

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE			32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
			32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	
38. S/R ACCOUNT NO.	39. S/R VOUCHER NUMBER	40. PAID BY		
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY (<i>Print</i>)		
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER		42b. RECEIVED AT (<i>Location</i>)		
		42c. DATE REC'D (YY/MM/DD)		42d. TOTAL CONTAINERS

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 3 OF 12 PAGES
This solicitation will be issued to service the customers' subsistence requirements for DoD and Non-DoD customers in Pennsylvania, New Jersey and Southern New York Regions. This solicitation will result in a five (5) year Indefinite Delivery Indefinite Quantity (IDIQ) contract consisting of three (3) Tier Periods. The first tier shall be a twenty-four (24) month period, inclusive of up to a 120-day implementation period which shall begin immediately after the award date and will end as the first order is placed for Tier 1. The second tier will be an eighteen-month (18) period immediately following the first tier. The third tier will be for an eighteen-month (18) period immediately following the second tier. The estimated dollar of this solicitation is \$23,641,271.94 for a five (5) year period. The guaranteed minimum dollar value is 10% of the estimated value or \$2,364,127.19, inclusive of all tier periods. The contract will consist of three tiers with a maximum dollar value that is 350% of the estimated dollar value or \$82,744,451.80, inclusive of all tier periods. The Government's legal obligation under this contract shall only be that of the guaranteed minimum. All prices will be Firm Fixed with an Economic Price Adjustment (EPA) for the 5 years. Block 11 should be checked.		
CONTINUED ON NEXT PAGE		

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 4 OF 12 PAGES
--------------------	--	--------------------

Form

PID Data - Custom Clause

Insert (copy and paste) text for the PID information here

Part 12 Clauses

CLAUSES ADDED TO PART 12 BY ADDENDUM

252.203-7000 REQUIREMENTS RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (SEP 2011) DFARS

252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (DEC 2022) DFARS

52.204-19 INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014) FAR

252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992) DFARS

252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (JAN 2023) DFARS

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEVIATION 2024-O0013) (MAY 2024) DFARS

(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

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 5 OF 12 PAGES
--------------------	--	--------------------

Part 12 Clauses (CONTINUED)

(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 --Other Than Commercial Products and Commercial Services, 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", Revision 2 (available via the internet at <http://dx.doi.org/10.6028/NIST.SP.800-171>).

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

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

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

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

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 6 OF 12 PAGES
Part 12 Clauses (CONTINUED) 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) <i>Cyber incident reporting requirement.</i> (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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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) <i>Malicious software.</i> 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) <i>Media preservation and protection.</i> 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) <i>Access to additional information or equipment necessary for forensic analysis.</i> Upon request by DoD, the Contractor shall provide DoD with access to additional information equipment that is necessary to conduct a forensic analysis. (g) <i>Cyber incident damage assessment activities.</i> 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) <i>DoD safeguarding and use of contractor attributional/proprietary information.</i> 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) <i>Use and release of contractor attributional/proprietary information not created by or for DoD.</i> 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) <i>Use and release of contractor attributional/proprietary information created by or for DoD.</i> 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 CONTINUED ON NEXT PAGE		

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 7 OF 12 PAGES
Part 12 Clauses (CONTINUED) 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) <i>Other safeguarding or reporting requirements.</i> 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) <i>Subcontracts.</i> 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 products or commercial services, 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. (End of clause) 252.204-7014 LIMITATIONS ON THE USE OR DISCLOSURE OF INFORMATION BY LITIGATION SUPPORT CONTRACTORS (JAN 2023) DFARS 52.215-8 ORDER OF PRECEDENCE - UNIFORM CONTRACT FORMAT (OCT 1997) FAR 52.222-50 COMBATING TRAFFICKING IN PERSONS (NOV 2021) FAR 52.222-62 PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706 (JAN 2022) FAR 252.223-7009 PROHIBITION OF PROCUREMENT OF FLOURINATED AQUEOUS FILM-FORMING FOAM FIRE-FIGHTING AGENT FOR USE ON MILITARY INSTALLATIONS (MAR 2024) FAR 252.225-7054 PROHIBITION ON USE OF CERTAIN ENERGY SOURCED FROM INSIDE THE RUSSIAN FEDERATION (JAN 2023) FAR 252.225-7056 PROHIBITION REGARDING BUSINESS OPERATIONS WITH THE MADURO REGIME (JAN 2023) DFARS 252.225-7058 POSTAWARD DISCLOSURE OF EMPLOYMENT OF INDIVIDUALS WHO WORK IN THE PEOPLE'S REPUBLIC OF CHINA (JAN 2023) DFARS 252.225-7062 RESTRICTION ON ACQUISITION OF LARGE MEDIUM-SPEED DIESEL ENGINES (JUL 2023) DFARS 252.225-7967 PROHIBITION REGARDING RUSSIAN FOSSIL FUEL BUSINESS OPERATIONS (CLASS DEVIATION 2024-O0006, REVISION 1) (FEB 2024) DFARS As prescribed in Class Deviation 2024-O0006, Revision 1, use the following clause: (a) <i>Definitions.</i> As used in this clause -- “<i>Business operations</i>” means knowingly engaging in commerce in any form, including acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other known apparatus of business or CONTINUED ON NEXT PAGE		

