Appendix A – Prime Contract Flowdowns – OTA (DOTC 19-01-INTI0209)

1. U.S. Government Contract Regulations. This Subcontract is being issued in support of a U.S. Government project through an Other Transaction Authority ("OTA"). The clauses below are incorporated herein with the same force and effect as if they were set forth in full text in the Subcontract.

2. The DFAR clauses referenced below in effect on the date of this Subcontract are incorporated herein. In all such clauses, unless the context of the clause required otherwise, the term "Contract" shall mean this Subcontract and the term "Contractor" shall mean Subcontractor as set forth in the Subcontract.

a. **DFARS 252-223-7002** – Safety Precautions for Ammunitions and Explosives
b. **DFARS 252-223-7006** – Prohibition on Storage and Disposable of Toxic and Hazardous Materials

3. DFARS 252.223-7007 Safeguarding Sensitive Conventional Arms, Ammunition, and Explosives

SAFEGUARDING SENSITIVE CONVENTIONAL ARMS, AMMUNITION, AND EXPLOSIVES (SEP 1999)

(a) Definition. "Arms, ammunition, and explosives (AA&E)," as used in this clause, means those items within the scope (chapter 1, paragraph B) of DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives.

(b) The requirements of DoD 5100.76-M apply to the following items of AA&E being developed, produced, manufactured, or purchased for the Government, or provided to the Contractor as Government-furnished property under this contract:

Lead/ Sub	Nomenclature	NSN	Sensitivity/Category	Hazard Class.	Physical Location	CAGE CODE/POC	Approved?
Sub	LF-2XA	N/A	SRC II	1.1D	Ensign-Bickford Aerospace & Defense Company 500 Bickford Rd. Graham, KY 42344	8K366 Alan Garvey, (860) 843-2507. ajgarvey@ebad.com	Not Approved

(c) The Contractor shall comply with the requirements of DoD 5100.76-M, as specified in the statement of work. The edition of DoD 5100.76-M in effect on the date of issuance of the solicitation for this contract shall apply.
(d) The Contractor shall allow representatives of the Defense Security Service (DSS), and representatives of other appropriate offices of the Government, access at all reasonable times into its facilities and those of its subcontractors, for the purpose of performing surveys, inspections, and investigations necessary to review compliance with the physical security standards applicable to this contract.
(e) The Contractor shall notify the cognizant DSS field office of any subcontract involving AA&E within 10 days after award of the subcontract.
(f) The Contractor shall ensure that the requirements of this clause are included in all subcontracts, at every tier
(1) for the development. Production, manufacture, or purchase of AA&E; or
(2) when AA&E will be provided to the subcontractor as Government-furnished property.
(g) Nothing in this clause shall relieve the Contractor of its responsibility for complying with applicable Federal, state, and local laws, ordinances, codes, and regulations (including requirements for obtaining licenses and permits) in connection with the performance of this contract.

4. 252.225-7048 Export-Controlled Items.
As prescribed in 225.7901-4, use the following clause:

Export-Controlled Items (JUN 2013)
(a) Definition. "Export-controlled items," as used in this clause, means items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The term includes -

(1) "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 CFR Part 120; and

(2) "Items," defined in the EAR as "commodities", "software", and "technology," terms that are also defined in the EAR, 15 CFR 772.1.

(b) The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.

(c) The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.
(d) Nothing in the terms of this contract adds, changes, supersedes, or waives any of the requirements of applicable Federal laws, Executive orders, and regulations, including but not limited to -

(1) The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, et seq.);

(2) The Arms Export Control Act (22 U.S.C. 2751, et seq.);

(3) The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);

(4) The Export Administration Regulations (15 CFR Parts 730-774);

(5) The International Traffic in Arms Regulations (22 CFR Parts 120-130); and

(6) Executive Order 13222, as extended.

(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts.

5. 252.204-7012 Safeguarding covered defense information and cyber incident reporting.
As prescribed in 204.7304c, use the following clause:

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 Governmentwide 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 nonapplicable 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.

