Raytheon
Space and Airborne Systems

Flowdown Attachment
FDA-2019.107

Prime Contract: W15QKN-17-9-5555
OTA / Contract No.: 17410
DPAS Rating:
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.

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

Counterfeit Parts Prevention

Definitions

(1) Authentic shall mean (A) genuine; (B) purchased from the Original Equipment Manufacturer ("OEM"), Original Component Manufacturer ("OCM") or through the OEM's/OCM's authorized dealers; and (C) manufactured by, or at the behest and to the standards of, the manufacturer that has lawfully applied its name and trademark for that model/version of the material.

(2) Authorized Dealer — A dealer or distributor that purchases directly from the OEM or OCM and is authorized or franchised by the OEM or OCM to sell or distribute the OEM's/OCM's products.

(3) Counterfeit Part — A part that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized part of the legally authorized source. This definition includes used parts represented as new parts.

(4) Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM) — An organization that designs and/or engineers a part or equipment and is pursuing or has obtained the intellectual property rights to that part or equipment.

(5) Non-Franchised Source — Any source that is not authorized by the OEM or OCM to sell its product lines. Non-franchised sources may also be referred to as brokers or independent distributors.

(6) Suspect Counterfeit Part — A part that BUYER becomes aware, or has reason to suspect, meets the definition of "counterfeit part", as defined above. For purposes of this document, the terms "counterfeit part" and "suspect counterfeit part" will be used interchangeably. If any individual part from a lot is determined to be counterfeit or suspect counterfeit, the entire lot of parts will be considered to be suspect counterfeit.

H.25.2 Terms and Conditions

(1) SELLER represents and warrants that only new and authentic materials (including embedded software and firmware) are used in products required to be delivered to BUYER and that the Work delivered contains no Counterfeit Parts. No material, part, or component other than a new and authentic part is to be used unless approved in advance in writing by BUYER. To further mitigate the possibility of the inadvertent use of Counterfeit Parts, SELLER shall only purchase authentic parts/components directly from the Original Equipment Manufacturers ("OEMs"), Original Component Manufacturers ("OCMs") or through the OEM's/OCM's authorized dealers. SELLER represents and warrants to BUYER that all parts/components delivered under this Subcontract are traceable back to the OEM/OCM.
SELLER must maintain and make available to BUYER at BUYER's request, OEM/OCM documentation that authenticates traceability of the parts/components to the applicable OEM/OCM. Purchase of parts/components from Non-Franchised Sources is not authorized unless first approved in writing by BUYER. SELLER must present complete and compelling support for its request and include in its request all actions to ensure the parts/components thus procured are legitimate parts. BUYER's approval of SELLER request(s) does not relieve SELLER's responsibility to comply with all Subcontract requirements, including the representations and warranties in this Section H.25.2(1).
(2) SELLER shall maintain a documented system (policy, procedure, or other documented approach) that provides for prior notification and BUYER's approval before parts/components are procured from sources other than OEMs/OCMs or the OEM's/OCM's authorized dealers. SELLER shall provide copies of such documentation for its system for BUYER's inspection upon BUYER's request.
(3) SELLER must maintain a counterfeit detection process that complies with SAE standard AS5553, Counterfeit Electronic Parts, Avoidance, Detection, Mitigation, and Disposition.
(4) If it is determined that counterfeit parts or suspect counterfeit parts were delivered to BUYER by SELLER, the suspect counterfeit parts will not be returned to the supplier. BUYER reserves the right to quarantine any and all suspect counterfeit parts it receives and to notify the Government Industry Data Exchange Program (GIDEP) and other relevant government agencies. SELLER shall promptly reimburse BUYER for the full cost of the suspect counterfeit parts and SELLER assumes responsibility and liability for all costs associated with the delivery of suspect counterfeit parts, including, but not limited to, costs for identification, testing, and any corrective action required to remove and replace the suspect counterfeit parts. The remedies in this section shall apply regardless of whether the warranty period or guarantee period has ended, and are in addition to any remedies available at law or in equity.
(5) If the procurement of materials under this Subcontract is pursuant to, or in support of, a contract, subcontract, or task order for delivery of goods or services to the Government, the making of a materially false, fictitious, or fraudulent statement, representation or claim or the falsification or concealment of a material fact in connection with this Subcontract may be punishable, as a Federal felony, by up to five years' imprisonment and/or substantial monetary fines. In addition, trafficking in counterfeit goods or services, to include military goods or services, constitutes a Federal felony offense, punishable by up to life imprisonment and a fine of fifteen million dollars.
(6) SELLER shall flow the requirements of this section ("COUNTERFEIT PARTS PREVENTION") to its subcontractors and suppliers at any tier for the performance of this Subcontract.

