Raytheon
Space and Airborne Systems

Flowdown Attachment
FDA-2019.181 R.2

(updated May 20, 2019)

OTA / Contract No.: FA8576-19-9-0001-OTA
DPAS Rating: None
SAS DUNS number: 799855812

The following customer contract requirements apply to this Purchase Order to the extent indicated below and are hereby incorporated into the Purchase Order by reference:

In all clauses listed herein terms shall be revised to suitably identify the party to establish Seller's obligations to Buyer and to the Government; and to enable Buyer to meet its obligations under its prime contract. Without limiting the generality of the foregoing, and except where further clarified or modified below, the term "Government" and equivalent phrases shall mean "Buyer", the term "Contracting Officer" shall mean "Buyer's Purchasing Representative", the term "Contractor" or "Offeror" shall mean "Seller", "Subcontractor" shall mean "Seller's Subcontractor" under this Purchase Order, and the term "Contract" shall mean this "Purchase Order". For the avoidance of doubt, the words "Government" and "Contracting Officer" do not change: (1) when a right, act, authorization or obligation can be granted or performed only by the Government or the prime contract Contracting Officer or duly authorized representative, such as in FAR 52.227-1 and FAR 52.227-2 and (2) when title to property is to be transferred directly to the Government. Seller shall incorporate into each lower tier contract issued in support of this Purchase Order all applicable FAR and DFARS clauses in accordance with the flow down requirements specified in such clauses.

CONFIDENTIAL AND/OR PROPRIETARY INFORMATION

A. Exchange of Information

Confidential and/or Proprietary Information includes information and materials of a Disclosing Party which are designated as confidential and/or proprietary or as a Trade Secret as defined in the Uniform Trade Secrets Act §1.4 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 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 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.

Trade Secret covers 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.

MCSC or cognizant Command may disclose its own Confidential and/or Proprietary Information to CMG for use by CMG Member Entity(ies) or PSH(s) in connection with particular Prototype Projects, and CMG, CMG Member Entity(ies) or PSH(s) may disclose information that is Confidential and/or Proprietary Information to the MCSC or cognizant Ordering Command in connection with a WP, project proposal, PA or performance thereunder.

Confidentiality and Authorized Disclosure: The Receiving Party agrees, to the extent permitted by law, that Confidential and/or Proprietary Information shall remain the property of the Disclosing Party, and that, unless otherwise agreed to by the Disclosing Party, Confidential and/or Proprietary Information 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 XVI - Patent Rights, and Article XXII - Data Rights and Copyrights. However, the duty to protect such Confidential and/or Proprietary Information 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, Agreement Between Marine Corps Systems Command (MCSC) and Consortium Management Group (CMG); 2) 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), 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 and/or Proprietary Information 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 to enable such Disclosing Party to seek a protective order or otherwise prevent disclosure of such information.

B. Return of Confidential and/or Proprietary Information Upon the request of CMG, MCSC or cognizant Ordering Command shall promptly return all copies and other tangible manifestations of the Confidential and/or Proprietary Information disclosed to MCSC or cognizant Ordering Command by CMG, PSHs or CMG Member Entity(ies). Upon request by the Government, CMG shall promptly return all copies and other tangible manifestations of the Confidential and/or Proprietary Information disclosed by the Government to CMG, PSHs or CMG Member Entity(ies). As used in this Section, tangible manifestations include human readable media, as well as, magnetic and digital storage media. If the return of all tangible manifestations is not practicable, the Party may propose an alternative process to ensure the verifiable destruction of such tangible manifestations. Such alternative process must be agreed upon in writing by both Parties prior to implementation.

C. Term
The obligations of the Receiving Party under this Article shall continue for a period of three (3) years after the expiration or termination of this Agreement.

D. Requirements Flow-down
MCSC or cognizant Ordering Command and CMG shall flow-down the requirements of this Article to their respective personnel, CMG Member Entity(ies), agents, and PSH(s) (including employees and subcontractors) at all levels, receiving such Confidential and/or Proprietary Information under this Agreement.

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

or indirectly, any products and/or technology, Confidential Information, Trade Secrets, or Classified and Unclassified Technical Data in violation of any U.S. Export laws or regulations.