6. CONFIDENTIAL INFORMATION

A. Definitions

"Confidential Information" means information and materials which are designated as Confidential or as a Trade Secret in writing, 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 Information or a Trade Secret if the Disclosing Party, within thirty (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 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 Information" also includes any information and materials considered a Trade Secret by the NAC on its own behalf or on behalf of the CMF or NAC Members, or their subcontractors or suppliers.

"Trade Secret" means all forms and types of financial, business, scientific, technical, economic, 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, regardless of how it is stored, compiled, or memorialized, including physically, electronically, graphically, photographically, or in writing if:

1. The owner 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.

B. Exchange of Information

The Government may from time to time disclose Government Confidential Information to the NAC for use by the CMF or NAC Members awarded OTIAs, their subcontractors or suppliers, in connection with the Annual Technology Plan and similar processes or particular projects. The CMF, on behalf of the NAC, NAC Members, their subcontractors or suppliers, may from time to time disclose information that is Trade Secret or Confidential Information to the Government in connection with this Agreement, a project proposal, DOTC Base Agreements, or performance under an OTIA. Neither Party shall be obligated to transfer Confidential Information or Trade Secrets independently developed by the Parties, absent an express written agreement between the Parties providing the terms and conditions for the disclosure.

C. Confidentiality and Authorized Disclosure

The Receiving Party agrees, to the extent permitted by law, that Confidential Information and Trade Secrets shall remain the property of the Disclosing Party, and that, unless otherwise agreed by the Disclosing Party, Confidential Information and Trade Secrets shall not be disclosed, divulged, or otherwise communicated to third parties or used by for any purposes other than in connection with specified project efforts and the licenses granted in Article X, Patent Rights, and Article XI, Data Rights and Copyrights. The aforementioned shall not extend to information or materials that:

1. Are received or become available without restriction to the Receiving Party under a proper, separate agreement;
2. Are not identified with a suitable notice or legend;
3. Are lawfully in possession of the Receiving Party without such restriction to the Receiving Party at the time of disclosure, as demonstrated by prior written records;
4. Are or later become part of the public domain through no fault of the Receiving Party;
5. Are received by the Receiving Party from a third party having no obligation of confidentiality to the Disclosing Party that made the disclosure;
6. Are developed independently by the Receiving Party without use of Confidential Information or Trade Secrets, as evidenced by written records; or
7. Are required by law or regulation to be disclosed, provided, however, that the Receiving Party has given written notice to the Disclosing Party promptly so as to enable such Disclosing Party to seek a protective order or otherwise prevent further disclosure of such information.

D. Return of Proprietary Information

Upon the request of either Party, the other Party shall promptly return all copies and other tangible manifestations of the Confidential Information or Trade Secrets that were disclosed. As used in this section, tangible manifestations include human readable media as well as magnetic and digital storage media.

E. Term

Except to the extent covered by and subject to other provisions of this Agreement or the specific OTIA, the obligations of the Receiving Party under this Article shall continue for a period of five (5) years after the expiration or termination of the OTIA under which the information was provided.

The NAC Member, shall flow down the requirements of this Article to their respective personnel, member entities, and agents at all levels.

7. PUBLICATION AND ACADEMIC RIGHTS

A. Use of Information

Subject to the provisions of Article VIII, Confidential Information, and other applicable provisions of this Agreement, the Government and the NAC Members awarded OTIAs shall have the right to publish or otherwise disclose information or data developed by the Government or the respective NAC Members under OTIAs. The NAC Members awarded OTIAs shall include an appropriate acknowledgement of the sponsorship of the projects by the Government in any such publications or disclosures.

B. Classified Research Projects

If a desired publication includes information relating to a Classified project, the provisions of the DoD Security Agreement (DD Form 441), Certificate Pertaining to Foreign Interests (SF 328), and the DoD Contract Security Classification Specification (DD Form 254) apply.

