Raytheon
Space and Airborne Systems

Flowdown Attachment
FDA-2019.272

Prime Contract No.: W15QKN-17-9-5555 and C5-18-0003
Contract No.: 38924
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.

H.18 Insurance. Subcontractor shall obtain at its own expense and provide evidence of the following insurance coverage:

(a) Worker's Compensation Insurance required by law of the State where performance is conducted.

(b) Comprehensive Bodily Injury Insurance with limits of not less than $1,000,000 for each occurrence.

(c) Property Damage Liability with a limit of not less than $100,000 for each occurrence.

(d) Automotive Bodily Injury Liability Insurance with limits of not less than $250,000 for each person and $1,000,000 for each occurrence, and property damage liability insurance with a limit of not less than $100,000 for each occurrence.

(e) Professional Liability and Errors and Omission Insurance of not less than $1,000,000 for each occurrence.

Prior to the commencement of work hereunder or immediately if the Subcontractor has personnel on site, the Subcontractor shall furnish to MTEQ a certificate of the above required insurance. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the interests of the Government or MTEQ shall not be effective (1) for such period as the laws of the State in which this Subcontract is to be performed prescribe, or (2) until

thirty (30) days after the insurer or the Subcontractor gives written notice to MTEQ, whichever period is longer.

The Subcontractor agrees to insert the substance of this clause, including this paragraph, in Subcontracts under this Subcontract that requires work on a Government installation. Any lower-tier subcontractor(s), will be obligated by MTEQ, to provide and maintain the insurance required by virtue of this Subcontract. At least five (5) days before entry of each such subcontractor's personnel on a Government installation, the Subcontractor shall furnish to MTEQ a current certificate of insurance, meeting the requirements of the above paragraphs.

The required insurance coverages above shall be primary and non-contributing with respect to any other insurance that may be maintained by MTEQ. Notwithstanding any provision contained herein, Subcontractor is not insured by MTEQ nor is Subcontractor covered under any insurance policy that MTEQ has in place.

The Subcontractor is required to present evidence of the amount of any deductibles in its insurance coverage. For any insurance required the Subcontractor's deductible is not allowable as a direct or indirect cost under this contract.

52.7106 RESPONSIBILITIES FOR AND PROHIBITIONS ON CONTRACTOR PERSONNEL USE OF MAY/2005 GOVERNMENT INFORMATION SYSTEMS (IS) MAY 2005

The contractor is reminded that, in addition to any other clauses in this contract, contractor personnel granted password access to Government IS or access to Government networks (including connecting contractor-owned assets to Government networks) shall comply with the following responsibilities and prohibitions:

1. Responsibilities:

(a) Participate in annual Information Assurance (IA) training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering. Sign and comply with local installation Acceptable Use Policy.

(b) Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them and with a valid need to know.

(c) Protect IS and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

(d) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

(e) Safeguard and report any unexpected or unrecognizable output products.

(f) Report the receipt of any media (for example, CD-ROM, floppy disk) received to the Information Assurance Manager (IAM) or System Administrator (SA), as appropriate, for authorization to use.

(g) Use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the IS.

(h) Report all known or suspected security incidents, spam, chain letters, and violations of acceptable use to the SA, IAM, or Information Assurance Security Officer (IASO).

(i) Immediately report suspicious, erratic, or anomalous IS operations, and missing or added files, services, or programs to the SA in accordance with local policy and cease operations on the affected IS.

(j) Comply with password or pass-phrase policy directives and protect passwords from disclosure.

(k) Invoke automatic password-protected screen locks on the workstation after not more than 10 minutes of non-use or inactivity.

(l) Log off IS at the end of each workday.

(m) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need to know, and assume only authorized roles and privileges.

(2) Prohibited activities. The following activities are specifically prohibited. Users will not-

(a) Use IS for personal commercial gain or illegal activities.

(b) Use IS in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct. (c) Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications. (Law Enforcement/Criminal Investigators, attorneys, or other official activities, operating in their official capacities only, shall be exempted from this requirement.)

(d) Participate in on-line gambling or other activities inconsistent with public service.

(e) Release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5, the individuals supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officers approval.

(f) Attempt to strain, test, circumvent, or bypass security mechanisms, or perform network line monitoring or keystroke monitoring (unless this is required by the Performance Work Statement of this contract).

(g) Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (for example, instant messaging, peer-to peer applications).

