Appendix G – Prime Contract Flowdowns – CDP2

(W900KK-23-9-0001/2024-495)

U.S. Government Contract Regulations. This Agreement, is being issued in support of a U.S. Government project through an Other Transaction Authority ("OTA"). The Prime Contract is an Agreement between Advanced Technology International (ATI), hereinafter referred to as the "Consortium Management Firm" or the "CMF", and Bigelow Family Holdings, LLC, dba Mettle Ops, hereinafter referred to as "Buyer", and this Subcontract from Buyer to Party identified on the Purchase Order, hereinafter referred to as "Subcontractor". The clauses below are incorporated herein with the same force and effect as if they were set forth in full text in the Subcontract.

ARTICLE I: NOT FLOWED DOWN

ARTICLE II: TERM

A. The Term of this Agreement

The Agreement is effective upon the Effective Date, which is the date of Purchase Order. The term of the project will be as stated in each individual Purchase Order.

ARTICLE III: NOT FLOWED DOWN

ARTICLE IV: NOT FLOWED DOWN

ARTICLE V: NOT FLOWED DOWN

ARTICLE VI: DISPUTES & TERMINATIONS

A. General.

The Buyer, and Subcontractor (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.

Any disagreement, claim, or dispute between the Parties 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.

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 months prior to the notification made under this Article, as was known to one or more parties, constitute the basis for relief under this article unless ACC-ORL, in the interest of justice, waives this requirement.

Failing resolution by mutual agreement, the aggrieved Party shall document the dispute, disagreement or misunderstanding by notifying the other Party in writing documenting the relevant facts, identifying unresolved issues, specifying the clarification or remedy sought and documenting the rationale as to why the clarification/remedy is appropriate. Within 10 working days after providing notice to the other Party, the aggrieved Party may, in writing, request a decision. The decision shall be rendered by an Officer authorized to bind the company.

The other Party shall submit a written position on the matter(s) in dispute within 30 calendar days after being notified that a decision has been requested. The receiving Party representative will conduct a review of the matter(s) in dispute and render a decision in writing within thirty calendar days of receipt of such position. In the event of a decision, or in the absence of a decision, within sixty calendar days of such referral for further review (or such other period as agreed to by the Parties), either party may pursue any right or remedy provided by law in a court of competent jurisdiction as authorized by 28 USC 1491, including but not limited to the right to seek extraordinary relief under Public Law 85-804. Alternatively, the parties may agree to explore and establish an Alternate Disputes Resolution procedure to resolve this dispute.

C. Termination Provisions

1. Termination by Mutual Consent
This Agreement, or any specific project under this Agreement, in whole or in part, may be terminated at any time upon mutual written consent of both Parties. In the event the Parties to this Agreement agree to terminate via mutual consent, the Parties shall negotiate in good faith what, if anything, is owed and due, including any applicable offset(s), prior to the Agreement, or any specific project under this Agreement, actually being terminated.

2. Termination for Failure to Perform
The Buyer may terminate this Agreement, or any part hereof, or any specific project hereunder, for "*cause"*. Cause shall be defined as:

a. In the event of any material failure to perform by the Subcontractor under the Agreement or under any project agreement;

b. In the event the Subcontractor fails to comply with any material term and/or condition of the Agreement, or specific project under this Agreement or a project agreement, fails to comply with any material term and/or condition of the Agreement and/or project agreement;

c. In the event the Subcontractor fails to provide the Buyer, upon written request, with adequate assurances of future performance.