Confidential and/or Proprietary Information

A. Definitions
"Disclosing Party" means CMG, C5 PAH(s), C5's Member Entity(ies), or the Government who discloses Confidential and/or Proprietary Information as contemplated by the subsequent paragraphs.
"Receiving Party" means CMG, C5 PAH(s), C5's Member Entity(ies), or the Government who receives Confidential and/or Proprietary Information disclosed by a Disclosing Party.
"Confidential and/or Proprietary Information" means information and materials of a Disclosing Party which are designated as confidential and/or proprietary or as a Trade Secret in writing by such Disclosing Party, whether by letter or by use of an appropriate stamp or legend, prior to or at the same time any such information or materials are disclosed by such Disclosing Party to the Receiving Party. Notwithstanding the foregoing, materials and other information which are orally, visually, or electronically disclosed by a Disclosing Party, or are disclosed in writing without an appropriate letter, stamp, or legend, shall constitute Confidential and/or Proprietary Information or a Trade Secret if such Disclosing Party, within 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" means all forms and types of financial, business, scientific, technical, economic or
engineering or otherwise proprietary information, including, but not limited to, patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

--The owner thereof has taken reasonable measures to keep such information secret; and
--The information derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means, by the public.

B. Exchange of Information: The Government may from time to time disclose Government Confidential and/or Proprietary Information to CMG for use by C5 Member Entity(ies) or C5 Project Agreement Holders (PAHs) in connection with particular Prototype Projects, and CMG, C5's Member Entity(ies) or C5's PAH(s) may from time to time disclose information that is Confidential and/or Proprietary Information to the Government in connection with a White Paper, Project Proposal, TDL, Project Agreement or performance thereunder.

C. 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 X - Patent Rights, and Article XI - 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,
(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 so as to enable such Disclosing Party to seek a protective order or otherwise prevent disclosure of such information.

D. Return of Confidential and/or Proprietary Information: Upon the request of CMG, the Government shall promptly return all copies and other tangible manifestations of the Confidential and/or Proprietary Information disclosed to the Government by CMG or C5 PAHs or C5 Member Entities. 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 or C5 PAHs or C5 Member Entities.

As used in this Section, tangible manifestations include human readable media as well as magnetic and digital storage media. In the event that 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.

E. 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.

F. The Government and CMG shall flow down the requirements of this Article to their respective personnel, C5 Member Entities, agents and C5 PAH(s) (including employees and subcontractors) at all levels, receiving such Confidential and/or Proprietary Information under this OTA.

Patent Rights

A. Definitions

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

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

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

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

"Background Invention" means any invention made by the SELLER, or their subcontractors of any tier, prior to performance of the Agreement or outside the scope of work performed under this Agreement.

B. Allocation of Principal Rights

The SELLER shall retain the entire right, title, and interest throughout the world to each subject invention consistent with the provisions of this Article, and 35 U.S.C § 202. With respect to any subject invention in which the SELLER retains title, the Government shall have a non-exclusive, nontransferable, irrevocable, paid-up license to practice or have practiced on behalf of the United States the subject invention throughout the world. The SELLER may elect to provide full or partial rights that it has retained to other parties.

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

1. The SELLER shall disclose each subject invention to the Government within four (4) months after the inventor discloses it in writing to his Seller personnel responsible for patent matters. The disclosure to the Government shall be in the form of a written report and shall identify the Agreement 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 for publication and, if so, whether it has been accepted for publication at the time of disclosure.

2. If the SELLER determines that it does not intend to retain title to any such invention, the SELLER shall notify the AO, in writing, within nine (9) months of disclosure to the ACC-NJ Contracting Activity. However, in any case where public disclosure by the inventor has initiated the one (1) year statutory period wherein valid patent protection can still be obtained in the United States, the period for such notice shall be in no event less than 60 days prior to the one (1) year statutory bar date.

3. The SELLER 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 a publication, or sale, or public use. The SELLER 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 of Patents and Trademarks to file foreign patent applications, where such filing has been prohibited by a Secrecy Order.

4. After considering the position of the SELLER, a request for extension of the time for disclosure election, and filing under this Article IX, paragraph C, may be approved by ACC-NJ Contracting Activity, which ACC-NJ approval shall not be unreasonably withheld.

D: Conditions When the Government May Obtain Title

Upon the Government's written request, the SELLER shall convey title to any Subject Invention to the Government under any of the following conditions:

1. If the SELLER fails to disclose (and does not correct such failure within thirty (30) days after notice of such failure from the Government) or elects not to retain title to the Subject Invention within the times specified in Article IX, paragraph C.; provided, that the Government may only request title within sixty (60) calendar days after learning of the failure of the SELLER to disclose or elect within the specified times.

2. In those countries in which the SELLER fails to file patent applications within the times specified in Article IX. paragraph C; provided, that if the SELLER has filed a patent application in a country after the times specified in Article IX, paragraph C, but prior to its receipt of the written request by the Government, the SELLER shall continue to retain title in that country; or

3. In any country in which the SELLER 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.

E: Minimum Rights to the SELLER and Protection of the SELLERs Right to File:

1. The SELLER shall retain a nonexclusive, royalty-free license throughout the world in each Subject Invention to which the Government obtains title. The SELLER license extends to the domestic (including Canada) subsidiaries and affiliates, if any, within the corporate structure of which the SELLER is a party and includes the right to grant licenses of the same scope to the extent that the SELLER was legally obligated to do so at the time the Agreement was awarded. The license is transferable only with the approval of the Government, except when transferred to the successor of that part of the business to which the invention pertains. The Government approval for license transfer shall not be unreasonably withheld.

