contracting at aflcmc.ebiw.contracting@us.af.mil