In the event the Buyer seeks to terminate for *cause* per the above, the Buyer will issue to the Subcontractor a written notification that the Subcontractor has failed under this Agreement, provide what failures the Buyer has identified, and which provision for cause, as outlined above, the Buyer seeks to move forward under. The Subcontractor shall have fifteen (15) calendar days (should the fifteenth day fall upon a weekend or Government sanctioned holiday the fifteenth day shall be deemed the next official Government work day) to respond to the Buyer and/or take corrective action to mollify, mitigate, correct and/or cure the Buyer cited defect (hereinafter "Remedial Action"). The Buyer will consult with the Subcontractor to discuss the cause of the termination notice and determine whether additional efforts are in the best interest of the Buyer and whether Remedial Action could cure the Buyer cited defect. In the event the Buyer or Subcontractor Remedial Action mollifies, mitigates, corrects and/or cures the Buyer cited defect, the issue shall be resolved, however, notwithstanding the preceding, the Buyer may move forward with termination of the Agreement, or any project under the Agreement, in whole or in part, under any other clause under this Article VI. In the event of termination for a failure to perform, the Subcontractor will stop work immediately, and if applicable, terminate all subcontractors. In the event of termination for a failure to perform the Buyer shall only be liable to the Subcontractor for the actual work performed to date, minus any applicable offset for the failure to perform. Further, the Subcontractor shall be liable to the Buyer for any and all rights and remedies provided by law and herein due to a failure to perform. Furthermore, in the event of a termination for failure to perform by the Subcontractor, the Buyer will receive all rights in data and computer software as identified in this Agreement and/or a project agreement, if applicable. If it is later determined that the Buyer improperly terminated this Agreement for failure to perform, such termination shall be deemed a termination for convenience.

3. Termination for Convenience
The Buyer reserves the right to terminate this Agreement, or any part hereof, or any specific project under this Agreement, in whole or in part, for its sole convenience, upon written notice to the Buyer, with such written notice providing the Subcontractor a reasonable time to execute the Buyer's directives under the termination for convenience. In the event of such termination, the Subcontractor shall immediately stop all work hereunder and shall immediately

cause any and all of its suppliers, subcontractors to cease work, if applicable.

Subject to the terms of this Agreement the Buyer shall pay the Subcontractor's reasonable costs and/or fees, that the Subcontractor can demonstrate to the reasonable satisfaction of the Buyer using the Subcontractor's standard record keeping system, that have resulted from the termination, which such charges shall include any costs and/or fees associated with carrying out the termination for convenience. Neither the Subcontractor, nor any of its subcontractors shall be paid for any work performed or costs incurred which reasonably could have been avoided upon receipt of the termination for convenience. The Government, CMF and the Buyer will negotiate in good faith resolution of data rights and technical data when funded with mixed funding. At the Government's direction, this negotiation may occur upon notice of termination or after termination is effective, with such election by the Government not bearing upon or interfering with any other rights, duties and obligations of the Parties under the Agreement.

4. Stop Work Order
The Buyer may, at any time, by written order to a Subcontractor, require the Subcontractor to stop all, or any part, of the work called for under the Purchase Order. Upon receipt of the Stop Work Order, the applicable Subcontractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the stop work order during the period of work stoppage. Within the period of ninety (90) calendar days after the stop work order is delivered to the applicable Subcontractor, or within any extension of that period to which the parties have agreed, the Buyer will either:

(1) Cancel the stop work order, or

(2) Terminate, in whole or in part, the work covered by the Purchase Order.

If a Stop Work Order issued under this section is canceled, the Subcontractor shall resume work under the Purchase Order. The Buyer reserves the right to make an equitable adjustment in the delivery schedule or Purchase Order cost or price, or both that result from the stoppage of work. The Subcontractor shall assert its right to an equitable adjustment as a result of the stop work order within thirty (30) calendar days after the end of the period of work stoppage.

5. Limitation on Damages
In the event of any full or partial termination of this Agreement, or a project funded hereunder, by the Buyer, the Buyer shall not be liable for any loss of profits, revenue, or any indirect or consequential damages incurred by the Subcontractor, its contractors, subcontractors, or customers. A Party's liability for any damages under this Agreement is limited solely to direct damages and costs and/or fees incurred by a Party as a result of any termination of this Agreement, and subject to mitigation of such damages by a Party. In no instance shall the Buyer's liability for termination exceed the total amount due under this Agreement. Similarly, in no instance shall the Subcontractor's liability for termination exceed the total amount due by the Buyer to the Subcontractor under the Agreement.

ARTICLE VII: CONFIDENTIAL AND/OR PROPRIETARY INFORMATION

A. Definitions, as used in this Article:

"Disclosing Party" means the Party who discloses Confidential and/or Proprietary Information as contemplated by the subsequent paragraphs.