C. Review or Approval of Technical Information for Public Release

At least thirty (30) calendar days prior to the scheduled release date, the NAC Member awarded an OTIA, shall submit to the AOR at least one (1) copy of the information to be released along with the required public release form. The AOR will route the information to the cognizant Public Affairs Office for review and approval. The AOR is hereby designated as the approval authority for the Agreements Officer for such releases.

Where an Academic Research Institution is awarded an OTIA, who is performing fundamental research on campus the CMF shall require such NAC Member to provide papers and publications to the AOR for review and comment at least thirty (30) calendar days prior to the formal paper or publication submission. However, if that Academic Research Institution incorporates into its research results or publications artifacts produced by and provided to these institutions by other (non-educational institution) NAC Members (or has authors listed on the paper who are not employees or students of the Academic Research Institution), then the procedures in the preceding paragraph shall be followed.

Parties to this Agreement are responsible for assuring that an acknowledgment of Government support will appear in any publication of any material based on or developed under the awarded OTIA, using the following acknowledgement terms:

"This effort was sponsored by the U.S. Government under the DoD Ordnance Technology Consortium (DOTC) Other Transaction Agreement (OTA) (W15QKN-18-9-1008) with the National Armaments Consortium (NAC). The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein."

Parties to this Agreement are also responsible for assuring that every publication of material based on or developed under an OTIA contains 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."

The NAC Member shall flow down these requirements to at all tiers.

D. Notices

To avoid disclosure of Confidential Information or Trade Secrets belonging to the Government or a NAC Member, or the loss of patent rights as a result of premature public disclosure of patentable information, the NAC Member that is proposing to publish or disclose such information provide advance notice to the CMF and identify such other parties, including the Government, as may have an interest in the information. The CMF shall notify such parties at least thirty (30) calendar days prior to any NAC Member's submission for publication or disclosure, together with any and all materials intended for publication or disclosure relating to technical reports, data, or information developed by the parties during the term of and pursuant to this Agreement. The Government must notify the CMF of any objection to disclosure within the thirty (30) day period, or the NAC Member shall be deemed authorized to make the disclosure.

E. Filing of Patent Applications

During the course of the aforementioned thirty (30) calendar day period, the NAC Member or the Government shall provide notice to the Agreements Officer if either desires that a patent application be filed on any invention potentially disclosed in the materials. In the event that the NAC Member or the Government desires that such a patent be filed, the NAC shall ensure that the publication of the materials is withheld until the occurrence of the first of the following:

1. Filing of a patent application covering the invention;
2. Written agreement, from the Agreements Officer and the CMF, with the authorization of the cognizant NAC Member, that no patentable invention is disclosed in such materials; or
3. Written agreement, from the Agreements Officer and the CMF, with the authorization of the cognizant NAC Member, that all potentially patentable information is removed from the proposed publication.

8. PATENT RIGHTS

A. Allocation of Principal Rights

Patent Rights under this Agreement or subsequent OTIAs shall be determined in accordance with FAR 52.227-11 (Patent Rights—Ownership by the Contractor (May 2014)), which is hereby incorporated by reference with the following modifications:

1. As appropriate, replace "Contractor" with "NAC Member"; "the agency" and "the Federal Agency" with "Government"; "contract" with "Agreement"; and "Contracting Officer" with "Agreements Officer".

2. The Government shall have the initial option to retain title to each subject invention made only by Government employees or made jointly by the NAC Member and Government employees. The Government shall promptly notify the NAC Member upon making this election, and agrees to timely file patent applications at its own expense and agrees to grant to the NAC Member a non-exclusive, irrevocable paid-up license to practice the subject invention throughout the world.
3. The NAC Member shall elect in writing whether or not to retain ownership of any subject invention by notifying the Agreements Officer within six (6) months of disclosure. In any case where publication, on sale, or public use has initiated the one (1) year statutory period during which valid patent protection can be obtained in the United States, the period of election of title shall no later than sixty (60) calendar days prior to the end of the statutory period.
4. The CMF, on behalf of the NAC Member, may request an extension to the six (6) month period for ownership election. The Agreements Officer may, in their discretion, extend the ownership election period, but the ownership election period shall not exceed two (2) years from the disclosure of the subject invention.