(h) Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization. Connect a non- Government IS to a Government network without authorization from an IAM or IASO.

(i) Share personal accounts and passwords or permit the use of remote access capabilities by any individual.

(j) Disable or remove security or protective software or mechanisms and their associated logs.

3. Any violation of the provisions listed above may result in the following: loss of, or limitations on, use of equipment and services; assessment of costs of any investigation, damage or repair to Government IS;

any other contractual remedies provided for by this contract up to and including termination of the contract for default; and criminal penalties. If the contract Performance Work Statement (PWS) prescribes different requirements than listed in this clause, the PWS takes precedence over this clause in only the areas where it conflicts.

ARTICLE XV: OPSEC & SECURITY

A. Security Requirements

1. The security level for this agreement is UNCLASSIFIED. All effort associated with Master Subcontract Agreement TS-01065 is currently unclassified. If the need arises for classification other than unclassified, the additional effort and cost to comply will be bid separately. This applies to all effort describe in paragraphs 2-12 below.

2. Work performed by Subcontractor 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.). Subcontractor and their 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 Subcontractor 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. Subcontractor performing on a classified agreement shall obtain and maintain a Facility Clearance from the Defense Security Service for the life of the AGREEMENT. Subcontractor shall receive classified material at the actual performance location(s) only as identified in block 8a of the DD254 issued for the Agreement.

5. Subcontractor shall issue all subcontract Security Classification Specifications (DD Form 254) to lower tier awards.

6. Subcontractor performing on a classified agreement shall have a Non-Disclosure Agreement (SF 312) signed by all Subcontractor employees working under this agreement and returned to the AOR. The contractor shall not release any information or data without the approval of the Government.

7. Subcontractor personnel shall have the appropriate level of investigation and/or security clearance for each Project Agreement. Subcontractor shall observe and comply with all security provisions in effect at each selected site. Only U.S. Citizens are authorized to work classified agreements. All Subcontractor 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 this AGREEMENT. Subcontractor 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 C5 in care of its consortium management firm, Consortium Management Group, Inc. (CMG.) 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 agreement. Upon completion or termination, the Subcontractor 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 Subcontractor.

11. For all Project Agreements, the following statement shall be flowed to the Subcontractor unless otherwise stated within the Project Agreements:

a. Anti-Terrorism Level I Training. Reserved. All effort associated with Master Subcontract Agreement TS-01065 will be conducted at Raytheon Vision Systems site. No Army controlled installation, facility or area will be utilized.b. Access and General Protection/Security Policy and Procedures. Reserved. All effort associated with Master Subcontract Agreement TS-01065 will be conducted at Raytheon Vision Systems

site. No Army controlled installation, facility or area will be utilized.c. Anti-Terrorism Awareness Training for Subcontractor Personnel Traveling Overseas. Reserved. All effort associated with Master Subcontract Agreement TS-01065 will be conducted at Raytheon Vision Systems site. Overseas travel is not required for efforts in support of Master Subcontract Agreement TS-01065.d. iWATCH Training. Reserved. All effort associated with Master Subcontract Agreement TS-01065 will be conducted at Raytheon Vision Systems site. No Army controlled installation, facility or area will be utilized.e. Impact on PA Subcontractor H 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: Reserved. All effort associated with Master Subcontract Agreement TS-01065 will be conducted at Raytheon Vision Systems site. No Army controlled installation, facility or area will be utilized.g. Subcontractor 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. Subcontractor personnel that do not require CAC, but require access to a DoD facility or installation: Subcontractor 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: Remove. RVS takes exception to this requirement as Threat Awareness and Reporting Program (TARP) training was not bid for effort associated with Master Subcontract Agreement TS-01065.j. Subcontractor Employees Who Require Access to Government Information Systems: All Subcontractor 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: Subcontractor 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 Subcontractor 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, Subcontractor shall identify an individual who will be an OPSEC Coordinator. Subcontractor will ensure this individual becomes OPSEC Level II certified per AR 530-1. All effort associated with Master Subcontract Agreement TS-01065 is currently unclassified. If the need arises for classification other than unclassified, the additional effort and cost to comply with OPSEC requirements will be bid separately.

l. For Projects that Require OPSEC Training: Per AR 530-1, Operations Security, new Subcontractor employees assigned by Subcontractor to perform under this Agreement must complete Level I OPSEC

awareness training within thirty (30) calendar days of starting work under the Project. All Subcontractor 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 Subcontractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All Subcontractor employees 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. Subcontractor 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 Subcontractor 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 Subcontractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the Subcontractor's compliance with combatant commander and subordinate task force commander policies and directives.