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 8 OF 12 PAGES
--------------------	--	--------------------

Part 12 Clauses (CONTINUED)

commerce. The term does not include --

(1) Any shipment subject to price caps as specified in the --

(i) "Statement of the G7 and Australia on a Price Cap for Seaborne Russian-Origin Crude Oil", issued on December 2, 2022, between member countries of that coalition; or

(ii) "Statement of the G7 and Australia on Price Caps for Seaborne Russian-Origin Petroleum Products Berlin, Brussels, Canberra, London, Ottawa, Paris, Rome, Tokyo, Washington", issued on February 4, 2023, between such members, if such shipment complies with the applicable price caps; or

(A) Actions taken for the benefit of the country of Ukraine, as determined by the Secretary; or

(B) Actions taken to support the suspension or termination of business operations for commercial activities during the period beginning on the effective date and ending on December 31, 2029, including --

(1) Any action to secure or divest from facilities, property, or equipment;

(2) The provision of products or services provided to reduce or eliminate operations in territory internationally recognized as the Russian Federation or to comply with sanctions relating to the Russian Federation; and;

(3) Activities that are incident to liquidating, dissolving, or winding down a subsidiary or legal entity in Russia.

Fossil fuel company means an entity or individual that --

(1) Carries out oil, gas, or coal exploration, development, or production activities;

(2) Processes or refines oil, gas, or coal; or

(3) Transports, or constructs facilities for the transportation of, Russian oil, gas, or coal.

(b) *Prohibition*. In accordance with section 804 of the National Defense Authorization Act for Fiscal Year 2024 (Pub. L. 118-31), the Contractor is prohibited from entering into a subcontract or other contractual instrument for the procurement of products or services with any entity or individual that is known to be, or that is known to have fossil fuel business operations with an entity or individual that is, not less than 50 percent owned, individually or collectively, by --

(1) An authority of the government of the Russian Federation; or

(2) A fossil fuel company that operates in the Russian Federation, except if the fossil fuel company transports oil or gas --

(i) Through the Russian Federation for sale outside of the Russian Federation; and

(ii) That was extracted from a country other than the Russian Federation with respect to the energy sector of which the President has not imposed sanctions as of the date on which the contract is awarded.

(c) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including those for the acquisition of commercial products or commercial services.

(End of clause)

52.232-25 PROMPT PAYMENT (JAN 2017) FAR

52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (MAR 2023) FAR

252.232-7003 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS AND RECEIVING REPORTS (DEC 2018) DFARS

52.233-3 PROTEST AFTER AWARD (AUG 1996) FAR

52.233-4 APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM (OCT 2004) FAR

252.244-7000 SUBCONTRACTS FOR COMMERCIAL PRODUCTS OR COMMERCIAL SERVICES (NOV 2023) DFARS

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) FAR

As prescribed in 52.107(b), insert the following clause:

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

FAR: <https://www.acquisition.gov/?q=browsefar>

DFARS: <https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>

DLAD: <http://www.dla.mil/HQ/Acquisition/Offers/DLAD.aspx>

(End of clause)

52.253-1 COMPUTER GENERATED FORMS (JAN 1991) FAR

252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (JAN 2023) DFARS

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 9 OF 12 PAGES
--------------------	--	--------------------

Part 12 Clauses (CONTINUED)