FAR 52.227-1 (Authorization and Consent (Dec 2007)) and Alternate I (Apr 1984) and FAR 52.227-2 (Notice and Assistance Regarding Patent and Copyright Infringement (Dec 2007)) are also incorporated by reference under this Agreement. If FAR 52.227-3 3 (Patent Indemnity (Apr 1984)) is applicable, it shall be incorporated into the OTIA.

B. Patent Reports

All DOTC Base Agreements shall require the use of DD Form 882, Report of Inventions and Subcontracts, to file an invention report for every OTIA. Negative reports are also required. The NAC Member shall provide the CMF, with an Annual Invention Report at the close of each performance year of each OTIA and at the end of the term of each OTIA.

C. Final Payment

Final payment of an OTIA cannot be made until the NAC Member delivers to the CMF all disclosures of subject inventions and confirmatory instruments required by this Agreement.

D. Lower Tier Agreements

The NAC Member shall include this Article, suitably modified in all lower tier agreements, regardless of tier, for experimental, developmental, or research work performed under the OTIAs awarded pursuant to this Agreement.

The provisions of this Article shall survive termination of this Agreement under Article II, Section C.

9. DATA RIGHTS AND COPYRIGHTS

Although this Article shall serve as the default and overarching terms and conditions for the handling of Data Rights and Copyrights, every OTIA is individually negotiated, and any specific Data Rights or Copyright terms and conditions in the OTIA Statement of Work will control over this Article.

Technical Data and Computer Software Rights under this Agreement shall be determined in accordance with DFARS 252-227-7013 (Rights in Technical Data—Noncommercial Items (Feb 2014)) and DFARS 252.227-7014 (Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (Feb 2014)), except at otherwise specified in this Article or the OTIA. The definitions included in this Article shall replace the definitions found in the referenced DFARS clauses.

A. Definitions

“Government Purpose” means any activity in which the Government is a party. 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” means the right to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and to 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 Government purposes. This is a middle path unique to defense contracts that allows contractors to have the exclusive right to use the technical data in the commercial market. Unless otherwise agreed, Government Purpose Rights convert to Unlimited Rights five years after execution of the OTIA.

“Limited Rights” means the right to use, modify, reproduce, release, perform, display, or disclose technical data, in whole or in part, within the Government. The Government may not, without the written permission of the party asserting limited rights, release or disclose the technical data outside the Government, use the technical data for manufacture, or authorize the technical data to be used by another

party. However, the Government may reproduce, release, or disclose such data or authorize the use or reproduction of the data by persons outside the Government if it is necessary for emergency repair and overhaul, or a release or disclosure to a covered Government support contractor in performance of its covered Government support contract (management and administrative support). The recipient of the technical data is subject to prohibition on the further reproduction, release, disclosure, or use of the technical data, and the contractor or subcontractor asserting the restriction shall be notified of such reproduction, release, disclosure, or use.

"Restricted Rights" applies only to noncommercial computer software and means the Government's right to use a computer program on a limited number of computers, and make the minimum number of copies of the computer software required for safekeeping (archive), backup, or modification purposes. However, the Government may allow the use of the noncommercial computer software outside of the Government under a limited set of circumstances, including use by a covered Government support contractor in performance of its covered Government support contract (management and administrative support), and after the contractor or subcontractor asserting the restriction is notified.

"SBIR Data Rights" refers to a Small Business Innovation Research contract and applies to both technical data and computer software. The contractor is entitled the SBIR data protection to all technical data and computer software developed during performance of a SBIR Phase III agreement, regardless of the funding source. SBIR Data Rights are generally equivalent to Limited Rights for technical data and Restricted Rights for computer software. In the DOD, SBIR Data Rights survive for five years from the completion of the project, at which point they will convert to Unlimited Rights. SBIR efforts are divided into three successive phases (I, II, III), with the ultimate goal of commercializing the technology in question. The Government can award an unlimited number of SBIR Phase III agreements as long as they are a logical follow-on to the technology being developed, and with the understanding that the five-year clock restarts with every award.

