Supplier Quality Requirements and Purchase Order Terms & Conditions
Rev. P (11/11/2021)
The following requirements apply based on the Purchase Order received from ACE

PACKING AND SHIPPING.

1. Supplier shall prepare and package product destined to ACE in a manner to prevent damage and deterioration during shipping.
2. Shipments, as specified in our Purchase Oder, shall be in accordance with specified quantities and due dates. It is requested that supplier notify ACE of any anticipated or actual delay.
3. Seller shall not insure collect or 3rd party shipments.
4. Unauthorized insured shipments will result in all shipping charges to be refused and will become the responsibility of the Seller
5. Premium transportation is to be used only when designated/authorized in writing by the buyer/ACE representative.
6. Unauthorized freight charges will be the responsibility of the seller.

SHIPMENT/DELIVERY. Shipments or deliveries, as specified in a ACE Purchase Order, shall be in accordance with the specified quantities and the specified schedules. Supplier is encouraged to notify ACE of any anticipated or actual delay.

ACE FURNISHED MATERIALS. All materials furnished by ACE are to be returned with the product upon completion of the order unless other arrangements have been made.

NON-CONFORMING MATERIAL. For material supplied by ACE, supplier must notify ACE of any nonconforming product and make arrangements for approval if submitting any nonconforming product.

SUBCONTRACTING/APPROVED SUPPLIERS. Any ACE supplier may subcontract work to another supplier provided that ACE is provided with the same rights and protection as stated in the Purchase Order and the ACE Terms and Conditions. Suppliers may only use approved suppliers of ACE and/or its customers.

RIGHT OF ENTRY. Supplier shall allow ACE representatives, ACE customers, statutory and regulatory agencies right of entry into the applicable areas of Supplier's facilities and the entire supply chain to verify all processes and records.

QUALITY. Supplier shall provide and maintain an inspection system which will assure that all delivered products conform to Purchase Order requirements, whether manufactured or processed by the supplier or a sub-tier supplier. Supplier shall maintain controls and perform all inspections and tests required to substantiate product conformance to Purchase Order requirements. If not specified in the Purchase Order, contact ACE for required revision of drawings, specifications, and other requirements. Supplier is required to notify ACE of changes in product and/or process definition to obtain ACE's approval prior to such changes.

INSPECTION AND TEST EQUIPMENT. Supplier shall maintain inspection and test equipment to assure calibration traceable to a known national or international standard. Calibration records must be maintained and made accessible to ACE, if required.

FOREIGN OBJECT DAMAGE. Supplier shall control/prevent foreign object damage or contamination during manufacture, assembly, inspection and/or shipment. The FOD program requirements must be made accessible to ACE upon request.

RECORDS. The Supplier shall maintain records of work performed for ACE. Records shall include the COC provided to ACE as well as records that support the certificate. Records must be available to ACE upon request. Records must be maintained for a minimum of fifteen (15) years. Disposition required is; a) hard copy records – shred, b) electronic/digital files – delete.

OBSOLESCENCE: It is requested that when products are known to become obsolete or superseded, a notice of such shall be communicated to ACE within 180 days.

CERTIFICATIONS. Supplier must ensure that individual parameters within a given specification have been met. Certifications must reflect that all applicable manufacturing and process specifications called for on the engineering drawing have been met.

FIRST ARTICLE INSPECTION. If required by ACE on the Purchase Order, first article inspections are to be recorded on form AS9102, current revision or on a form compliant with AS9102.

CALIBRATION SERVICES ONLY. Calibration of inspection equipment shall be performed traceable to National Institute of Standards and Technology (NIST) or other national or international standards. Certificates of Calibration shall be provided.

CHANGES. Any change to the requirements as stated on the Purchase Order must be approved by ACE prior to acting on those proposed changes.

COUNTERFEIT PARTS PROGRAM.

