PRIME CONTRACT FLOWDOWN

HQ08452490034 (effective Feb 12,2024)

ARTICLE 5: OBLIGATION AND PAYMENT

5.1. Obligation

This Agreement is funded in accordance with the amount annotated in the SF 26 Section G. In no case shall the Government's financial obligations exceed the amount obligated on the Agreement or by amendment to this Agreement. The Government is not obligated to reimburse the COMPANY for expenditures in excess of the amount of obligated funds allotted by the Government. If a modification becomes necessary in performance of this Agreement, pursuant to Article 4.2, the Agreements Officer and the COMPANY shall execute a revised Schedule of Milestones and Payments for prospective milestones.

5.2. Payments

5.2.1. The Parties agree that payments will be made in accordance with completion of milestones. These payments reflect value received by the Government toward the accomplishment of the prototype project goals of this Agreement.

5.2.2. The COMPANY shall document the accomplishments of each completed milestone by submitting or otherwise providing the Milestone Report required by the SOW. After verification (written or otherwise) of the accomplishment of the milestone by the AOR, the COMPANY will submit their invoice through Wide Area Workflow (WAWF), as detailed in Attachment 2.

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

5.2.4. Payments will be made by the cognizant Defense Finance and Accounting Service office, as indicated in Attachment 2, within thirty (30) calendar days of an accepted invoice in WAWF. Attachment 2 details how to submit and process invoices through WAWF.

5.2.5. Payments shall be made in the amounts set forth in SF26 Section B, provided the AOR has verified the completion of the milestones.

5.2.6. The COMPANY shall maintain adequate records to account for all funding under this Agreement.

5.3. Financial Records and Reports:

5.3.1. The COMPANY shall maintain adequate records to account for Federal funds received under this Agreement and shall maintain adequate records to account for COMPANY Project Agreement funding provided under this Agreement. COMPANY relevant financial records are subject to examination or audit by or on behalf of the Comptroller General, DIU Contracting Activity, or other Government Official for a period not to exceed three years after expiration of the term of the Agreement. The Comptroller General, Agreements Officer or designee shall have direct access to sufficient records and information of any party to this agreement or any entity that participates in the performance of this agreement to ensure full accountability for all funding under this Agreement. Such audit, examination or access shall be performed during business hours on business days upon prior written notice and shall be subject to the security requirements of the audited party. Any audit required during the course of the program may be conducted by the Comptroller General or other Government Official using Government auditors or, at the request of COMPANY's external CPA accounting firm at the expense of the COMPANY. This requirement shall not apply with respect to a party or entity, or a subordinate element of a party or entity, that has not entered into any other agreement that provides for audit access by a Government entity in the year prior to the date of the agreement.

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

ARTICLE 7: CONFIDENTIAL INFORMATION

7.1. Exchange of Information

The Government may from time to time disclose Government Confidential Information to the COMPANY and its subcontractors or suppliers, in connection with a particular project, and the COMPANY and its subcontractors or suppliers, may from time to time disclose information that is Trade Secret or Confidential Information to the Government in connection with the OTA or performance thereunder. Neither the Government nor COMPANY or their subcontractors or suppliers shall be obligated to transfer Confidential Information or Trade Secrets independently developed by the Government or the COMPANY or their subcontractors or suppliers, absent an express written agreement between the Parties providing the terms and conditions for such disclosure.

7.2. 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 (no one shall disclose unless they have the right to do so), and that, unless otherwise agreed to by the Disclosing Party, Confidential 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 8, Article 9, and Article 10, provided that the duty to protect such "Confidential Information" and "Trade Secrets" shall not extend to materials or information 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 per Article entitled "Confidential Information" herein,

3. 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,

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,

7. 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.

7.3. Return of Proprietary Information

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

7.4. Term

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

7.5. Subcontracts

The Government and the COMPANY shall flow down the requirements of this Article to their respective personnel, agents, partners, and team members receiving such Confidential Information or Trade Secrets under this OTA.

ARTICLE 8: PUBLICATION AND ACADEMIC RIGHTS

8.1. Use of Information

Subject to the provisions of Article 7, Confidential Information, and this Article, Publication and Academic Rights, the COMPANY and the Government shall have the right to publish or otherwise disclose information and/or data developed by the Government and/or the respective COMPANY under this Agreement. The COMPANY and the Government (and its employees) shall include an appropriate acknowledgement of the sponsorship of the Research Projects by the Government and the COMPANY in such publication or disclosure. The Parties 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 Parties shall not be deemed authorized by Article 8.1, alone, to disclose any Confidential Information or Trade Secrets of the Government or the COMPANY. Nothing contained herein shall contradict or contravene any use of unlimited data rights obtained under Article 10 below.