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

s. For Projects That Require Handling or Access to Classified Information: Subcontractor 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 Subcontractor.

t. For Projects that require access to Potential Critical Program Information (PCPI) / Critical Program Information (CPI): Subcontractor shall comply with the associated Interim Program Protection Plan (IPPP) / Program Protection Plan (PPP) / or Technology Protection Plan (TPP). Subcontractor 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): Subcontractor 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, 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://dx.doi.org/10.6028/NIST.SP.800-171 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 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.

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.

ARTICLE XX: LIABILITY OF THE PARTIES

A. Waiver of Liability

With regard to the activities undertaken pursuant to this Agreement, no Party shall make any claim against the other, contractors or subcontractors, for any injury to or death of its own employees or employees of

contractors or subcontractors, or for damage to or loss of its own property 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.

C. Extension of Waiver of Liability

Subcontractor agrees to extend the waiver of liability set forth above to Subcontractor's at any tier under this Agreement by requiring them, by contract or otherwise, to agree to waive all claims described above against the Parties to this Agreement. Subcontractor also agrees to flow down the damages limitation set forth above to Subcontractor 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 C5 Member Entities) and the Government 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 RVS or any other entity performing research activities under a resulting purchase order exceed the amount obligated by that purchase order..

Nothing in this Article shall be construed to create the basis of a claim or suit where none would otherwise exist.

The Government does not contemplate any unusually hazardous risks being associated with the awarded Projects, however, the Government will consider going forward with a request for special indemnification or the inclusion of specially negotiated liability provisions where a Project, as identified by the Government or by CMG, on behalf of C5 PAH(s) or proposing C5 Member Entity(ies), may pose a risk of such nature.

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

952.222-0001	Prohibition Against Human Trafficking, Inhumane Living Conditions, and Withholding of Employee Passports (AUG 2011)	Applicable to all purchase orders.

952.225-0001	Arming Requirements And Procedures for Personal Security Services Contractors and For Requests for Personal Protection (Dec 2011)	Applicable to all contracts with performance in Iraq or Afghanistan that require arming of contractors as part of private security services or individual employees for self-defense.
952.225-0002	ARMED PERSONNEL INCIDENT REPORTS (DEC 2011)	Applicable to all contracts with performance in Iraq or Afghanistan that require arming of contractors as part of private security services or individual employees for self-defense.
952.225-0003	Fitness For Duty and Medical/Dental Care Limitations (Afghanistan) (Feb 2013)	Applicable to all contracts with place of performance in Afghanistan.
952.225-0005	MONTHLY CONTRACTOR CENSUS REPORTING (AUG 2011)	Applicable to all service and construction contracts with place of performance in Iraq or Afghanistan.
952.225-0009	Medical Screening and Vaccination Requirements for Contractor Employees Operating in the CENTCOM Area of Responsibility (Dec 2011)	Applicable to all purchase orders requiring performance in Iraq or Afghanistan.
952.225-0013	CONTRACTOR HEALTH AND SAFETY (DEC 2011)	Applicable to all service and construction contracts in Iraq and Afghanistan that affect the living and work spaces of U.S. Forces (military, civilian, and contractors accompanying the force).
952.225-0016	CONTRACTOR DEMOBILIZATION (AFGHANISTAN) (AUG 2011)	Applicable to all solicitations and contracts, except commodities, with performance in Afghanistan.
FAR 52.211-15	Defense Priority and Allocation Requirements. (Aug 2008)	Applicable to all Purchase Orders with a DPAS rating.
FAR 52.225-19	Contractor Personnel in a Designated Operational Area or Supporting a	Applicable to all Purchase Orders that require Seller personnel to perform outside the United States— (1) In a designated operational area during— (i) Contingency operations; (ii) Humanitarian or peacekeeping operations; or (2) When