"Specifically Negotiated License Rights" means any modification by mutual agreement to the standard DFARS noncommercial data rights categories (Unlimited Rights, Government Purpose Rights, Limited/Restricted Rights) laid out in this Article that the Government and NAC Member consider appropriate to the specific contract action, but shall not provide rights less than that provided by Limited Rights. Any rights so negotiated shall be identified in a license agreement written into or made part of the OTIA.

"Technical Data" means recorded information, regardless of the form or method of recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial or management information.

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

B. Allocation of Principle Rights

The Government shall receive a Government Purpose Rights license or an Unlimited Rights license to all technical data and computer software developed and delivered under this Agreement, except for the technical data and computer software that was previously developed exclusively at private expense and identified in the OTIA Statement of Work. To the maximum extent practicable, segregable portions of deliverables that will be restricted shall be clearly identified and labeled by the NAC Member.

The Government and the NAC Member can negotiate for a specific level of rights to all, or a distinct subset of the technical data and computer software that is developed and delivered for a specific OTIA, which will have the full force and effect of an executed license.

If the Government and the NAC Member agree to engage in a Cost Share OTIA, and the NAC Member desires to contribute more than 50% of the total costs of the project, the Government may agree to a Limited or Restricted Rights license to all technical data and computer software developed and delivered under the OTIA, or any other mutually agreed upon level of rights to a distinct subset of the technical data and computer software developed and delivered under the OTIA.

C. Copyrights

The NAC Member reserves the right to protect by copyright original works developed under this Agreement and any subsequent OTIA, pursuant to 17 U.S.C. §§ 401 and 402. All such copyrights will be in the name of the individual NAC Member. The NAC Member, hereby grants to the 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.

In the event that information is exchanged with a notice indicating that it is protected under copyright as a published, copyrighted work, and it is also indicated that such information existed prior to, or was produced outside of this Agreement or any subsequent OTIA, the Government, the CMF or the NAC Member receiving the information and others acting on its behalf may reproduce, distribute, and prepare derivative works for the sole purpose of carrying out its responsibilities under this Agreement.

D. Handling of Data

The NAC Member shall clearly identify, prior to award, the technical data and computer software (and the items, components or processes to which they pertain) that will have asserted restrictions in each OTIA Statement of Work. If, after award, the NAC Member wishes to use any other internally developed technical data or computer software, or any other pre-existing proprietary information not previously identified in the OTIA Statement of Work, then the NAC Member shall disclose its intent in writing the CMF prior to its use, and shall receive written approval from the Agreements Officer through the CMF prior to its use or incorporation. The asserted restrictions in the OTIA Statement of Work are the unilateral claims of the NAC Member, and the inclusion of those restrictions in the OTIA Statement of Work does not equate to the Government's agreement to those claims. At any time, the Government has the right to request substantiating information supporting those claims, and can challenge or reject those claims if they are unsupported.

Technical Data and Computer Software Provided by the Government: Technical data and computer software provided by the Government under this Agreement shall be appropriately marked with a suitable notice or legend and maintained in confidence and disclosed and used by the NAC Member only for the purpose of carrying out their responsibilities under a specific OTIA. At no time will technical data and computer software provided by the Government under this Agreement become the property of the NAC Member, nor does its use in carrying out their responsibilities grant any form of license to the NAC Member to disclose or use that technical data or computer software for any other purpose, unless specifically agreed to in writing by the Agreements Officer. This includes all technical data and computer software first produced by the Government under this Agreement. All OTIAs that contain technical data or computer software provided by the Government shall have appropriate non-disclosure agreements signed by the NAC Member. Upon completion of an OTIA, the aforementioned technical data and computer software shall be disposed of as requested by the Government.