8.2. Classified Research Projects

If a release of Confidential Information or Trade Secrets is for a classified Research 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. The Government will be responsible for the completion of the DD Form 254. The COMPANY member must complete the DD Form 441 and SF 328 and provide them to the Government through for review by the proper Government representatives, the Industrial Security Representative at the cognizant Defense Security Service (DSS) office for DD Form 441 and SF 328 and the requiring activity's local Security office for the DD Form 254.

8.3. Review or Approval of Technical Information for Public Release

8.3.1. At least 30 days prior to the scheduled release date, COMPANY shall submit to the Agreements Officer two copies of the information to be released. The Agreements Officer will route the information to the AOR and other appropriate parties for review and approval.

8.3.2. The AOR is hereby designated as the approval authority for the Agreements Officer for such releases.

8.3.3. Parties to this Agreement are responsible for ensuring that an 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 Other Transaction number HQ0845-24-9-0034 between the COMPANY and the Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon."*

8.3.4. Parties to this Agreement are also responsible for assuring that every publication of material based on or developed under this project 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."*

8.3.5. The COMPANY shall flow down these requirements to its partners and team members, at all tiers.

8.4. Filing of Patent Applications

During the course of any such thirty (30) calendar day period, the COMPANY and/or the Government shall provide notice to the Agreements Officer as to whether it desires that a patent application be filed on any invention disclosed in such materials. In the event that a COMPANY and/or the Government desires that such a patent be filed, the COMPANY or the Government proposing to publish or disclose such materials agrees to withhold publication and disclosure of such materials until the occurrence of the first of the following:

1. Filing of a patent application covering such invention, or

2. Written agreement, from the Agreements Officer and the COMPANY that no patentable invention is disclosed in such materials.

3. Further, during the course of any such thirty (30) calendar day period, the COMPANY shall notify the Agreements Officer and the Government if it believes any of its Confidential Information or Trade Secrets have been included in the proposed publication or disclosure and shall identify the specific Confidential Information or Trade Secrets that need to be removed from such proposed publication. The Government and the COMPANY agree to remove from the proposed publication or disclosure all such Confidential Information or Trade Secrets so identified by the COMPANY.

ARTICLE 9: PATENT RIGHTS

9.1. Allocation of Principal Rights

9.1.1. Unless the COMPANY notifies the Government, in accordance with subparagraph 2 below, that the COMPANY does not intend to retain title, the COMPANY shall retain the entire right, title, and interest throughout the world to each Subject Invention consistent with the provisions of this Article.

9.1.2. With respect to any Subject Invention in which the COMPANY retains title, the Government shall receive a nonexclusive, nontransferable, irrevocable, paid-up license to practice, or to have practiced (make, have made, use, have used, or import) the Subject Invention throughout the world on behalf of the United States for U.S. Government purposes and on behalf of any foreign government or international organization pursuant to any existing or future treaty or agreement with the United States in accordance with 35 U.S.C. § 209(d)(1) and 37 C.F.R. 404.7(a)(2)(i). The COMPANY shall record a confirmatory instrument of the Government's license to the Subject Invention with the United States Patent and Trademark Office.

9.1.3. In accordance with 37 C.F.R. 404.7(a)(2)(ii), the Government retains the right to grant licenses to third parties on reasonable terms when necessary to fulfill health, safety, or other needs of the public to the extent such needs are not being reasonably satisfied by COMPANY.

9.2. Marking of Data

Pursuant to Article 9.1 and Article 1 any Data delivered under this Agreement, except for Data subject to COMPANY's EULA, if any, shall be marked with the appropriate data rights markings and the COMPANY's name and address and include the following legend:

"Use, duplication, or disclosure is subject to the restrictions as stated in Agreement HQ0845-24-9-0034 between the Government and the COMPANY."

9.3. Lower Tier Agreements

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

ARTICLE 10: DATA RIGHTS

10.1. Allocation of Principal Rights

10.1.1. Data that will be delivered, furnished, or otherwise provided to the Government under this Agreement, in which the Government has previously obtained rights, shall be delivered, furnished, or provided with the pre-existing rights, unless (a) the parties have agreed otherwise, or (b) any restrictions on the Government's rights to use, modify, reproduce, release, perform, display, or disclose the data have expired or no longer apply.