252.225-7048 EXPORT CONTROLLED ITEMS (JUN 2013) DFARS

252.225-7051 PROHIBITION ON ACQUISITION OF CERTAIN FOREIGN COMMERCIAL SATELLITE SERVICES (DEC 2022) DFARS

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB COVERED ENTITIES (DEC 2023) FAR

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021) FAR

52.204-27 PROHIBITION ON A BYTEDANCE COVERED APPLICATION (JUN 2023) FAR

52.204-28 FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT ORDERS -- FEDERAL SUPPLY SCHEDULES, GOVERNMENTWIDE ACQUISITION CONTRACTS, AND MULTI-AGENCY CONTRACTS (DEC 2023) FAR

52.204-30 FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT ORDERS -- PROHIBITION (DEC 2023) FAR

52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013) FAR

Attachments

List of Attachments

Description	File Name
ATTACH_ATTACHMENT_1__MARKET_BASKET_P RICE_PROPOSAL_Spread sheet__PA_NJ_NY	ATTACHMENT 1 - MARKET BASKET PRICE PROPOSAL Spreadsheet - PA NJ NY.xlsx
ATTACH_ATTACHMENT_10__DIBBS_Proposal_Ins tructions	ATTACHMENT 10 - DIBBS Proposal Instructions.pdf
ATTACH_ATTACHMENT_11__SPE300_25_R_0002 __STATEMENT_OF_WO RK__PA_NJ_NY	ATTACHMENT 11 - SPE300-25-R-0002 - STATEMENT OF WORK - PA NJ NY.pdf
ATTACH_ATTACHMENT_2__PA_NJ_NY_CATALO G_OF_ITEMS	ATTACHMENT 2 - PA NJ NY CATALOG OF ITEMS . xlsx
ATTACH_ATTACHMENT_3__FPCON	ATTACHMENT 3 - FPCON.pdf
ATTACH_ATTACHMENT_4__JOINT_SUBSISTENC E_POLICY_BOARD__JSP B__DOD_MENU_STANDA RDS	ATTACHMENT 4 - JOINT SUBSISTENCE POLICY BOARD (JSPB) DOD MENU STANDARDS.pdf
ATTACH_ATTACHMENT_5__EDI_IMPLEMENTATI ON_GUIDELINES_FOR_S UBSISTENCE_PRIME_VE NDORS_STORES__	ATTACHMENT 5 - EDI IMPLEMENTATION GUIDELINES FOR SUBSISTENCE PRIME VENDORS (STORES).pdf
ATTACH_ATTACHMENT_6__STORES_AMPS_CU STOMER_VENDOR_REQ UEST	ATTACHMENT 6 - STORES-AMPS CUSTOMER_VENDOR_R EQUEST.pdf
ATTACH_ATTACHMENT_7__FEMA_NOTIFICATIO N_SPREADSHEET	ATTACHMENT 7 - FEMA NOTIFICATION SPREADSHEET.xlsx

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 10 OF 12 PAGES
--------------------	--	---------------------

Attachments (CONTINUED)

Description	File Name
ATTACH_ATTACHMENT_8____Past_Performance_Questionnaire	ATTACHMENT 8 - Past Performance Questionnaire.pdf
ATTACH_ATTACHMENT_9____STORES_NEW_ITEM_REQUEST_PROCESS_FOR_CONTRACTORS	ATTACHMENT 9 - STORES NEW ITEM REQUEST PROCESS FOR CONTRACTORS.pdf

PID Data - Custom Clause

Header
C1

Part 12 Provisions

PROVISIONS ADDED TO PART 12 BY ADDENDUM

252.203-7005 REPRESENTATION RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (SEP 2022) DFARS
252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016) DFARS
H18 DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM (DPAS) RATED AWARDS (FEB 2025)
252.219-7000 ADVANCING SMALL BUSINESS GROWTH (JUN 2023) FAR
252.225-7055 REPRESENTATION REGARDING BUSINESS OPERATIONS WITH THE MADURO REGIME (MAY 2022) DFARS
252.225-7057 PREAWARD DISCLOSURE OF EMPLOYMENT OF INDIVIDUALS WHO WORK IN THE PEOPLE'S REPUBLIC OF CHINA (AUG 2022) DFARS
252.225-7966 PROHIBITION REGARDING RUSSIAN FOSSIL FUEL BUSINESS OPERATIONS - REPRESENTATION (CLASS DEVIATION 2024-O0006, REVISION 1) (MAR 2024) DFARS