B. Flow down
CMG Member Entity(ies), PSH(s), and their subcontractors include this Article, suitably modified, to identify all Parties, in all lower tier agreements. This Article shall, in turn, be included in all sub-tier subcontracts or other forms of lower tier agreements, regardless of tier.

TITLE AND DISPOSITION OF PROPERTY
The following provisions apply for all PAs:
A. Definitions
In this Article, "property" means any tangible personal property other than property consumed during the execution of work under this Agreement.
B. Title to Property
No significant items of property are expected to be acquired under this Agreement by CMG. Title to any item of property valued at $50,000 or less that is acquired by a PSH pursuant to a PA shall vest in the PSH upon acquisition with no further obligation of the Parties unless otherwise determined by the AO or OAO. Should any item of property with an acquisition value greater than $50,000 be required, CMG, at the request of the PSH(s) and on its behalf, shall obtain prior written approval of the AO or OAO. Upon written approval of the AO or OAO, title to this property also shall vest in the PSH(s) upon acquisition. The PSH(s) shall be responsible for the maintenance, repair, protection and preservation of all such property at its own expense. Property acquired pursuant to this clause shall not be considered as in exchange for services in performance of the Project but shall be considered a Government contribution to the Project.
C. Government Furnished Property
MCSC and Ordering Commands may provide CMG, the CMG Member Entity, or the PSH Government Furnished Property (GFP) to facilitate the performance of individual PPs. Such GFP will be specifically identified to a PP and subsequently incorporated into a resulting PA. The GFP shall be utilized only for the performance of that individual PP unless a specific exception is made in writing by the AO or OAO.

All property shall be returned at the end of the PA in the same condition as when received, except for reasonable wear and tear, or in accordance with the provisions of the PA regarding its use. CMG, the CMG Member Entity, or the PSH(s) shall obtain explicit written authorization for any transfer or disposition of GFP. All GFP transfer and disposition instructions will be made for each specific PA, as appropriate.

LIABILITY OF THE PARTIES
The following provisions apply for all PAs:
A. Waiver of Liability
With regard to the activities undertaken pursuant to this Agreement, no Party shall make any claim against the other, employees of the other, the other's Member Entity(ies), PSH(s), contractors, or subcontractors, or employees of the other's Member Entity(ies), PSH(s), contractors, or subcontractors for any injury to or death of its own employees or employees of its Member Entity(ies), PSH(s), contractors, or subcontractors, or for damage to or loss of its own property or that of its Member Entity(ies), PSH(s), contractors or subcontractors, whether such injury, death, damage or loss arises through negligence or otherwise, except in the case of willful misconduct.
B. 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.
C. Extension of Waiver of Liability

CMG agrees to extend the waiver of liability set forth above to PSH(s) at any tier under a PA by requiring them, by contract or otherwise, to agree to waive all claims described above against the Parties to this Agreement. CMG also agrees to flow-down the damages limitation set forth above to CMG Member Entity(ies) and PSH(s) at any tier.

D. Applicability

Notwithstanding the other provisions of this Article, this Waiver of Liability shall not be applicable to: 1) Claims between CMG (or CMG Member Entity(ies)) and MCSC or cognizant Ordering Command regarding a breach, noncompliance, or nonpayment of funds; 2) Claims for damage caused by willful misconduct; and 3) Intellectual property claims.

E. Limitation of Liability

In no event shall the liability of MCSC, Ordering Commands, CMG, PSH(s), or a CMG Member Entity(ies) or any other entity performing research activities under a PA exceed the amount obligated by the Government for that Project. If cost-sharing occurs, the liability of the PSH(s) or CMG Member Entity under a specific Project is limited to the amount committed as a Cash Contribution or In-kind Contribution by the PSH(s) or CMG Member Entity. Nothing in this Article shall be construed to create the basis of a claim or suit where none would otherwise exist. MCSC and Ordering Commands do not contemplate any unusually hazardous risks being associated with the awarded PPs, 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 MCSC, Ordering Commands or by CMG, on behalf of PSH(s) or proposing CMG Member Entity(ies), may pose a risk of such nature.