2. The SELLER domestic license may be revoked or modified by the Government 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 CFR Part 401. This license shall not be revoked in that field of use or the geographical areas in which the SELLER has achieved practical application and continues to make the benefits of the invention reasonably accessible to the public. The license in any foreign country may be revoked or modified at the discretion of the Government to the extent the SELLER, 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, the Government shall furnish the SELLER a written notice of its intention to revoke or modify the license, and the SELLER 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.

F. Action to Protect the Governments Interest:

1. The SELLER agrees to execute or to have executed and promptly deliver to the Government all instruments necessary to: 1. establish or confirm the rights the Government has throughout the world in those Subject Inventions to which the SELLER elects to retain title; and 2. convey title to the Government when requested under this Article and to enable the Government to obtain patent protection throughout the world in that Subject Invention.

2. The SELLER agrees to require, by written agreement, its employees, other than clerical and nontechnical employees, to disclose promptly in writing to personnel identified, as responsible for the administration of patent matters, and in a format suggested by the SELLER, each Subject Invention made under this Agreement in order that the SELLER can comply with the disclosure provisions under this Article. The SELLER 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 U. S. or foreign statutory bars.

3. The SELLER shall notify the Government 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.

4. The SELLER 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. INSERT CONTRACT NUMBER awarded by USACC-NJ. The Government has certain rights in the invention.”

G. Lower Tier Agreements: The SELLER 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.

H. Reporting on Utilization of Subject Inventions: The SELLER agrees to submit, during the term of the Agreement, an annual report on the utilization of a Subject Invention or on efforts at obtaining such utilization that are being made by the SELLER or licensees or assignees of the inventor. Such reports shall include information regarding the status of development, date of first commercial sale or use, gross royalties received by the SELLER, and such other data and information as the agency may reasonably specify. The SELLER also agrees to provide additional reports as may be requested by the Government in connection with any march-in proceedings undertaken by the Government in accordance with paragraph G of this Article. Consistent with 35 U.S.C. 206, the Government agrees it shall not disclose such information to persons outside the Government without permission of the SELLER.

I. Preference for American Industry: Notwithstanding any other provision of this Article, the SELLER agrees that it shall not grant to any person the exclusive right to use or sell any Subject Invention in the United States or Canada 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 or Canada. However, in individual cases, the requirements for such an agreement may be waived by the Government upon a showing by the SELLER 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.

Data Rights and Copyrights

A. Definitions

“Commercial Computer Software” as used in the Article is defined in DFARS 252-227-7014(a)(1) (Jun 1995).

“Commercial Computer Software License” means the license terms under which Commercial Computer Software is sold or offered for sale, lease or license to the general public.

“Computer Data Base” as used in this Agreement, means a collection of data recorded in a form capable of being processed by a computer. The term does not include computer software.

“Computer program” as used in this Agreement means a set of instructions, rules, or routines in a form that is capable of causing a computer to perform a specific operation or series of operations.

“Computer software” as used in this Agreement means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated or recompiled. Computer software does not include computer data bases or computer software documentation.

“Computer software documentation” means owner’s manuals, user’s manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" as used in this Article of this Agreement, means computer software, computer software documentation, form, fit and function data, and technical data as defined in this Article.
"Form, fit and function data" means technical data that describes the required overall physical, functional and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items.
"Government purpose rights" means the rights to use, modify, duplicate or disclose the "Data" licensed with such rights under this Agreement within the Government for United States Government purposes only; and to release or disclose data outside the Government to any authorized persons pursuant to an executed non-disclosure agreement for such persons' use, modification, or reproduction for United States Government purposes only. United States Government purposes include Foreign Military Sales purposes and competitive re-procurement.
"Limited rights" as used in this Article is as defined in DFARS 252.227-7013(a)(14).
"Restricted rights" as used in this Article is as defined in DFARS 252.227-7014(a)(15).
"Specially Negotiated License Rights" are those rights to Data that have been specifically negotiated between the Government and the SELLER.
"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.
"Unlimited rights" means the rights to use, modify, duplicate, release, or disclose Data, in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.

B. Data Categories:
1. Category A is Data developed and paid for totally by non-governmental funds, whether pre-existing or concurrently developed proprietary data, trade secret data, or data related to SELLER products. The SELLER retains all rights to Category A Data.
2. Category B is any Data developed under this Agreement, using Government funds, which cannot be disclosed without compromising the Category A data.
3. Category C is any SELLER developed Data, excluding Category A and B data, developed during the performance of work under this Agreement.
4. Category D is third party proprietary data used in performance of work under this Agreement, including but not limited to, technical data, software, trade secrets and mask works.
Any Data developed outside of this Agreement with Government funding in whole or in part under a Government agreement, contract or subcontract shall have the rights negotiated under such prior agreement, contract or subcontract; the Government shall get no additional rights in such Data under this Agreement.