"Receiving Party" means the Party who receives Confidential and/or Proprietary Information disclosed by a Disclosing Party.

"Confidential and/or Proprietary Information" means information and materials of a Disclosing Party which are designated as confidential and/or proprietary or as a Trade Secret in writing by such Disclosing Party, whether by letter or by use of an appropriate stamp or legend, prior to or at the same time any such information or materials are disclosed by such Disclosing Party to the Receiving Party. Notwithstanding the foregoing, materials and other information which are orally, visually, or electronically disclosed by a Disclosing Party, or are disclosed in writing without an appropriate letter, stamp, or legend, shall constitute Confidential and/or Proprietary Information or a Trade Secret if such Disclosing Party, within 30 calendar days after such disclosure, delivers to the Receiving Party a written document or documents describing the material or information and indicating that it is confidential and/or proprietary

or a Trade Secret, provided that any disclosure of information by the Receiving Party prior to receipt of such notice shall not constitute a breach by the Receiving Party of its obligations under this Paragraph. Confidential and/or Proprietary Information includes any information and materials considered and marked as Trade Secret by the Party. Confidential and/or Proprietary Information does not mean data, software, or software documentation delivered and to be delivered in performance of this Agreement and each Purchase Order, which would be governed by TReX Article X, Data Rights and Copyrights.

"Trade Secret" means all forms and types of financial, business, scientific, technical, economic or engineering or otherwise proprietary information, including, but not limited to, patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(1) The owner thereof has taken reasonable measures to keep such information secret; and

(2) The information derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means, by the public.

Trade Secret does not mean data, software, or software documentation delivered and to be delivered in performance of this Agreement and each Purchase Order, which would be governed by Article X, Data Rights and Copyrights.

C. **Exchange of Information.**

Neither the Buyer or Subcontractor shall be obligated to transfer Confidential and/or Proprietary Information or Trade Secrets independently developed by the Buyer or Subcontractor absent an express written agreement between the Parties providing the terms and conditions for such disclosure. The obligations of the Receiving Party under this shall continue for an agreed-to period after the expiration or termination of this Agreement.

D. **Confidentiality and Authorized Disclosure.**

The Receiving Party agrees, to the extent permitted by law, that Confidential and/or Proprietary Information and Trade Secrets shall remain the property of the Disclosing Party (no one shall disclose unless they have the right to do so), and that, unless otherwise agreed to by the Disclosing Party, Confidential and/or Proprietary Information and Trade Secrets shall not be disclosed, divulged or otherwise communicated by it to third parties or used by it for any purposes other than in connection with specified Project efforts and the licenses granted in Article IX, Patent Rights, and Article X, Data Rights and Copyrights, provided that the duty to protect such "Confidential and/or Proprietary Information" and "Trade Secrets" shall not extend to materials or information that:

(3) Are received or become available without restriction to the Receiving Party under a proper, separate agreement,

(4) Are not identified with a suitable notice or legend (subject to the cure procedures described in the definition of "Confidential and/or Proprietary Information" above),

(5) Are lawfully in possession of the Receiving Party without such restriction to the Receiving Party at the time of disclosure thereof as demonstrated by prior written records,

(6) Are or later become part of the public domain through no fault of the Receiving Party,

(7) Are received by the Receiving Party from a third party having no obligation of confidentiality to the Disclosing Party that made the disclosure,

(8) Are developed independently by the Receiving Party without use of Confidential and/or Proprietary Information or Trade Secrets as evidenced by written records,

(9) Are required by law or regulation to be disclosed; provided, however, that the Receiving Party has

provided written notice to the Disclosing Party promptly so as to enable such Disclosing Party to seek a protective order or otherwise prevent disclosure of such information.

ARTICLE VIII: PUBLICATION AND ACADEMIC RIGHTS

A. Use of Information.

The Government, CMF, and the Buyer shall have the right to publish or otherwise disclose information and/or data developed by the Subcontractor under the projects conducted through TReX II. The Government, CMF, and the Buyer shall include an appropriate acknowledgement of the sponsorship of the projects by the Subcontractor in such publication or disclosure. The Government, CMF, and the Buyer shall have only the right to use, disclose and exploit any such data and Confidential Information or Trade Secrets in accordance with the rights held by them pursuant to this Agreement. Notwithstanding the above, the Government, CMF, and the Buyer shall not be deemed authorized by this paragraph alone to disclose any Confidential Information or Trade Secrets of the Subcontractor.