ARTICLE IX: PATENT RIGHTS

A. Allocation of Principal Rights

1. Unless CMG, the Performer or its SubContractors shall have notified AFLCMC/WNY, in accordance with subparagraph B.2 below, that the Performer or its SubContractors does not intend to retain title, CMG, the Performer or its SubContractors shall retain the entire right, title, and interest throughout the world to each Subject Invention consistent with the provisions of this Article. 2. With respect to any Subject Invention in which the Performer retains title, the Department of the Air Force shall have a nonexclusive, nontransferable, irrevocable, paid-up license to practice or have practiced on behalf of the United States the Subject Invention throughout the world.

B. Invention Disclosure, Election of Title, and Filing of Patent Application

1. CMG, the Performer or its SubContractors shall disclose each Subject Invention to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY within four (4) months after the inventor discloses it in writing to his company personnel responsible for patent matters. The disclosure to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY shall be in the form of a written report and shall identify the Agreement and circumstances under which the Invention was made and the identity of the inventor(s). It shall be sufficiently complete in technical detail to convey a clear understanding, to the extent known at the time of the disclosure, of the nature, purpose, operation, and the physical, chemical, biological, or electrical characteristics of the Invention. The disclosure shall also identify any publication, sale, or public use of the invention and whether a manuscript describing the Invention has been submitted and/or accepted for publication at the time of disclosure.

2. If CMG, the Performer or its SubContractors determines that it does not intend to retain title to any such Invention, CMG, the Performer or its SubContractors shall notify Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNYBBA, in writing, within eight (8) months of disclosure to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNYBBA. However, in any case where publication, sale, or public use has initiated the one-year statutory period wherein valid patent protection can still be obtained in the United States, the period for such notice may be shortened by Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY to a date that is no more than sixty (60) calendar days prior to the end of the statutory period.

3. CMG, the Performer or its SubContractors shall file its initial patent application on a Subject Invention to which it elects to retain title within one (1) year after election of title or, if earlier, prior to the end of the statutory period wherein valid patent protection can be obtained in the United States after a publication, or sale, or public use. CMG, the Performer or its SubContractors may elect to file patent applications in additional countries, including the European Patent Office and the Patent Cooperation Treaty, within either ten (10) months of the corresponding

initial patent application or six (6) months from the date permission is granted by the Commissioner for Patents to file foreign patent applications, where such filing has been prohibited by a Secrecy Order.

4. CMG, the Performer or its SubContractors shall notify Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY of any decisions not to continue the prosecution of a patent application, pay maintenance fees, or defend in a reexamination or opposition proceedings on a patent, in any country, not less than thirty (30) calendar days before the expiration of the response period required by the relevant patent office.

5. Requests for extension of the time for disclosure election, and filing under Article VII, may be granted at Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY discretion after considering the circumstances of CMG, the Performer or its SubContractors and the overall effect of the extension.

6. CMG, the Performer or its SubContractors shall submit to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY annual listings of Subject Inventions. At the completion of the Agreement, the Performer shall submit a comprehensive listing of all subject inventions identified during the course of the Agreement and the current status of each.

C. Conditions When the Government May Obtain Title

Upon Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNYBBA, the Performer shall convey title to any Subject Invention to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY under any of the following conditions: 1. If CMG, the Performer or its SubContractors fails to disclose or elects not to retain title to the Subject Invention within the times specified in Paragraph B of this Article; however, Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY may only request title within sixty (60) calendar days after learning of the failure of the Performer to disclose or elect within the specified times; 2. In those countries in which CMG, the Performer or its SubContractors fails to file patent applications within the times specified in Paragraph B of this Article; however, if CMG, the Performer or its SubContractors has filed a patent application in a country after the times specified in Paragraph B of this Article, but prior to its receipt of the written request Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY, the Performer shall continue to retain title in that country; or 3. In any country in which CMG, the Performer or its SubContractors decides not to continue the prosecution of any application for, to pay the maintenance fees on, or defend in reexamination or opposition proceedings on, a patent on a Subject Invention.