C. Allocation of Principal Rights
1. The parties agree that in consideration for the Government's funding, and in lieu of any Government rights to Category A, B or D data (except as contained in paragraph 4 below), the SELLER intends to reduce to practical application materials and processes developed under this Agreement.
2. No deliveries to the Government of Category A and B data are contemplated or required under this Agreement. The Government reserves the right to negotiate certain rights in Category A and B data with the owner of the data.
3. The Government shall have immediate and irrevocable Government Purpose Rights to all Category C Data.
4. The SELLER shall deliver third-party computer software, Category D data, as required for the performance or operation of other computer software required to be delivered in the performance of this Agreement, with such rights as it is able to negotiate with the software vendor.
5. 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.

D. Identification of Principal Rights. Identify Data Rights Assertions below:

TYPE-PROPERTY NUMBER-RIGHTS ASSERTION
1. Application: provide date and type of application/title with brief description
2. Patent: provide patent no. and/or entity identifier/number
3. Rights: provide the type/category of right asserted
E. Marking of Data: Any Data delivered under this Agreement/PA shall be marked with the following legend:

"This data is being delivered as Category (insert category) Data, as defined in Agreement W15QKN-17-9-5555. Use, duplication, or disclosure is subject to the restrictions as stated in Agreement W15QKN-17-9-5555 between C5 and the Government."
In the event that the PAH learns of a release to the Government of its unmarked Data that should have contained a restricted legend, the PAH will have the opportunity to cure such omission going forward by providing written notice to the AO within six (6) months of the erroneous release.

E. Marking of Data: Any Data delivered under this Agreement shall be marked with the following legend: "This data is being delivered as Category (insert category) Data, as defined in Agreement ENTER AGREEMENT NUMBER. Use, duplication, or disclosure is subject to the restrictions as stated in Agreement ENTER AGREEMENT NUMBER between the SELLER and the Government."

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

F. Prior Technology
1. In the event it is necessary for the SELLER 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 SELLER 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 SELLER.
2.Oral and Visual Information: If information which the SELLER 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, SELLER shall provide addition detail at the Government's request, subject to restrictions on use and disclosure.
3. Disclaimer of Liability: 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 in Data which the SELLER has furnished, or is required to furnish to the Government without restriction on disclosure and use.

Notwithstanding F.3.(a) of this Article above, if the SELLER cures the omission of the suitable notice or legend, the restrictions, and related liability for disclosure and use of such information shall apply after cure unless it is then unrestricted under F.3(b) of this Article above.

G. Copyright
The SELLER reserves the right to protect by copyright works developed under this Agreement. All such copyrights will be in the name of the SELLER or the author, as determined by SELLER policies. The SELLER hereby grants to the U.S. Government a non-exclusive, non-transferable, royalty-free, fully paid-up license to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, for governmental purposes, any copyrighted materials developed (excluding Data) under this Agreement to which it owns the copyright, and to authorize others to do so.

H. Lower Tier Agreements
The SELLER shall include this Article, suitably modified to identify the parties, in all, subcontracts or lower tier agreements, regardless of tier, or experimental, developmental, or research work.

I. Survival Rights
Provisions of this Article shall survive termination of this Agreement.

Export Control
A. Information subject to Export Control Laws/International Traffic in Arms Regulation (ITAR): Public Law 90-629, the Arms Export Control Act, as amended (22 U.S.C. 2751 et. seq.) requires that unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license. For purposes of making this determination, the Military Critical Techniques List (MCTL) shall be used as general guidance. All documents determined to contain export controlled technical data will be marked with the following notice:

WARNING: This document contains technical data, export of which is restricted by the Arms Export Control Act (22 U.S.C. 2751, et seq.) or the Export Administration Act of 1979, as amended, 50 U.S.C. App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties.