1. Seller shall have counterfeit avoidance program to prevent introduction of counterfeit product into the supply chain. When supplying EEE parts, the program must be compliant to AS5553 and/or AS6174 if. Supplier is REQUIRED to prevent the shipment of counterfeit/suspect unapproved products to ACE. Seller shall immediately notify ACE if it is aware or suspects that it has furnished counterfeit work.

2. If suspect/counterfeit parts are furnished under this purchase agreement, such items shall be impounded. The seller shall promptly replace such items with items acceptable to ACE and the seller may be liable for all costs relating to impoundment, removal, and replacement. ACE may turn such items over to US Governmental authorities (Office of Inspector General, Defense Criminal Investigative Service, Federal Bureau of investigation, etc.) for investigation and reserves the right to withhold payment for the suspect items pending the results of the investigation.

SUPPLIER RATING REQUIREMENTS. Supplier quality and on time delivery are reviewed at least annually. Suppliers who fall behind 75% on time delivery and have more than 250 ppm rejected may be required to supply action/correction plan in order to stay on the ACE approved supplier list. ACE may request action at any time if supplier falls below either on time delivery or quality requirements.

COMPLIANCE, CONFLICT MINERALS, REACH/RoHS AND SPECIALTY METALS.

1. If the products on a Purchase Order contain the "Conflict Minerals" (tantalum, tin, tungsten and gold), our expectation is that the seller acquire these minerals only from responsible sources. If these minerals are known to be from the Democratic Republic of the Congo or surrounding area, ACE CANNOT accept the parts.
2. Supplier is encouraged to have a due diligence program regarding the Conflict Minerals included in the Dodd-Frank Act.
3. Parts must be in compliance with DFARS 252.225-7009 Restriction on Acquisition of Certain Articles Containing Specialty Metals.
4. Parts must be in compliance with DFARS 252.225-7001 – Buy American and Balance of Payments Program.
5. Suppliers shall label products which contain or are manufactured with ozone-depleting substances as required by 42 U.S.C. 7671j (b), (c), and (d) and 40 CFR Part 82, Subpart E, with the following as applicable. Warning Contains *_____, a substance(s) which harm(s) public health and environment by destroying ozone in the upper atmosphere.
6. Warning Manufactured with *_____, a substance(s) which harm(s) public health and environment by destroying ozone in the upper atmosphere.
    - Suppliers shall insert the name of the substance(s).

7. ACE requires products supplied on this purchase order to be in compliance with RoHS Directive 2011/65/EU and REACH regulation EC 1907/2006 before processing. Where applicable, those results MUST be noted on the incoming shipping documentation.

PRODUCT TRACEABLITY. The seller shall maintain a method of item traceability that ensures tracking of the supply chain back to the manufacturer of all parts included in assemblies and subassemblies being delivered per this order. This traceability method shall clearly identify the name and location of all of the supply chain intermediaries from the manufacturer to the direct source of the product for the seller and shall include the manufacturer's batch identification for the item(s) such as date codes, lot codes, serializations, or other batch identifications.

PURCHASE ORDER PRODUCT TERMS & CONDITIONS.

1. Supplier shall provide and maintain an inspection/verification system which will assure that all delivered products conform to Purchase Order requirements. Supplier shall maintain controls and perform all inspections and tests required to substantiate product conformance to requirements.
2. Latest revision of product required if a revision level is not called out, and that revision level must be indicated on shipping document and C of C. This does not apply to commercial products.
3. To ensure product performance, reliability, and quality the supplier shall notify ACE of any non-conformities or changes in product definition that would affect this material.
4. **Shelf life products must be provided with at least 85% of shelf life remaining, unless otherwise noted on Purchase Order.**
5. If products are ITAR regulated, ACE must be notified in writing before shipment.
6. Once accepted, please acknowledge this PO via fax or email promptly.
7. No reworked, refurbished, or overhauled product will be accepted.