D. Minimum Rights to CMG, the Performer or its SubContractors and Protection of the Performer's Right to File

1. CMG, the Performer or its SubContractors shall retain a nonexclusive, royalty-free license throughout the world in each subject invention to which the Government obtains title, except if the Performer fails to disclose the Subject Invention within the times specified in Paragraph B of this Article. CMG, the Performer or the SubContractors's license extends to its domestic subsidiaries and affiliates, including Canada, if any, and includes the right to grant licenses of the same scope to the extent that CMG, the Performer or its SubContractors was legally obligated to do so at the time the Agreement was awarded. The license is transferable only with the approval of AFLCMC/WNY, except when transferred to the successor of that part of the business to which the Subject Invention pertains AFLCMC/WNY approval for license transfer shall not be unreasonably withheld.

2. CMG, the Performer or its SubContractors's domestic license may be revoked or modified by AFLCMC/WNY to the extent necessary to achieve expeditious practical application of the Subject Invention pursuant to an application for an exclusive license submitted consistent with appropriate provisions at 37 C.F.R. Part 404. This license shall not be revoked in that field of use or the geographical areas in which the Performer has achieved practical application and continues to make the benefits of the Subject Invention reasonably accessible to the public. The license in any foreign country may be revoked or modified at the discretion of Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY to the extent CMG, the Performer or its SubContractors its licensees, or the subsidiaries or affiliates have failed to achieve practical application in that foreign country.

3. Before revocation or modification of the license, Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY shall furnish CMG, the Performer or its SubContractors a written notice of its intention to revoke or modify the license, and the Performer shall be allowed thirty (30) calendar days (or such other time as may be authorized for good cause shown) after the notice to show cause why the license should not be revoked or modified.

E. Action to Protect the Government's Interest

1. CMG, the Performer or its SubContractors agrees to execute or to have executed and promptly deliver to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY all instruments necessary to (i) establish or confirm the rights the Government has throughout the world in those Subject Inventions to which CMG, the

Performer or its SubContractors elects to retain title, and (ii) convey title to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY when requested under Paragraph C of this Article and to enable the Government to obtain patent protection throughout the world in that Subject Invention.

2. CMG, the Performer or its SubContractors agrees to require by written agreement with its employees, other than clerical and non-technical employees, to disclose promptly in writing to personnel identified as responsible for the administration of patent matters and in a format suggested by CMG, the Performer or its SubContractors each Subject Invention made under this Agreement in order that CMG, the Performer or its SubContractors can comply with the disclosure provisions of Paragraph B of this Article. CMG, the Performer or its SubContractors shall instruct employees, through employee agreements or other suitable educational programs, on the importance of reporting inventions in sufficient time to permit the filing of patent applications prior to United States or foreign statutory bars.

3. CMG, the Performer or its SubContractors shall include, within the specification of any United States patent application and any patent issuing thereon covering a subject invention, the following statement: This invention was made with Government support under Agreement No. FA8576-19-9-0001 awarded by Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNKF. The Government has certain rights in the invention.

F. Lower Tier Agreements

CMG, the Performer or its SubContractors shall include this Article, suitably modified, in all subcontracts or lower tier agreements, regardless of tier, for experimental, developmental, or research work.

G. Reporting on Utilization of Subject Inventions

1. CMG, the Performer or its SubContractors agrees to submit, during the term of the Agreement, an annual report on the utilization of a Subject Invention or on efforts at obtaining such utilization that are being made by CMG, the Performer or its SubContractors or its licensees or assignees. Such reports shall include information regarding the status of development, date of first commercial sale or use, gross royalties received by CMG, the Performer or its SubContractors, and such other data and information as the agency may reasonably specify. CMG, the Performer or its SubContractors also agrees to provide additional reports as may be requested by AFLCMC/WNY in connection with any march-in proceedings undertaken by AFLCMC/WNY in accordance with Paragraph I of this Article. AFLCMC/WNY agrees it shall not disclose such information to persons outside the Government without permission of CMG, the Performer or its SubContractors, unless required by law.