	Diplomatic or Consular Mission Outside the United States (Mar 2008)	supporting a diplomatic or consular mission— (i) That has been designated by the Department of State as a danger pay post (see http://aoprals.state.gov/Web920/danger_pay_all.asp); or (ii) That the Contracting Officer has indicated is subject to this clause.
DFARS 252.225-7043	Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States (JUN 2015)	Applicable to all Purchase Orders that require performance or travel outside the U.S., except subcontractors who are a foreign government, a representative of a foreign government, or a foreign corporation wholly owned by a foreign government.
DFARS 252.225-7997	CONTRACTOR DEMOBILIZATION (Deviation 2010-O0014) (Aug 2010)	Applicable to all Purchase Orders with performance in Afghanistan, except those for commodities.
DFARS 252.237-7010	Prohibition on Interrogation of Detainees by Contractor Personnel (JUN 2013)	Applicable to Purchase Orders that require Seller personnel to interact with detainees in the course of their duties.
FAR 52.203-6	Restrictions on Subcontractor Sales to the Government. (Sept 2006)	Applicable to Purchase Orders over the Simplified Acquisition Threshold.
FAR 52.203-7	Anti-Kickback Procedures. (October 2010)	Applicable to Purchase Orders that exceed $150,000, excepting paragraph (c)(1))
FAR 52.203-12	Limitation on Payments to Influence Certain Federal Transactions. (October 2010)	Applicable to Purchase Orders exceeding $150,000.
FAR 52.203-13	Contractor Code of Business Ethics and Conduct. (April 2010)	Applicable to Purchase Orders (i) that have a value more than $5,000,000 and (ii) that have a performance period of more than 120 days.) (In Paragraph (b)(3)(i), the meaning of “agency office of the Inspector General” and “Contracting Officer” does not change, in Paragraph (b)(3)(ii) the meaning of “Government” does not change, and in Paragraphs (b)(3)(iii) and (c)(2)(ii)(F), the meaning of “OIG of the ordering agency”, “IG of the agency” “agency OIG” and “Contracting Officer” do not change.
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 52.204-9	Personal Identity Verification of Contractor Personnel. (Jan 2011)	Applicable to Purchase Orders when Seller’s employees are required to have routine physical access to a Federally-controlled facility and / or routine access to a Federally-controlled information system.

FAR 52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards (Aug 2012)	Applicable when the Buyer is the Prime Contractor and the Purchase Order exceeds $25,000. Substitution of the parties is not applicable to this clause. Seller shall report to Buyer the information required under the clause.
FAR 52.209-6	Protecting the Governments Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Dec 2010)	Applicable to Purchase Orders exceeding $30,000.
FAR 52.215-23	Limitations on Pass-Through Charges. (Oct 2009)	Applicable to all cost-reimbursement Purchase Orders that exceed the simplified acquisition threshold; except if the Buyers' prime contract is with the DoD, then applicable to all cost-reimbursement Purchase Orders and all fixed-price Purchase Orders, except those identified in 15.408(n)(2)(i)(B)(2), that exceed the threshold for obtaining cost or pricing data in accordance with FAR 15.403-4.
FAR 52.222-21	Prohibition of Segregated Facilities. (Feb 1999)	Applicable to all offers Purchase Orders over $10,000. Foreign Sellers: Applicable to Purchase Orders except to the extent that work under the Purchase Order will be performed outside the United States or by employees that are not recruited within the United States to work on the Purchase Order. "United States", as used in this parenthetical, means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.
FAR 52.222-35	Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans. (Sept 2010)	Applicable to Purchase Orders of $100,000 or more ($150,000 under prime contracts awarded after 9/30/2015). Foreign Sellers: Applicable to Purchase Orders when the listing of employment openings for purposes of work to be performed under this Purchase Order occur and are filled within the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island. No substitution of parties.
FAR 52.222-36	Affirmative Action for Workers With Disabilities. (Oct 2010)	Applicable to Purchase Orders exceeding $15,000. Foreign Sellers: Applicable to Purchase Orders to the extent that work under the Purchase Order will be performed in the United States, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, or Wake Island or Seller is recruiting employees in the United States, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, or Wake Island to work on the Purchase Order. No substitution of parties.
FAR 52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible	Applicable to Purchase Orders of $100,000 or more. Foreign Sellers: Applicable to Purchase Orders when the listing of employment openings for purposes of work to be performed under this Purchase Order occur and are filled within the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands,