B. Flowdown.
The SELLER shall 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.

OPSEC & Security
A. Security Requirements
1. The security level for this agreement is UNCLASSIFIED. CMG provides administrative services only. CMG is the CMF for C5. CMG does not receive, generate or store any classified information or material at its locations nor have access to classified information made available to or developed by any PAH.
2. Work performed by a PAH under a Project Agreement may involve access to Controlled Unclassified Information (CUI) as well as information Classified as CONFIDENTIAL, SECRET, or TOP SECRET (pending facility clearance approval by Defense Security Services.). The PAH and its employees who work on such Project Agreements shall comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operation Manual (DOD 5220.22M), Security Classification Specification (DD Form 254), and (2) any revisions to that manual that may be issued. During the course of this Agreement, the parties may determine that information developed by the PAH and/or the Government pursuant to this Agreement shall be treated as classified. Such information shall be classified in accordance with DOD 5220.22M.
3. Each Project Agreement Scope of Work will be provided by the Agreement Officer Representative (AOR) to the AOR industrial security office prior to award. The AOR industrial security office will provide the Security Classification Specification (DD form 254) for the Project Agreement. US Army ARDEC Intelligence and Technology Protection Office (I&TPO) will review Project Agreements where ARDEC is the AOR prior to award and will issue a Security Classification Specification (DD form 254).
4. Any PAH performing on a classified Project Agreement shall obtain and maintain a Facility Clearance from the Defense Security Service for the life of the Project Agreement. The PAH shall receive classified material at the actual performance location(s) only as identified in block 8a of the DD254 issued for the Agreement.
5. The PAH shall issue all subcontract Security Classification Specifications (DD Form 254) to lower tier awards.
6. Any PAH performing on a Classified Project Agreement shall have a Non-Disclosure Agreement (SF 312) signed by all PAH employees working under the Project Agreement and returned to the AOR. The contractor shall not release any information or data without the approval of the Government.
7. PAH personnel shall have the appropriate level of investigation and/or security clearance for each Project Agreement. The PAH shall observe and comply with all security provisions in effect at each selected site. Only U.S. Citizens are authorized to work Classified Project Agreements. All PAH personnel that require access to classified information and/or material will be required to have the appropriate level clearance and must maintain the level of security clearance for the life of the Project Agreement. The PAH shall notify the AOR the same day as an employee receives notice that they will be released, have been fired, or have had their security clearance revoked or suspended.
8. Research and Development under these Project Agreements will be in accordance with the Other Transaction Agreement (OTA) between the United States Army Contracting Command – New Jersey (ACC-NJ) and the C5. Within the Project Agreements, sharing of classified information shall be on a need-to-know basis, as required by the Project Agreement.

9. The AO will make the decision and/or final determination as to the disposition of any classified information and/or material held by the contractor at the completion of the Project Agreement. Upon completion or termination, the PAH shall:
a. Return ALL classified material received or generated under the Project Agreement;
b. Destroy all classified material; or
c. Request retention for a specific period of time.
10. If a Project Agreement involves a classified effort or a Controlled Unclassified Information (CUI) effort, the below listed Department of Defense Directives, Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), and ARDEC clauses shall be incorporated into this agreement by reference with the same force and effect as if they were given in full text. Full text versions shall be made available upon request. Specific applicable security classification guides, policies, instructions, and regulations will be identified in each Project Agreement. Throughout the life of the Project Agreement, if any policy, instruction, or regulation is replaced or superseded, the replacement or superseding version shall apply. The following is a snapshot of key regulatory documents, policies, regulations, etc. applicable at time of award.
a. DoDM 5200.01 DoD Information Security Program, 24 Feb 12
b. DoD 5200.2-R Personnel Security Regulation, Jan 87
c. DoD 5220.22-M National Industrial Security Program, 28 Feb 06
d. DoDI 5200.01, Information Security Program and Protection of Sensitive Compartmented Information, 21 Apr 2016
e. DoDM 5400.7-R, DOD Freedom of Information Act Program, 25 Jan 2017
f. DoDI 2000.12, Antiterrorism Program, 1 Mar 12
g. DODD 5205.02E, DOD Operations Security (OPSEC) Program, 20 Jun 2012
h. DODI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), 28 May 2015
i. AR 380-5, Department of the Army Information Security, 29 Sep 2000
j. AR 380-49, Industrial Security Program, 20 Mar 2013
k. AR 530-1, Operations Security, 26 Sep 2014
l. ARDEC Clause 68, Identification and Access Eligibility Requirements of Contractor Employees (requirement is only applicable to contractor employees working on Picatinny Arsenal)
m. ARDEC Clause 18, Physical Security Standards for Sensitive Items (Required when AA&E apply)
n. ARDEC Clause 70, (FOUO) Release of Information Research and Development (reference FAR 2.101)
o. FAR Clause 4.402, Safeguarding Classified Information Within Industry
p. FAR Clause 52.204-2, Security Requirements, Aug 1996
q. SECURITY CLASSIFICATION GUIDES will be identified per each Individual Project Agreement and supplied to the PAH by the AOR as needed.
11. For all Project Agreements, the following statement shall be flowed to the C5 PAHs to the extent required within the Project Agreements:
a. Anti-Terrorism Level I Training. This provision is for PAH employees with an area of performance within an Army controlled installation, facility or area. All PAH employees requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training within forty five (45) calendar days after Project start date or effective date of incorporation of this requirement into the Project, whichever is applicable. PAH(s) shall submit certificates of completion for each affected employee and PAH employee to the AOR or to the AO. AT level I awareness training is available at the following website: http://jko.jten.mil/
b. Access and General Protection/Security Policy and Procedures. This standard language text is for PAH employees with an area of performance within a DoD controlled installation, facility or area. PAH employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The PAH also shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. The PAH workforce must comply with all personal identity verification requirements as directed by DoD, HQDA and/or local policy. Should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in PAH security matters or processes.
c. Anti-Terrorism Awareness Training for PAH Personnel Traveling Overseas. This standard language text requires U.S.-based PAH employees to receive Government provided area of responsibility specific AT awareness training as directed by AR 525-13. Specific area of responsibility training content is directed by the combatant commander with the unit Anti-terrorism Officer (ATO) being the local point of contact.
d. iWATCH Training. This standard language text is for PAH employees with an area of performance within a DoD controlled installation, facility or area. PAH(s) shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the

types of behavior to watch for and instruct employees to report suspicious activity to the AOR. This training shall be completed within forty-five (45) calendar days of a Project Agreement award and within forty- five (45) calendar days of new employees' commencing performance with the results reported to the AOR NLT thirty (30) calendar days after training completion.