(a) Publication, Public Disclosure of Information, or Other Public Announcements.

Any public announcements (including press releases, website postings or other public statements) by any party regarding this Agreement or Purchase Orders awarded thereafter shall be coordinated with the CMF through the Buyer and cognizant ACC-ORL AO.

Acknowledgment of Government support will appear in any publication of any material based on or developed under this OTA, using the following acknowledgement terms:
"Effort sponsored by the U.S. Government under the Training and Readiness Accelerator II (TReX II), OTA. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon."

Every publication of material based on or developed under this Agreement must contain the following disclaimer:
"The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government."

ARTICLE IX: PATENT RIGHTS

A. Definitions, as used in this Article:

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

"Made" when used in relation to any Invention means the conception or first actual reduction to practice of such Invention.

"Practical Application" means to manufacture, in the case of a composition of product; to practice, in the case of a process or method, or to operate, in the case of a machine or system; and in each case, under such conditions as to establish that the Invention is capable of being utilized and that its benefits are, to the extent permitted by law or Government regulations, available to the public on reasonable terms.

"Subject Invention" means any Invention of a Subcontractor conceived or first actually reduced to practice in the performance of work under this Agreement.

"Background Invention" means any Invention Made by a Subcontractor (or their subcontractors of any tier) prior to performance of the Agreement or outside the scope of work performed under this Agreement.

(a) Allocation of Principal Rights.

Buyer shall retain the entire right, title and interest throughout the world to each Subject Invention consistent with the provisions of this Article, and 35 U.S.C. § 202. With respect to any Subject Invention in which Buyer retains title, the

Government shall have a non-exclusive, nontransferable, irrevocable, paid-up license to practice or have practiced on behalf of the United States the Subject Invention throughout the world.

Buyer may elect to provide full or partial rights that it has retained to other parties.

(b) Survival Rights.

Provisions of this Article IX shall survive termination of this Agreement.

ARTICLE X: DATA RIGHTS AND COPYRIGHTS

Allocation and levels of Data Rights will be considered, negotiated, and documented for each prototype project.

The Buyer reserves the right to protect by copyright original works developed under this Agreement. All such copyrights will be in the name of the individual TReX II member entity(ies). The Buyer grants to the U.S. Government a non-exclusive, non-transferable, royalty-free, fully paid-up license to reproduce, prepare derivative works, distribute copies to the public and perform publicly and display publicly, for governmental purposes, any copyrighted materials developed under this Agreement, and to authorize others to do so. However, notwithstanding the above, proprietary or otherwise protected information (including technical data and software) shall not be disclosed or released.

A. Prior Technology.

In the event it is necessary for the Buyer to furnish Subcontractor with Data which existed prior to, or was produced outside of this Agreement, and such Data is so identified with a suitable notice or legend, the Data will be maintained in confidence and disclosed and used by the Subcontractor only for the purpose of carrying out their responsibilities under this Agreement. Data protection will include proprietary markings and handling, and, upon request by the Buyer, the signing of non-disclosure agreements by Subcontractor employees and/or their subcontractors' employees. Upon completion of activities under this Agreement, such Data will be disposed of as requested by the Government.

(a) Consortium Member Organization's Prior Technology.

In the event it is necessary for a Subcontractor to furnish the Buyer with Data which existed prior to, or was produced outside of this Agreement, and such Data embodies trade secrets or comprises commercial or financial information which is privileged or confidential, and such Data is so identified with a suitable notice or legend, the Data will be maintained in confidence and disclosed and used by the Buyer under this Agreement. Data protection will include proprietary markings and handling, and the signing of non-disclosure agreements by such Government Contractors or contract employees as needed.

Subcontractor shall not be obligated to provide Data that existed prior to, or was developed outside of this Agreement to Buyer. Upon completion of activities under this Agreement, such Data will be disposed of as requested by the Subcontractor. If any Subcontractor contemplates incorporating proprietary commercial software into their prototype solution, the Subcontractor must self-certify that the software does not violate federal law or regulation.