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

H. Preference for American Industry

Notwithstanding any other provision of this clause, CMG, the Performer or its SubContractors agrees that it shall not grant to any person the exclusive right to use or sell any Subject Invention in the United States unless such person agrees that any product embodying the Subject Invention or produced through the use of the subject invention shall be manufactured substantially in the United States. However, in individual cases, the requirements for such an agreement may be waived by Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY upon a showing by CMG, the Performer or its SubContractors that reasonable but unsuccessful efforts have been made to grant licenses on similar terms to potential licensees that would be likely to manufacture substantially in the United States or that, under the circumstances, domestic manufacture is not commercially feasible.

I. March-in Rights

CMG, the Performer or its SubContractors agrees that, with respect to any Subject Invention in which it has retained title, Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY has the right to require the Performer, an assignee, or exclusive licensee of a Subject Invention to grant a nonexclusive license to a responsible applicant or applicants, upon terms that are reasonable under the circumstances, and if CMG, the Performer or its SubContractors, assignee, or exclusive licensee refuses such a request, Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY has the right to grant such a license itself if Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY determines that: 1. Such action is necessary because CMG, the Performer or its SubContractors or assignee has not taken effective steps, consistent with the intent of this Agreement, to achieve practical application of the Subject Invention; 2. Such action is necessary to alleviate health or safety needs which are not reasonably satisfied by CMG, the Performer or its SubContractors,

assignee, or their licensees; 3. Such action is necessary to meet requirements for public use and such requirements are not reasonably satisfied by CMG, the Performer or its SubContractors, assignee, or licensees; or 4. Such action is necessary because the agreement required by Paragraph H of this Article has not been obtained or waived or because a licensee of the exclusive right to use or sell any Subject Invention in the United States is in breach of such Agreement.

ARTICLE X DATA RIGHTS

A. Allocation of Principal Rights

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

2. With respect to Data developed or generated under this Agreement related to the Airborne HF Radio Modernization Prototype, , the Government shall receive the data rights as outlined in the Performer's SOW, which includes Government Purpose and Unlimited Rights, as defined in Article III, Paragraph B.

3. With respect to all non-commercial technical data delivered pursuant to Attachment A under the Agreement, the Government shall receive data rights outlined in the Performer's SOW, which includes Government Purpose and Unlimited Rights.

4. March-In Rights

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

(b) To facilitate any potential deliveries, CMG and the Performer agrees to retain and maintain in good condition until five years after completion or termination of this Agreement, all Data necessary to achieve practical application of any Subject Invention as defined in Article III, Section B of this Agreement.

B. Marking of Data

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

Use, duplication, or disclosure is subject to the restrictions as stated in Agreement FA8576-19-9-0001 between the Government, CMG and the Performer.

C. Lower Tier Agreements

The Performer 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 XIFOREIGN ACCESS TO TECHNOLOGY

This Article shall remain in effect during the term of the Agreement and for 25 years thereafter.

A. 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 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.).

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

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 subparagraphs B.2, B.3, and B.4 below shall apply to any transfer of Technology. For purposes of this paragraph, a transfer includes a sale of the company, and sales or licensing of Technology. Transfers do not include: a. Sales of products or components; or b. Licenses of software or documentation related to sales of products or components; or c. Transfer to foreign subsidiaries of the Performer 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.

2. CMG and the Performer shall provide timely notice to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY of any proposed transfers from CMG and the Performer of Technology developed under this Agreement to Foreign Firms or Institutions. If Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY determines that the transfer may have adverse consequences to the national security interests of the United States, CMG and the Performer, its vendors, and Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY 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 CMG and the Performer.

3. In any event, CMG and the Performer shall provide written notice to the AFLCMC/WNYAOR and the AFLCMC/WNKF AO 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 Performer's written notification, the AFLCMC/WNKF AO shall advise the Performer whether it consents to the proposed transfer. In cases where Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY does not concur or sixty (60) calendar days after receipt and Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY

provides no decision, the Performer may utilize the procedures under Article VIII, Disputes. No transfer shall take place until a decision is rendered.

4. In the event a transfer of Technology to Foreign Firms or Institutions which is NOT approved by Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY takes place, CMG and the Performer shall (a) refund to Air Force Life Cycle Management Center Robins Air Force Base, AFLCMC/WNY 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, CMG and the Performer shall provide written confirmation of such licenses.