10.1.2. Identification of Principal Rights: See Attachment 4.

10.1.3. Marking of Data: Any Data delivered under this Agreement shall be marked with the following legend:

> *"This data is being delivered as Commercial Computer Software or Technical Data, as defined in Agreement HQ0845-24-9-0034. Use, duplication, or disclosure is subject to the restrictions as stated in Agreement HQ0845- 24-9-0034 between the COMPANY and the Government."*

10.1.4. In the event that the COMPANY learns of a release to the Government of its unmarked Data that should have contained a restricted legend, the COMPANY will have the opportunity to cure such omission going forward by providing written notice to the Agreements Officer within six (6) months of the erroneous release.

10.2. Prior Technology

In the event it is necessary for the COMPANY to furnish the Government 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 Government and such Government Contractors or contract employees that the Government may hire on a temporary or periodic basis only for the purpose of carrying out the Government's responsibilities under this Agreement. Data protection will include proprietary markings and handling, and the signing of nondisclosure agreements by such Government Contractors or contract employees. The COMPANY shall not be obligated to provide Data that existed prior to, or was developed outside of this Agreement to the Government. Upon completion of activities under this Agreement, such Data will be disposed of as requested by the COMPANY.

10.3. Oral and Visual Information

If information which the COMPANY considers to embody trade secrets or to comprise commercial or financial information which is privileged or confidential is expressly disclosed orally or visually directly to the Government, the exchange of such information must be memorialized in tangible, recorded form and marked with a suitable notice or legend, and furnished to the Government within thirty (30) 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. If the Government reasonably determines that the memorialization of the exchange is insufficiently detailed to enable it to identify the privileged or confidential information, COMPANY shall provide additional detail at the Government's request, subject to restrictions on use and disclosure. Notwithstanding the forgoing, information that is disclosed without a restrictive legend or without an identifying statement at the time of the disclosure will nonetheless constitute Proprietary Information if by virtue of the information itself, or the circumstances under which it is disclosed, a reasonable person would understand that such information is Proprietary Information.

10.4. Disclaimer of Liability

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

a. Data not identified with a suitable notice or legend as set forth in this Article; nor

b. Information contained in any Data for which disclosure and use is restricted, if such information is or becomes generally known without breach of the above, is properly known to the Government or is generated by the Government independent of carrying out responsibilities under this Agreement, is rightfully received from a third party without restriction, or is included

ARTICLE 12: FOREIGN ACCESS TO TECHNOLOGY

This Article shall remain in effect during the term of the Agreement and for five (5) years thereafter.

12.1. General

The Parties agree that research findings and technology developments arising under this Agreement may constitute a significant enhancement to the national defense, and to the economic vitality of the United States. Accordingly, access to important technology developments under this Agreement by Foreign Firms or Institutions must be carefully controlled. The controls contemplated in this Article are in addition to, and are not intended to change or supersede, the provisions of the International Traffic in Arms Regulations (22 C.F.R. Part 120, et seq.), the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M), and the Department of Commerce's Export Administration Regulations (15 C.F.R. Part 730, et seq.).

12.2. Restrictions on Sale or Transfer of Technology to Foreign Firms or Institutions

12.2.1. In order to promote the national security interests of the United States and to effectuate the policies that underlie the regulations cited above, the procedures stated in Article 12.2.2, 12.2.3, and 12.2.4 below shall apply to any transfer of Technology. For purposes of this paragraph, a transfer includes a sale of the company, or sales or licensing of Technology. Transfers include:

a. Sales of products or components; or

b. Licenses of the software or documentation related to sales of products or components; or

c. Transfer to foreign subsidiaries of the COMPANY for purposes related to this Agreement; or

d. Transfer which provides access to Technology to a Foreign Firm or Institution which is an approved source of supply or source for the conduct of research under this Agreement provided that such transfer shall be limited to that necessary to allow the firm or institution to perform its approved role under this Agreement.

12.2.2. The COMPANY shall provide timely notice to the Government of any proposed transfers from the COMPANY of Technology developed under this Agreement to Foreign Firms or Institutions. If the Government determines that the transfer may have adverse consequences to the national security interests of the United States, the COMPANY, its vendors, and the Government shall jointly endeavor to find alternatives to the proposed transfer which obviate or mitigate potential adverse consequences of the transfer but which provide substantially equivalent benefits to the COMPANY.