(b) Marking of Data.

Any Data delivered under this Agreement, by the Buyer or Subcontractor, shall be marked with a suitable notice or legend.

ARTICLE XI: EXPORT CONTROL

A. Export Compliance

Information subject to Export Control Laws/International Traffic in Arms Regulation (ITAR) Public Law 90 629,« Arms Export Control Act, » as amended (22 U.S.C. § 2751 et. Seq.) requires that all unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license under Executive Order (EO) 12470 or the Arms Export Control Act and that such data require an approval, authorization, or license under EO 12470 or the Arms Export Control Act. For purposes of making this determination, the Military Critical Techniques

List (MCTL) shall be used as general guidance. All documents determined to contain export controlled technical data will be marked with the following notice:

WARNING – this document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., and Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provision of DOD Directive 5230.25.

(a) Flowdown.

The Buyer shall include this Article, suitably modified to identify all parties, in all Purchase Orders or lower-tier agreements. This Article shall, in turn, be included in all sub-tier subcontracts or other forms of lower-tier agreements, regardless of tier.

ARTICLE XII: TITLE AND DISPOSITION OF PROPERTY

In this Article, "property" means any tangible personal property, other than property actually consumed during the execution of work under this Agreement. No significant items of property are expected to be acquired under this Agreement by the Subcontractor. Title to any item of property that is acquired by the Subcontractor pursuant to a Purchase Order based on the Buyer's selection of Subcontractor's quote in response to a Request for Quote under this OTA, shall vest with the Buyer upon acquisition with no further obligation unless otherwise determined by the AO.

The Subcontractor shall be responsible for the maintenance, repair, protection and preservation of all such property at its own expense during performance.

ARTICLE XIII: OPERATIONAL SECURITY (OPSEC), SECURITY & CREDENTIALING

A. Flowdown

For all Purchase Orders, the following statement shall be flowed to the Buyer's sub tier ubcontractors unless otherwise stated within the Purchase Order.

Classification guidance for requirement - "The security level for this agreement is UNCLASSIFIED."

ARTICLE XIV: LIABILITY OF THE PARTIES

A. Waiver of Liability.

With regard to the activities undertaken pursuant to this Agreement, no Party shall make any claim against the others, employees of the others, the others' related entities (e.g., contractors, subcontractors, etc.), or employees of the others' related entities for any injury to or death of its own employees or employees of its related entities, or for damage to or loss of its own property or that of its related entities, whether such injury, death, damage or loss arises through negligence or otherwise, except in the case of willful misconduct.

(a) Damages.

The Parties shall not be liable to each other for consequential, punitive, special and incidental damages or other indirect damages, whether arising in contract (including warranty), tort (whether or not arising from the negligence of a Party) or otherwise, except to the extent such damages are caused by a Party's willful misconduct.

Notwithstanding the foregoing, claims for contribution toward third-party injury, damage, or loss are not limited, waived, released, or disclaimed.

(b) Extension of Waiver of Liability.

The Buyer agrees to extend the waiver of liability as set forth above to subcontractors at any tier under a Purchase

Order by requiring them, by contract or otherwise, to agree to waive all claims against the Government and the CMF.

(c) Applicability.

Notwithstanding the other provisions of this article, this Waiver of Liability shall not be applicable to:

(1) Claims between the CMF, the Buyer and the Government regarding a material breach, noncompliance, or nonpayment of funds;

(2) Claims for damage caused by willful misconduct; and

(3) Intellectual property claims.

(d) Limitation of Liability.

In no event shall the liability of the Government, the CMF, Buyer, or any other entity performing activities under a Purchase Order, exceed the amount obligated by the Government and/or if cost-sharing occurs, committed as a cash contribution or in-kind contribution by a consortium member entity, for the performance of a Purchase Order.

Notwithstanding the foregoing, claims for contribution toward third-party injury, damage, or loss are not limited, waived, released, or disclaimed. 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, however, the Government will consider going forward with a request for special indemnification or the inclusion of specially negotiated liability provisions where a project, as identified by the Government or by the CMF, on behalf of the Buyer, may pose a risk of such nature.