	Veterans. (Sept 2010)	and Wake Island.
FAR 52.222-54	Employment Eligibility Verification (Jan 2009)	Applicable to Purchase Orders (i) for construction or commercial or noncommercial services (except commercial services that are part of a purchase of a COTS item, or an item that would be a COTS item, but for minor modifications, performed by the COTS provider, and that are normally provided for that COTS item); (ii) has a value more than $3,000 (more than $3,500 under prime contracts awarded after 9/30/2015); and (iii) includes work performed in the United States. Foreign Sellers: "United States", as used in this parenthetical, means the 50 States, the District of Columbia, Puerto Rico, Guam, the Commonwealth of the Northern Mariana Islands, and the U.S. Virgin Islands.
FAR 52.223-18	Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011)	Applicable to Purchase Orders over the Micro-Purchase Threshold.
FAR 52.225-13	Restrictions on Certain Foreign Purchases. (June 2008)	Applicable to all Purchase Orders.
FAR 52.227-1	Authorization and Consent. (Dec 2007)	Applicable to Purchase Orders over the Simplified Acquisition Threshold.
FAR 52.227-1 Alt. I	Authorization and Consent. (Dec 2007)	Applicable to Purchase Orders over the Simplified Acquisition Threshold.
FAR 52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement. (Dec 2007)	Applicable to Purchase Orders expected to exceed the Simplified Acquisition Threshold.
FAR 52.244-6	Subcontracts for Commercial Items. (Dec 2010)	Applicable to all Purchase Orders.
FAR 52.247-63	Preference for U.S.-Flag Air Carriers. (June 2003)	Applicable to Purchase Orders that involve international air transportation.
DFARS 252.203-7002	Requirement to Inform Employees of Whistleblower Rights (Jan 2009)	Applicable to all Purchase Orders with a Substitution of Seller for Contractor, but not Raytheon for Government.

DFARS 252.204-7000	Disclosure of Information. (Dec 1991)	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 252.225-7012	Preference for Certain Domestic Commodities. (Jun 2010)	Applicable to all Purchase Orders ("Government" means "Government and/or Buyer".)
DFARS 252.225-7040	Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States. (Jun 2011)	Applicable to Purchase Orders that will be performed when Seller's personnel or Seller's subcontractors are supporting U.S. Armed Forces deployed outside the United States in contingency operations, peace operations consistent with Joint Publication 3-07.3, or other military operations or military exercises, when designated by the Combatant Commander or as directed by the Secretary of Defense.
DFARS 252.226-7001	Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns. (Sept 2004)	Applicable to all Purchase Orders exceeding $500,000.
DFARS 252.227-7013	Rights in Technical Data--Noncommercial Items. (Feb 2012)	Applicable to solicitations and resulting Purchase Orders when Buyer will be required to deliver to the Government Seller's technical data pertaining to noncommercial items, or pertaining to commercial items for which the Government will have paid for any portion of the development costs.
DFARS 252.227-7016	Rights in Bid or Proposal Information. (Jan 2011)	Applicable to all Purchase Orders.
DFARS 252.227-7019	Validation of Asserted Restrictions--Computer Software. (Sept 2011)	Applicable to all Purchase Orders when Seller's performance includes the furnishing of computer software that Buyer will furnish to the Government.
DFARS 252.227-7039	Patents--Reporting of Subject Inventions. (April 1990)	Applicable to solicitations and resulting Purchase Orders that will include the clause at FAR 52.227-11 for experimental, developmental, or research work to be performed by a small business concern or nonprofit organization
DFARS 252.244-7000	Subcontracts for Commercial Items and Commercial Components (DoD Contracts). (Sep 2011)	Applicable to all Purchase Orders.
DFARS 252.247-7023	Transportation of Supplies by Sea. (May 2002)	Applicable if the Seller is transporting supplies by sea under this Purchase Order shall use U.S.-flag vessels if— (i) This Purchase Order is a construction contract; or (ii) The supplies being transported are—(A) Noncommercial items; or (B) Commercial items that— (1) The Seller is reselling or distributing to the

		Government without adding value (generally, the Seller does not add value to items that it subcontracts for f.o.b. destination shipment); (2) Are shipped in direct support of U.S. military contingency operations, exercises, or forces deployed in humanitarian or peacekeeping operations; or (3) Are commissary or exchange cargoes transported outside of the Defense Transportation System in accordance with 10 U.S.C. 2643.