e. Impact on PAH performance during increased FPCON during periods of increased threat. During FPCONs Charlie and Delta, services may be discontinued / postponed due to higher threat. Services will resume when FPCON level is reduced to Bravo or lower.

f. Random Antiterrorism Measures Program (RAMP) participation: PAH personnel working on a DoD installation are subject to participation in the Installation RAMP security program (e.g., vehicle searches, wearing of ID badges, etc.)

g. For PAH personnel requiring CAC: Before CAC issuance, the PAH personnel requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The PAH employee will be issued a CAC only if duties involve one of the following: (1) both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of six (6) months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled National Awareness Check with Inquiries (NACI) at the Office of Personnel Management.

h. For PAH personnel that do not require CAC, but require access to a DoD facility or installation: PAH employees and all associated subcontracted employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (Army Directive 2014-05/AR 190-13); applicable installation, facility and area commander installation and facility access and local security policies and procedures (provided by Government representative); or, at OCONUS locations, in accordance with status-of-forces agreements and other theater regulations.

i. TARP Training: Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in AR 381- 12. This training shall be completed within twelve (12) months after contract start date or effective date of incorporation of this requirement into the contract, whichever applies, and then annually thereafter.

The contractor shall submit documentation of completion for each affected contractor employee and subcontractor employee to the AOR within fourteen (14) calendar days after completion of training by all employees and subcontractor personnel. Training can be executed by a local CI agent, online via the Army Learning Management System at https://www.lms.army.mil (and search for TARP), or by contacting the 902nd military intelligence unit.

j. PAH Employees Who Require Access to Government Information Systems: All PAH employees with access to a Government information systems must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DoD Information Assurance Awareness training prior to accessing the IS and then annually thereafter.

k. For Projects that Require an OPSEC Standing Operating Procedure/Plan: The PAH shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within ninety (90) calendar days of Project award to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This plan will be submitted by CMG on behalf of the PAH(s) to the AO for coordination of approvals. This SOP/Plan will include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it and how to protect it. In addition, PAH shall identify an individual who will be an OPSEC Coordinator. The PAH will ensure this individual becomes OPSEC Level II certified per AR 530-1.

l. For Projects that Require OPSEC Training: Per AR 530-1, Operations Security, new PAH employees assigned by the PAH(s) to perform under a C5 Project Agreement must complete Level I OPSEC awareness training within thirty (30) calendar days of starting work under the Project. All PAH employees performing under an OPSEC-designated Prototype Project must complete annual Level I OPSEC awareness training. Level I OPSEC awareness training is available at the following website: http://cdsetrain.dtic.mil/opsec/.

m. For Contracts that Involve the Public Release of Information: Per AR 530-1, Operations Security, an OPSEC review is required prior to all public releases. All government information intended for public release by a contractor will undergo a Government OPSEC review prior to release.

n. Information assurance (IA)/information technology (IT) training: All PAH employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All PAH(s) working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six (6) months of employment.

o. Information assurance (IA)/information technology (IT) certification: Per DoD 8570.01-M , DFARS 252.239-7001 and AR 25-2, all PAH employees supporting IA/IT functions shall be appropriately certified upon Project Agreement award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon Project Agreement award.

p. For PAH personnel Authorized to Accompany the Force: DFARS Clause 252.225-7040, Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States, shall be used in Projects that authorize PAH personnel to accompany U.S. Armed Forces deployed outside the U.S. in contingency operations; humanitarian or peacekeeping operations; or other military operations or exercises, when designated by the combatant commander. The clause discusses the following AT/OPSEC related topics: required compliance with laws and regulations, pre-deployment requirements, required training (per combatant command guidance) and personnel data required.

q. For Projects Requiring Performance or Delivery in a Foreign Country: DFARS Clause 252.225-7043, Antiterrorism/Force Protection Policy for Defense Contractors Outside the U.S., shall be used in Projects that require performance or delivery in a foreign country. This clause applies to both contingencies and non-contingency support. The key AT requirement is for non-local national PAH personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the PAH's compliance with combatant commander and subordinate task force commander policies and directives.

r. For Projects requiring the PAH to obtain U.S. Government Common Access Cards (CACs), installation badges, and/or access passes: The PAH shall return all issued U.S. Government CACs, installation badges, and/or access passes to the AOR when the project is completed or when the PAH employee no longer requires access to the installation or facility.