Oral and Visual Information: If information which the NAC or any NAC Member considers to embody trade secrets or to comprise commercial or financial information which is privileged or confidential is disclosed orally or visually to the Government, the exchange of such information must be reduced to a tangible, recorded form and marked with a suitable notice or legend, and furnished to the Government within ten (10) calendar days after such oral or visual disclosure, or the Government shall have no duty to limit or restrict, and shall not incur any liability for any disclosure and use of such information.

Disclaimer of Liability: Notwithstanding the above, the Government shall not be restricted in, nor incur any liability for, the disclosure and use of:

1. Data or software not identified with a suitable notice or legend as set forth in this Article; nor
2. Information contained in any data or software for which disclosure and use is restricted under Article VIII, Confidential Information, if such information is or becomes generally known without breach of the above, is known to or is generated by the Government independently of carrying out responsibilities under this Agreement, is rightfully received from a third party without restriction, or is included in data or software which the NAC Member have or is required to furnish to the Government without restriction on disclosure and use.

E. Marking of Data

Except for technical data and computer software developed or delivered with Unlimited Rights, all technical data and computer software developed and delivered under this Agreement shall have appropriate Data Rights Markings in accordance with DFARS 252.227-7013(f) and 252.227-7014(f). The Government will have Unlimited Rights to all unmarked technical data or computer software. In the event that unmarked technical data or computer software should have contained a restrictive legend, the CMF, on behalf of the NAC Member, can cure the omission by providing written notice to the Agreements Officer within thirty (30) calendar days of the erroneous disclosure. The Government will not be responsible for any additional disclosures of the inappropriately marked technical data or computer software prior to that written notice.

F. Lower Tier Agreements

The NAC Member shall include this Article, suitably modified, in all lower tier agreements, regardless of tier, for work performed under the OTIAs awarded pursuant to this Agreement.

The provisions of this Article shall survive termination of this Agreement under Article II, Section C.

10. EXPORT CONTROL

A. Export Control

The Parties 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, the NAC Member shall not export, directly or indirectly, any products or technology, Confidential Information, Trade Secrets, or Classified and Unclassified Technical Data in violation of any U.S. Export laws or regulations.

B. Lower Tier Agreements

The NAC Member shall include this Article, suitably modified in all lower tier agreements, regardless of tier, for work performed under the OTIAs awarded pursuant to this Agreement.

The provisions of this Article shall survive termination of this Agreement under Article II, Section C.

11. SECURITY

The DOTC Base Agreement is Unclassified. However, individual OTIAs may require access to Classified Information, including but not limited to information classified as Controlled Unclassified Information (CUI), Confidential, Secret, or Top Secret. As such, DoD Manual 5200.01 (DoD Information Security Program: Protection of Classified Information) shall apply and all appropriate measures shall be followed. The NAC Member shall also comply with DD Form 254 (Contract Security Classification Specification), DD Form 441 (DoD Security Agreement), DoD 5220.22-M (National Industrial Security Program Operating Manual), and all other security requirements including but not limited to OPSEC requirements.

The NAC Member shall comply with Distribution Statements, as mandated by DoDI 5230.24 (Distribution Statements on Technical Documents).

Covered Defense Information (CDI) will be identified at the OTIA level. The NAC Member shall comply with DFARS 252.204-7012 (Oct 2016): Safeguarding Covered Defense Information and Cyber Incident Reporting, which includes implementing on its covered contractor information systems the security requirements specified by DFARS 252.204-7012. Nothing in this paragraph shall be interpreted to foreclose the NAC Member's right to seek alternate means of complying with the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (as contemplated in DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) (Oct 2016) and DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)).

12. SAFETY AND ENVIRONMENTAL

OTIAs that involve the handling of Arms, Ammunition and Explosives (AA&E) shall be subject to all appropriate FAR and DFARS clauses, as well as all Federal, State and local rules and regulations required in order to maintain a safe and non-hazardous occupational environment. A Safety Survey will be conducted by the Government prior to handling of explosives, production of any hardware or fire testing under the OTIAs.