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:

FAR 52.227-3	Patent Indemnity. (April 1984)	Applicable to all purchase orders.
DFARS 252.225-7006	Quarterly Reporting of Actual Contract Performance Outside the United States. (Oct 2010)	Applicable to all first-tier subcontracts exceeding $650,000, except those for commercial items, construction, ores, natural gases, utilities, petroleum products and crudes, timber (logs), or subsistence.
FAR 52.215-2	Audit and Records – Negotiation. (Oct 2010)	Applicable to the following Purchase Orders that exceed the simplified acquisition threshold: (i) that are cost-reimbursement, incentive, time-and-materials, labor-hour, or price-redeterminable type or any combination of these, (ii) for which certified cost or pricing data are required; or (iii) that require Seller to furnish reports as discussed in paragraph (e) of the clause. This clause does not apply to Purchase Orders for commercial items.
FAR 52.215-14	Integrity of Unit Prices. (Oct 2010)	Applicable to all Purchase Orders OTHER THAN: acquisitions at or below the simplified acquisition threshold in FAR Part 2; construction or architect-engineer services under FAR Part 36; utility services under FAR Part 41; services where supplies are not required; commercial items; and petroleum products
FAR 52.215-15	Pension Adjustments and Asset Reversions. (Oct 2010)	Applicable to all Purchase Orders that require certified cost or pricing data. This clause does not apply to Purchase Orders for commercial items or if the Seller qualifies for any of the other exemptions in FAR 15.403-1.
FAR 52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions. (July 2005)	Applicable to all Purchase Orders that require certified cost or pricing data. This clause does not apply to Purchase Orders for commercial items or if the Seller qualifies for any of the other exemptions in FAR 15.403-1.
FAR 52.215-19	Notification of Ownership Changes. (Oct 1997)	Applicable to all Purchase Orders that require certified cost or pricing data. This clause does not apply to Purchase Orders for commercial items or if the Seller qualifies for any of the other exemptions in FAR 15.403-1.
FAR 52.222-26	Equal Opportunity. (March 2007)	Applicable to Purchase Orders exceeding $10,000. Foreign Sellers: Applicable to Purchase Orders except to the extent that work under the Purchase Order will be performed outside the United States or by employees that are not recruited within the United States to work on the Purchase Order. "United States", as used in this parenthetical, means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.

FAR 52.222-41	Service Contract Labor Standards. (Nov 2007)	Applicable to Purchase Orders that are subject to the Service Contract Labor Standards statute.
FAR 52.222-50	Combating Trafficking in Persons. (Feb 2009)	
FAR 52.224-1	Privacy Act Notification (April 1984)	Applicable to Purchase Orders when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.
FAR 52.224-2	Privacy Act. (April 1984)	Applicable to Purchase Orders that require the design, development, or operation of any system of records on individuals that is subject to the Privacy Act.
FAR 52.227-10	Filing of Patent Applications -- Classified Subject Matter.(Dec 2007)	Applicable to Purchase Orders that cover or likely to cover classified subject matter.
FAR 52.227-11	Patent Rights -- Ownership by the Contractor. (Dec 2007)	Applicable to Purchase Orders for experimental, developmental, or research work to be performed by a small business concern or nonprofit organization.
FAR 52.228-5	Insurance -- Work on a Government Installation. (Jan 1997)	Applicable to Purchase Orders that require work on a Government installation.
FAR 52.237-2	Protection of Government Buildings, Equipment, and Vegetation. (April 1984)	Applicable to all Purchase Orders for services to be performed on Government installations.
DFARS 252.203-7001	Prohibition on Persons Convicted of Fraud or Other Defense-Contract-Related Felonies. (Dec 2008)	Applicable to all Purchase Orders exceeding $150,000, except those for commercial items.
DFARS 252.223-7006	Prohibition on Storage and Disposal of Toxic and Hazardous Materials. (Apr 1993)	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.
DFARS 252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation. (Feb 2012)	Applicable to solicitations and resulting Purchase Orders when Seller's performance will require delivery of non-commercial computer software or computer software documentation. Not applicable to Purchase Orders for commercial goods.
DFARS 252.231-7000	Supplemental Cost Principles. (Dec 1991)	Applicable to solicitations and resulting Purchase Orders that are subject to the principles and procedures described in FAR subparts 31.1, 31.2, 31.6, or 31.7.
DFARS 252.239-7016	Telecommunications Security Equipment, Devices, Techniques, and Services. (Dec 1991)	Applicable to Purchase Orders which require securing telecommunications.