s. For Projects That Require Handling or Access to Classified Information: PAH personnel shall comply with FAR 52.204-2, Security Requirements. This clause applies if the Project may require access to information Classified "Confidential," "Secret," or "Top Secret," and requires PAHs to comply with the Security Agreement (DD Form 441), Security Classification Specification (DD Form 254), National Industrial Security Program Operating Manual (DoD 5220.22-M) and any revisions to DOD 5220.22-M, notice of which will be furnished to the PAH.

t. For Projects that require access to Potential Critical Program Information (PCPI) / Critical Program Information (CPI): The PAH shall comply with the associated Interim Program Protection Plan (IPPP) / Program Protection Plan (PPP) / or Technology Protection Plan (TPP). The PAH shall comply with DoD, DA and AMC technology protection requirements in DODI 5200.39, AR 70-1, DA PAM 70-3 and AMC-R-380-13.

u. Information Subject to Export Control Laws/International Traffic in Arms Regulation (ITAR): Public Law 90-629, "Arms Export Control Act," as amended (22 U.S.C 2751 et. Seq.) requires that all unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license under EO 12470 or the Arms Export Control Act and that such data required an approval, authorization, or license for export under EO 12470 or Arms Export Control Act. For purposes of making this determination, the Militarily Critical Technologies List (MCTL) shall be used as general guidance. All documents determined to contain export controlled technical data will be marked with the following notice: WARNING: - This document contains technical data whose export is Restricted by the Arms Export Control Act (Title 22, U.S.C., App. 2401 et seq.) Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

v. For Official Use Only Information (FOUO) and Controlled Unclassified Information (CUI): PAH personnel shall be capable of accessing, handling, receiving, and storing unclassified documents, equipment, hardware, and test items, using the applicable standards. All Controlled Unclassified Information (documents designated as FOR OFFICIAL USE ONLY and/or LIMITED DISTRIBUTION) shall be transmitted electronically using DoD-approved encryption standards.

w. All PAH personnel performing classified work under this Project Agreement are required to have valid JPAS visit requests submitted to the Security Management Office (SMO) by their Facility Security Officer (FSO) for each Government location where work is being performed.

12. Flow down for Security Requirements: CMG shall include the aspects of this Article as they pertain to each Project Agreement. Each Project Agreement will include specific security requirements within each SOW and RPP. The requirements delineated within each Project Agreement, in turn, shall be included in all sub-tier subcontracts or other forms of lower-tier agreements, regardless of tier.

B. Safeguarding Covered Defense Information and Cyber Incident Reporting

(a) Definitions. As used in this Article—

"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, Raytheon Competition Sensitive SCS-TMP-022 (05/24/2017) Page 41 of 45 Subcontract Number: 17410 GPS Source Proprietary Information commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

“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 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 information that—

(i) Is:

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(ii) Falls in any of the following categories:

(A) Controlled technical information.

(B) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information).

“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.

“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 information is recorded, stored, or printed within an 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.

“Rapid(ly) report(ing)” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial 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 that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

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

(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; or (ii) 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)(i) of this clause—

(A) 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," http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD 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; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(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, 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 systems 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.

The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by 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 a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and
(2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

Program Protection

The tasks listed below shall be performed by the Subcontractor as described and will flow down to any Second-tier Subcontractors performing on the contract:
1. The Subcontractor shall assist and support the Contractor in performing CFA, CPI assessments, and controlled technical information (CTI) assessments on the system(s) as necessary, in order to identify critical components, critical functions, CPI and CTI. Additionally, the Subcontractor shall implement Government specified supply chain risk management countermeasures to safeguard Government identified critical components. The Subcontractor shall assist the Contractor to provide and implement a program protection implementation plan (PPIP) within 30 days of receiving the Government countermeasures as detailed in the relevant portions of the Government's Program Protection Plan (PPP), and provide monthly PPIP status reports to the Agreements Officer Representative (AOR) IAW Data Item Description (DID) number DI-ADMN-81306, and D2-10 and D2-33 in the reporting requirements table. The Government intends to provide relevant portions of the PPP to the Contractor 30 days after the technical exchange meeting identified in section 3.2.2.2.1.
2. The Subcontractor shall provide technical support for the Government PPP process IAW DoDI 5000.02; DoDI 5200.39; DoDI 5200.44; Program Protection Plan Outline and Guidance; and Key Practices and Implementation Guide for the DoD Comprehensive National Cyber Security Initiative 11 Supply Chain Risk Management. The Subcontractor shall assist the Contractor to develop, document and update the application of software assurance countermeasures table IAW the Program Protection Plan Outline and Guidance (https://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1- July2011.pdf) and Software Assurance Countermeasures in Program Protection Planning (https://www.acq.osd.mil/se/docs/SwA-CM-in-PPP.pdf). The Subcontractor shall assist the Contractor to complete and provide the USG with the software assurance countermeasures table in the PPIP IAW DI-ADMN-81306, and D2-10 and D2-33 in the reporting requirements table.
3. The Subcontractor shall establish appropriate safeguards to protect program CTI and establish procedures for ensuring compliance with DFARS Clauses 252.204-7012, "Safeguarding Unclassified Controlled Technical Information" and 252.239-7018, "Supply Chain Risk."
4. The Subcontractor shall provide and implement a supplier management plan that identifies the bill of materials and supply chain IAW DI-PSSS-81656B and D2-15 in the reporting requirements table, and that applies best practices to identify, assess, effectively monitor and mitigate supply chain risks. These plan(s) shall, at a minimum, include: 1) supply chain information to the component and lowest sub-tier supplier level, 2) supply chain vulnerabilities, 3) identification and implementation of countermeasures to mitigate risks.
5. The Subcontractor shall provide support to the Contractor for Government counterintelligence activities, consistent with established authorities, in support of program protection objectives, to include: 1) support to Government