Use the following provision in solicitations that include the clause at 252.225-7967:

- (a) *Definitions.* The terms *business operations* and *fossil fuel company* have the meanings given in the 252.225-7967 clause of this solicitation.
- (b) *Representation.* By submission of an offer, the Offeror represents it is not, or that it does not knowingly have fossil fuel business operations with an entity or individual that is, 50 percent or more owned, individually or collectively, by --
- (1) An authority of the government of the Russian Federation; or
 - (2) A fossil fuel company that operates in the Russian Federation, except if the fossil fuel company transports oil or gas --
 - (i) Through the Russian Federation for sale outside of the Russian Federation; and
 - (ii) That was extracted from a country other than the Russian Federation with respect to the energy sector of which the President has not imposed sanctions as of the date on which the contract is awarded.

(End of provision)

L06 AGENCY PROTESTS (DEC 2016)

252.204-7016 COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES---REPRESENTATION (DEC 2019) DFARS

As prescribed in [204.2105](#) (a), use the following provision:

- (a) *Definitions.* As used in this provision, “covered defense telecommunications equipment or services” has the meaning provided in the clause 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.
- (b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered defense telecommunications equipment or services”.
- (c) *Representation.* The Offeror represents that it [] does, [] does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

252.204-7024 NOTICE ON THE USE OF THE SUPPLIER PERFORMANCE RISK SYSTEM (MAR 2023) DFARS

252.209-7011 REPRESENTATION FOR RESTRICTION ON THE USE OF CERTAIN INSTITUTIONS OF HIGHER EDUCATION (OCT 2023) FAR

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 11 OF 12 PAGES
--------------------	--	---------------------

Part 12 Provisions (CONTINUED)

252.239-7098 PROHIBITION ON CONTRACTING TO MAINTAIN OR ESTABLISH A COMPUTER NETWORK UNLESS SUCH NETWORK IS DESIGNED TO BLOCK ACCESS TO CERTAIN WEBSITES--REPRESENTATION (DEVIATION 2021-O0003) (APR 2021)

Include the following provision in all solicitations, including solicitations for the acquisition of commercial items under FAR part 12, that will use funds made available by the Consolidated Appropriations Act, 2021 (Pub. L. 116-260), or any other Act that extends to fiscal year 2021 funds the same prohibitions as contained in section 8116, division C, title VIII, of the Consolidated Appropriations Act, 2021 (Pub. L. 116-260).

(a) In accordance with section 8116 of Division C of the Consolidated Appropriations Act, 2021 (Pub. L. 116-260), or any other Act that extends to fiscal year 2021 funds the same prohibitions, none of the funds appropriated (or otherwise made available) by this or any other Act for DoD may be used to enter into a contract to maintain or establish a computer network unless such network is designed to block access to pornography websites. This prohibition does not limit the use of funds necessary for any Federal, State, tribal, or local law enforcement agency or any other entity carrying out criminal investigations, prosecution, or adjudication activities, or for any activity necessary for the national defense, including intelligence activities.

(b) *Representation.* By submission of its offer, the Offeror represents that it is not providing as part of its offer a proposal to maintain or establish a computer network unless such network is designed to block access to pornography websites.

(End of provision)

52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021) FAR

As prescribed in 4.2105(a), insert the following provision:

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it “does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument” in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services --Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Products and Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it “does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services” in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) *Definitions.* As used in this provision-

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to --

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to --

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered telecommunications equipment or services.”

(d) *Representations.* The Offeror represents that --

(1) It [] will, [] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds “will” in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that --

It [] does, [] does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds “does” in paragraph (d)(2) of this section.

(e) *Disclosures.* (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded “will” in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment --

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-25-R-0002	PAGE 12 OF 12 PAGES
--------------------	--	---------------------

Part 12 Provisions (CONTINUED)

(ii) For covered services --

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded “does” in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment --

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services --

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-26 COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES---REPRESENTATION (OCT 2020) FAR

As prescribed in [4.2105\(c\)](#), insert the following provision:

(a) *Definitions.* As used in this provision, “covered telecommunications equipment or services” has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

(c) *Representation.* The Offeror represents that it ☐ does, ☐ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it ☐ does, ☐ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

52.204-29 FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT ORDERS -- REPRESENTATION AND DISCLOSURES (DEC 2023) FAR