12.2.3. In any event, the COMPANY shall provide written notice to the Agreements Officer of any proposed transfer to a foreign firm or institution at least sixty (60) calendar days prior to the proposed date of transfer. Such notice shall cite this Article and shall state specifically what is to be transferred and the general terms of the transfer. Within thirty (30) calendar days of receipt of the COMPANY's written notification, the Agreements Officer shall advise the COMPANY whether it consents to the proposed transfer. In cases where the Government does not concur or sixty (60) calendar days after receipt and the Government provides no decision, the COMPANY may utilize the procedures under Article 6, Disputes. No transfer shall take place until a decision is rendered.

12.2.4. In the event a transfer of Technology to Foreign firms or Institutions which is NOT approved by the Government takes place, the COMPANY shall (a) refund to the Government funds paid for the development of the Technology and (b) the Government shall have a non-exclusive, nontransferable, irrevocable, paid-up license to practice, or to have practiced on behalf of the United States the Technology throughout the world for Government and any and all other purposes, particularly to effectuate the intent of this Agreement. Upon request of the Government, the COMPANY shall provide written confirmation of such licenses.

12.3. Export Compliance

Each Party agrees to 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 COMPANY shall not export, directly, or indirectly, any products and/or technology, Confidential Information, Trade Secrets, or Classified and Unclassified Technical Data in violation of any U.S. Export laws or regulations.

12.4. Lower Tier Agreements

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

ARTICLE 17: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

17.1. Adequate Security. The COMPANY shall provide adequate security on all covered COMPANY information systems. To provide adequate security, the COMPANY shall implement, at a minimum, the following information security protections:

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

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

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

(2) The COMPANY shall maintain within the United States or outlying areas all Government data that is not physically located on Government premises, unless the COMPANY receives written notification from the Agreements Officer Representative to use another location.

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

17.1.2. For 'covered COMPANY 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 Article 17.1.1., the following security requirements apply:

a. Except as provided in Article 17.1.1.b, the covered COMPANY 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.

b. The National Institute of Standards and Technology Considerations:

(1) The COMPANY shall implement NIST SP 800-171, as soon as practical.

(2) The COMPANY shall submit requests to vary from NIST SP 800-171 in writing to the Agreements Officer, for consideration by the DoD CIO. The COMPANY 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 measures that may be implemented in its place.

(3) If the DoD CIO has previously adjudicated the COMPANY'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 Agreements Officer or Agreements Officer Representative when requesting its recognition under this agreement.

(4) If the COMPANY intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the COMPANY 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 Article 17.2 to 17.6 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.

17.1.3. Apply other information systems security measures when the COMPANY reasonably determines that information systems security measures, in addition to those identified in Article 17.1.2.b(1) and Article 17.1.2.b(2), 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.

17.2. Cyber Incident Reporting Requirement

17.2.1. When the COMPANY discovers a cyber incident that affects a covered COMPANY information system or the covered defense information residing therein, or that affects the COMPANY's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the agreement, the COMPANY shall—

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

b. Rapidly report any cyber incident(s) within 72 hours of discovery to DoD at http://dibnet.dod.mil

17.2.2. 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 http://dibnet.dod.mil.
17.2.3. Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the COMPANY 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 http://iase.disa.mil/pki/eca/Pages/index.aspx.

17.3. Malicious software. When the COMPANY or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) at this website: https://www.dc3.mil/ or in accordance with additional instructions provided by DC3 or the Agreements Officer or the Agreements Officer Representative. Do not send the malicious software to the Agreements Officer or Agreements Officer Representative.

17.4. Media preservation and protection. When a COMPANY discovers a cyber incident has occurred, the COMPANY shall preserve and protect images of all known affected information systems identified in Article 17.2.1.a 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.

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

17.6. Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the AO will request that the COMPANY provide all of the damage assessment information gathered in accordance with Article 17.4.

17.7. DoD safeguarding and use of COMPANY attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the COMPANY (or derived from information obtained from the COMPANY) under this clause that includes COMPANY attributional/proprietary information, including such information submitted in accordance with Article 17.2. To the maximum extent practicable, the COMPANY shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the COMPANY 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.

17.8. Use and release of COMPANY attributional/proprietary information not created by or for DoD

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

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).

17.9. Use and release of COMPANY attributional/proprietary information created by or for DoD
Information that is obtained from the COMPANY (or derived from information obtained from the COMPANY) under this Article that is created by or for the Government (including the information submitted pursuant to Article 17.2) is authorized to be used and released outside of the Government for purposes and activities authorized by Article 17.8 , 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.

17.10. Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the COMPANY'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.

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