execution of program protection surveys, 2) monthly reports of foreign travel and foreign contact for all personnel performing on the contract IAW DI-ADMN-81306 and D2-33 in the reporting requirements table.

6. CPI is defined as the U.S. capability elements that contribute to the Warfighters' technical advantage, which if compromised, undermine U.S. military pre-eminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, training equipment, and/or maintenance support equipment, as defined in DoDI 5200.39. CPI are often DoD-unique capabilities that are developed and owned by the U.S. Government and are necessary for U.S. technological superiority. CPI present in a system or program, which if divulged to unauthorized individuals, could result in the reduction of a critical technological advantage. All CPI must be protected by the Subcontractor and flowed down to Second-tier Subcontractors where CPI is resident in accordance with a specifically tailored PPP produced by the Government. CPI should be identified early and reassessed throughout the life cycle of the program both by the U.S. Government, the Contractor and Subcontractor, if previously unidentified CPI becomes apparent, to include: prior to each acquisition milestone; prior to each system's engineering technical review; throughout operations and sustainment, and specifically during software/hardware technology updates. Consequently, the Government may update the PPP to reflect changes to CPI as identified by the U.S. Government, Contractor or Subcontractor, within a reasonable period of time after identification.

7. The Subcontractor shall provide the Contractor all information related to any previously identified CPI that could be utilized in the current subcontract in accordance with DI-ADMN-81306, and D2-10 and D2-33 in the reporting requirements table, (to include previous PPPs used). The Government reserves the right to update the PPP or similar documentation and identify CPI at any point during the course of contract performance. The Subcontractor shall protect all CPI in accordance with a specifically tailored PPP produced by the Government.

8. All individual Subcontractor employees working under the Government contract shall sign the Government provided Authorized User Agreement (AUA). The Subcontractor shall be responsible for compliance of its employees and records management of the signed agreements. The Subcontractor shall modify/accommodate its computer network(s)/information system(s) being used in performance of this Subcontract to include a banner or notice that informs individual Subcontractor employees that the systems are subject to Government monitoring. The banner or notice shall inform individual Subcontractor employees that use of the system(s) in performance of this Subcontract implies consent to the monitoring and/or collection of PCAP data. The banner or notice shall also inform Subcontractor employees that they do not have a reasonable expectation of privacy in PCAP data. Subcontractor shall ensure that the notice and AUA requirements of this paragraph shall be binding on any and all second tier Subcontractors/Subcontractor employees required to work with CPI with or in concert with the Contractor.

9. The Subcontractor shall provide such support, as required, to support U.S. Government/Army Counterintelligence (CI) operations as delineated, described, and authorized by AR 381-14 and 380-53, to include technical surveillance countermeasures network analysis.

10. The Subcontractor shall consent to digital and multi-media forensic investigations as that term is defined by DoDD 5505.13E, DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3), and in accordance with the consent form and the following:

a. DoDI 5200.39, CPI Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), May 28,2015;

b. DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012;

c. DoD Instruction O-5240.24, "CI Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended;

d. AR 70-77, RDA Program Protection, June 8, 2018;

e. PEO IEW&S-Policy Letter-Program Protection Plans, June 10, 2016

DFARS 252.246-7007	Contractor Counterfeit Electronic Part Detection and Avoidance System. (Aug 2016)	Applicable to Purchase Orders when the goods or services include electronic parts or assemblies containing electronic parts. This clause applies to all Sellers, at all tiers, without regard to whether the Seller itself is subject to CAS.

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:

DFARS 252.223-7002	Safety Precautions for Ammunition and Explosives.	Applicable to all subcontract that involve

	(May 1994)	ammunition or explosives.
DFARS 252.223-7006	Prohibition on Storage and Disposal of Toxic and Hazardous Materials. (Sept 2014)	Applicable to Purchase Orders that require, may require, or permit a Seller or its lower tier subcontractor's access to a DoD installation.
DFARS 252.223-7007	Safeguarding Sensitive Conventional Arms, Ammunition, and Explosives. (Sept 1999)	Applicable to Purchase Orders for (i) the development, production, manufacture, or purchase of arms, ammunition, and explosives (AA&E), or (ii) when AA&E will be provided to the Seller as Government-furnished property.