SHIPPING INFORMATION

1. Supplier shall prepare, and package product destined to ACE in a manner to prevent damage and deterioration during shipping.
2. Shipments, as specified in our Purchase Oder, shall be in accordance with specified quantities and due dates. It is requested that supplier notify ACE of any anticipated or actual delay.
3. Seller shall not insure collect or 3rd party shipments.
    a. Unauthorized insured shipments will result in all shipping charges to be refused and will become the responsibility of the Seller
4. Premium transportation is to be used only when designated/authorized in writing by the buyer/ACE representative.
    a. Unauthorized freight charges will be the responsibility of the seller.

EXPORT COMPLIANCE REQUIREMENTS. If any products on this purchase order are controlled by ITAR (22 CFR 120-130) or EAR (15 CFR 730-774), seller shall provide that information including Export Control Classification Numbers, HTS, and Schedule B numbers. Seller agrees to abide by all U.S. import and export laws and regulations.

PERSONNEL COMPETENCY. ACE may specify specific qualification for personnel performing work related to the details of the Purchase Order provided. The supplier should be ready to provide evidence of this to A.C.E. if requested.

PERSONNEL COMMUNICATION. Supplier is required to communicate with their personnel regarding the following:
Their contribution to product or service conformity to requirements
Their contribution to product safety
The importance of ethical behavior

FAR and DFAR Flowdown Provisions

FAR 52.204-23 Prohibition on contracting for hardware, software, and services developed or provided by Kaspersky Lab and other covered countries.

Hardware (or components of), Software (or components of), or service developed or provided in whole or in part by a Kaspersky Lab, successor entity to Kaspersky Lab, entity that controls, is controlled by, is under common control with Kaspersky Lab, or an entity of which Kaspersky Lab has a majority ownership is not allowed under this contract. If any escapes of this clause are found after delivery, a notice must be sent to the quality manager (email at the bottom of this document) within 1 day. This must be flowed down to any subcontractors utilized for this contract.

FAR 52.222-50 HUMAN TRAFFICKING AND THE CALIFORNIA TRANSPARENCY IN SUPPLY CHAINS ACT

Aircraft & Commercial Enterprises requires its suppliers and manufacturers within its supply chain to report any human trafficking or slavery acts. A.C.E. does not have a verification process and we do not hire any third-party auditors.

A.C.E. has zero tolerance for any employee or representative engaging in any conduct that would facilitate any trafficking in persons.

A.C.E. requires its suppliers and manufacturers to comply with laws regarding trafficking and slavery in the country or countries in which they do business.

A.C.E. provides company employees and management with training on human trafficking and slavery with respect to mitigating risks within the supply chain.

FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

(a) Definitions. As used in this clause -

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

(a) Definitions. As used in this clause –

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is -

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

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

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Operationally critical support means supplies, or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Rapidly report means within 72 hours of discovery of any cyber incident.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data - Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

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

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

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall -

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

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

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD -

(1) To entities with missions that may be affected by such information.

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents.

(3) To Government entities that conduct counterintelligence or law enforcement investigations.

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) Subcontracts. The Contractor shall -

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to -

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause

DFARS 252.223-7999 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS

(a) Definition. As used in this clause –

United States or its outlying areas means—

(1) The fifty States;

(2) The District of Columbia;

(3) The commonwealths of Puerto Rico and the Northern Mariana Islands;

(4) The territories of American Samoa, Guam, and the United States Virgin Islands; and

(5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).

(c) Compliance. The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor or subcontractor workplace locations published by the Safer Federal Workforce Task Force (Task Force Guidance) at

https:/www.saferfederalworkforce.gov/contractors/.

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part within the United States or its outlying areas.

FAR 52.223-99 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS

(a) Definition. As used in this clause -

United States or its outlying areas means—

(1) The fifty States;

(2) The District of Columbia;

(3) The commonwealths of Puerto Rico and the Northern Mariana Islands;

(4) The territories of American Samoa, Guam, and the United States Virgin Islands; and

(5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).

(c) Compliance. The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor workplace locations published by the Safer Federal Workforce Task Force (Task Force Guidance) at https:/www.saferfederalworkforce.gov/contractors/.

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part within the United States or its outlying areas.

If there are any questions, please direct to Steve Langholz (steve@aircoment.com) (316)788-0400