C. Lower Tier Agreements

CMG and the Performer 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 XIV SECURITY

The Contractor shall comply with guidelines specified on the DD Form 254 (Attachment D). Access to classified spaces and material and generation of classified material shall be in accordance with the DD Form 254, NISPOM and the NSWCDD Command Security Manual.

SECURITY REQUIREMENTS

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DOD 5220.22-M); and (2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of the basic contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS

(a) Definitions. As used in this clause--

"Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.
"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).
"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
"Safeguarding" means measures or controls that are prescribed to protect information systems.
(b) Safeguarding requirements and procedures.
(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls: (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute. (iii) Verify and control/limit connections to and use of external information systems. (iv) Control information posted or processed on publicly accessible information systems. (v) Identify information system users, processes acting on behalf of users, or devices. (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices. (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. (xii) Identify, report, and correct information and information system flaws in a timely manner. (xiii) Provide protection from malicious code at appropriate locations within organizational information systems. (xiv) Update malicious code protection mechanisms when new releases are available. (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.
(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

DISCLOSURE OF INFORMATION

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless— (1) The Agreement Officer has given prior written approval; (2) The information is otherwise in the public domain before the date of release; or (3) The information results from or arises during the performance of a project that involves no covered defense information as defined in Safeguarding Covered Defense Information and Cyber Incident Reporting) and has been scoped and negotiated by the by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering

Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008.
(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.
(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION

(a) Definitions. As used in this clause--
"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.
"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 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.
"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
"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.
"Technical information" means technical data or computer software, as those terms are defined in the clause at 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) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause): (1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause Safeguarding Covered Defense Information and Cyber Incident Reporting, and shall not be used for any other purpose. (2) The Contractor shall protect the information against unauthorized release or disclosure. (3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information. (4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the nondisclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause. (5) A breach of these obligations or restrictions may subject the Contractor to-- (i) Criminal, civil, administrative, and contractual actions

in law and equity for penalties, damages, and other appropriate remedies by the United States; and (ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) Subcontracts. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

(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 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 for all covered defense information 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 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 http://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 http://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 http://iase.disa.mil/pki/eca/Pages/index.aspx.

(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.

The following clauses apply to all Purchase Orders, including those for "Commercial Item(s)", as defined in FAR 2.101:

DFARS 252.204-7008	Compliance with Safeguarding Covered Defense Information Controls. (Dec. 2015)	Buyer's contract contains Compliance with Safeguarding Covered Defense Information Controls. (Dec. 2015); SELLER SHALL INDICATE WHETHER DEVIATION FROM ANY OF THE SECURITY REQUIREMENTS IN THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800-171, "PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, http://dx.doi.org/10.6028/NIST.SP.800-171 THAT IS IN EFFECT AT THE TIME THE PRIME CONTRACT SOLICITATION IS ISSUED IS ANTICIPATED IN THE PERFORMANCE OF THE PURCHASE ORDER BY SELLER OR CONTRACTORS AT ANY TIER.
DFARS 252.204-7009	Limitations on the use or disclosure of third-party contractor reported cyber incident information (Oct 2016)	Applicable to Purchase Orders for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items.
FAR 52.204-2	Security Requirements. (Aug 1996)	Applicable to Purchase Orders that involve access to classified information. Any reference to the Changes clause is excluded.
FAR 52.204-21	Basic Safeguarding of Covered Contractor Information Systems. (June 2016)	Applies to all Purchase Orders (including Purchase Orders for the acquisition of commercial items, other than commercially available off-the-shelf items) in which the Seller may have Federal contract information residing in or transiting through its information system.
DFARS 252.204-7000	Disclosure of Information. (Oct 2016)	Applicable to Purchase Orders when the seller will have access to or generate unclassified information that may be sensitive and inappropriate for release to the public.
DFARS 252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)	Applicable to all 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.

In addition to the clauses listed above, the following clauses apply to all Purchase Orders for goods or services not meeting the definition of a "Commercial Item" in FAR 2.101:

None identified.