ARTICLE XV: GENERAL PROVISIONS

A. Severability.

In the event that any provision of this Agreement or Purchase Order becomes or is declared by a court of competent jurisdiction to be illegal, unenforceable or void, this Agreement shall continue in full force and effect without said provision; Provided that no such severability shall be effective if the result of such action materially changes the economic benefit of this Agreement to the Parties.

(a) Force Majeure

No failure or omission by the CMF, Buyer, or Subcontractor in the performance of any obligation of this Agreement shall be deemed a breach of this Agreement or create any liability if the same shall arise from any cause or causes beyond the control of the parties including but not limited to, the following: acts of God; Acts or omissions of any Government; Any rules, regulations or orders issued by any Governmental authority or by any officer, department, and agency or instrumentality thereof; fire; storm; flood; earthquake; accident; war; rebellion; insurrection; riot; and invasion and provided that such failure or omission resulting from one of the above causes is cured as soon as is practicable after the occurrence of one or more of the above mentioned causes.

ARTICLE XVI: NOT FLOWED DOWN

ARTICLE XVII: NOT FLOWED DOWN

ARTICLE XVIII: FLOW DOWN PROVISION

The Buyer is obligated under this Agreement to ensure flow down provisions, where applicable, are properly incorporated in whatever controlling agreement(s) the Buyer has executed between itself and its subcontractors

(including, but not limited to: agents, partners, joint ventures, consultants, service providers etc.), and to monitor compliance thereof. Nothing in this Agreement is meant to prohibit the Buyer and the lower tier subcontractors from negotiating additional terms and conditions, provided that the negotiated terms and conditions adhere to the flow down provisions from this Agreement.

ARTICLE XIX: TELECOMMUNICATIONS

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

A. *Definitions.* As used in this provision:

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 article means any hardware, software, or service that–

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

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

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

Covered entity means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(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. *Covered foreign country* means The People's Republic of China. *Covered telecommunications equipment or services* means–

(1) Telecommunications equipment produced by Huawei Technologies Company 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 Company, or Dahua Technology Company (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).

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.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

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.

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

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub.L. 115-91) prohibits Government use of any covered article. The Vendor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contractual agreement.

(c) *Reporting requirement.*

(1) In the event the Vendor identifies a covered article provided to the Government during performance of the contractual agreement, or the Vendor is notified of such by a subcontractor at any tier or any other source, the Vendor shall report, in writing, to the Agreements Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil. For indefinite delivery contractual agreements, the Vendor shall report to the Agreements Officer for the indefinite delivery contractual agreement and the Agreements Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contractual agreement and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Vendor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: the contractual agreement number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Vendor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) Subcontracts. The Vendor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of Provision)

ARTICLE XX: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)

A. Definitions. As used in this clause—

"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.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an unclassified information system that is owned, or operated by or for, a contractor 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—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

“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.

“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.

“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 contractor 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.

“Rapidly report” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT)

service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

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

(2) For covered contractor 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 (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor 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 in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

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

(C) If the DoD CIO has previously adjudicated the contractor'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 Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor 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/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause 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 Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, 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.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) 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 contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor'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 Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor 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.

(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(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 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, 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.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) Subcontracts. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

ARTICLE XXI: ORDER OF PRECEDENCE

In the event of any inconsistency between the terms of this Agreement and Purchase Orders, the inconsistency shall be resolved by giving precedence in the following order:

(1) this Agreement;

(2) Attachments to this Agreement;

(3) the Purchase Order documentation. In any event, specifically negotiated Purchase Order terms will govern over general terms of each project.

ARTICLE XXII: EXCESS MATERIAL

In the event of the Subcontractor delivering excess material under this Agreement, Buyer retains the right to reject and return all material in excess of quantities stated in the Purchase Order, at Subcontractor's expense. The Subcontractor shall notify Buyer and receive written approval from Buyer before delivering material in excess of quantities stated in the Purchase Order.

Revision History

Rev	Date	Section	Paragraph	Summary of change	Authorized by
1.0	3/26/24			Initial issue	Kathryn Bigelow