If an OTIA will involve AA&E or other Hazardous Material, the following clauses with their prescribed usages MUST be reviewed for applicability to the procurement action. The following Federal Acquisition Regulation Supplement (FARS), Defense Federal Acquisition Regulation Supplement (DFARS) clauses by reference, and local clauses with the same force and effect as if they were given in full text shall be incorporated into the OTIAs if applicable. Upon request, the CMF will make their full text available.

DFARS 252.223-7001	Hazard Warning Labels
DFARS 252.223-7002	Safety Precautions for Ammunition and Explosives
DFARS 252.223-7003	Change in Place of Performance
DFARS 252.223-7006	Prohibition on Storage and Disposal of Toxic and Hazardous Materials
DFARS 252.223-7007	Safeguarding Sensitive Conventional Arms, Ammunition and Explosives
FAR 52.223-3	Identification and Material Safety Data
FAR 52.247-29	F.O.B. Origin
ARDEC 18	Physical Security Standards for Sensitive Items
ARDEC 169	Explosive Material Handling
ARDEC 66	Safety Requirements for Hazardous Items
ARDEC 77	Material Safety Data Sheets

At a minimum, The NAC Member shall provide the following reports and materials on an as needed basis:

1. Accident/Incident Report: The NAC Member shall report immediately any major accident/incident (including fire) resulting in any one or more of the following: causing one or more fatalities or one or more disabling injuries; damage of Government property exceeding $10,000; affecting program planning or production schedules; degrading the safety of equipment under initiative, such as personnel

injury or property damage may be involved; and identifying a potential hazard requiring corrective action. The NAC Member shall prepare a DI-SAFT-81563 report for each incident.
2. Material Safety Data Sheets (MSDS): The NAC Member shall prepare and maintain MSDS for all materials used and generated under this Agreement.
3. Explosive Hazard Classification Report: The NAC Member shall submit an explosive hazard classification report (DI-SAFT-81299A) for each item that requires utilizing ARDEC capabilities to obtain Interim Hazard Classification (IHC) for shipment of R&D quantities of energetic materials and items in support of this Agreement. The NAC Member shall utilize the capability of ARDEC to obtain IHC for shipment of R&D quantities of energetic materials and items only on an as needed basis. In order to use this support, the NAC Member shall provide technical data (Explosive Hazard Classification Data) to ARDEC System Safety Group at least sixty (60) calendar days prior to shipment of the energetic materials or items. This will include the necessary data explained in Army Technical Bulletin (TB) 700-2 and DI-SAFT-81299A. DOT and UN Serial number information, along with packaging methods, will be based on Title 49, Code of Federal regulations (CFR). The NAC Member shall determine the explosive weight for quantity-distance determination in accordance with the guidance of paragraph 15.4C of AMC-R 385-100.
4. Pollution Prevention: Consideration should be given to alternative materials and processes in order to eliminate, reduce, or minimize hazardous waste being generated. This is to be accomplished while minimizing item cost and risk to item performance.
5. Environmental Compliance: All activities must be in compliance with Federal, State, and local environmental laws and regulations, Executive orders, treaties, and agreements. The NAC Member shall evaluate the environmental consequences and identify the specific types and amounts of hazardous waste being generated during projects under this Agreement.
6. Hazardous Waste Report: The NAC Member shall evaluate the environmental consequences and identify the specific types and amounts of hazardous waste being generated during this Agreement. NAC Members shall submit a Hazardous Waste Report in accordance with DI-MGMT-80899.
7. Disposal Instructions for Residual/Scrap Materials: The NAC Member shall dispose of all residual and scrap materials generated from this Agreement, including high explosives. The NAC Member shall specify the anticipated quantities, methods, and disposal costs.

Revision History

Rev	Date	Section	Paragraph	Summary of change	Authorized by
1.0	2/16/21			Initial issue, Changed document nr from MO SUB-001-A-OTA to F-840-008	Kathryn Bigelow