TABLE OF CONTENTS

Contents

[SECTION I SCHEDULES 3](#_Toc122634875)

[I.1 SCHEDULE OF SUPPLIES/SERVICES 3](#_Toc122634876)

[I.2 DELIVERY SCHEDULE 3](#_Toc122634877)

[SECTION II CONTRACT CLAUSES 4](#_Toc122634878)

[II.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 4](#_Toc122634879)

[II.2 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017) 4](#_Toc122634880)

[II.3 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (NOV 2021) 4](#_Toc122634881)

[II.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013) 4](#_Toc122634882)

[II.5 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984) 4](#_Toc122634883)

[II.6 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 4](#_Toc122634884)

[II.7 Basic Safeguarding of Covered Contractor Information Systems (Nov 2021) 4](#_Toc122634885)

[II.8 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (DEVIATION 20-05) (DEC 2020) 6](#_Toc122634886)

[II.9 52.204-23 – PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KAPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 20-05) 8](#_Toc122634887)

[II.10 52.227-14 RIGHTS IN DATA—GENERAL (MAY 2014) 9](#_Toc122634888)

[II.11 Rights in Data-Special Works (Dec 2007) 13](#_Toc122634889)

[II.12 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984) 14](#_Toc122634890)

[II.13 3052.209-72 ORGANIZATIONAL CONFLICT OF INTEREST (JUN 2006) 14](#_Toc122634891)

[II.14 3052.209-73 LIMITATION OF FUTURE CONTRACTING (JUN 2006) 15](#_Toc122634892)

[II.15 3052.209-75 PROHIBITED FINANCIAL INTERESTS FOR LEAD SYSEMS INTEGRATORS (JUL 2010) 15](#_Toc122634893)

[II.16 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012) 16](#_Toc122634894)

[II.17 NON-PERSONAL SERVICE (MAR 2003) 17](#_Toc122634895)

[II.18 CONTRACT TYPE (OCT 2008) 18](#_Toc122634896)

[II.19 PERIOD OF PERFORMANCE (MAR 2003) 18](#_Toc122634897)

[II.20 CONTRACTING OFFICER'S AUTHORITY (MAR 2003) 18](#_Toc122634898)

[II.21 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2014) 18](#_Toc122634899)

[II.22 HOLIDAYS AND ADMINISTRATIVE LEAVE (OCT 2021) 19](#_Toc122634900)

[II.23 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (AUG 2022) 20](#_Toc122634901)

[II.24 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003) 20](#_Toc122634902)

[II.25 SECURITY PROCEDURES (AUG 2022) 20](#_Toc122634903)

[II.26 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (AUG 2022) 25](#_Toc122634904)

[II.27 ADDITIONAL CONTRACTOR PERSONNEL REQUIREMENTS (OCT 2007) 26](#_Toc122634905)

[II.28 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015) 26](#_Toc122634906)

[II.29 DISCLOSURE OF INFORMATION 32](#_Toc122634907)

[II.30 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015) 32](#_Toc122634908)

[II.31 SPECIFICATIONS, STATEMETN OF WORK, STATEMENT OF OBJECTIVES OR PERFORMANCE WORK STATEMENT ATTACHED (JUN 2013) 33](#_Toc122634909)

[II.32 TERM OF THE CONTRACT 33](#_Toc122634910)

[II.33 BPA ORDERING 34](#_Toc122634911)

[Attachment No. Attachment Title 34](#_Toc122634912)

[SECTION III SOLICITATION PROVISIONS 36](#_Toc122634913)

[III.1 52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIOSN AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021) 36](#_Toc122634914)

[III.2 52.204-26 COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES-REPRESENTATION (OCT 2020) 38](#_Toc122634915)

[III.3 52.216-1 TYPE OF CONTRACT (APR 1984) 38](#_Toc122634916)

[III.4 52.216-31 Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Acquisition (Nov 2021) 38](#_Toc122634917)

[III.5 52.217-5 EVALUATION OF OPTIONS (JUL 1990) 38](#_Toc122634918)

[III.6 AGENCY LEVEL PROTEST NOTICE (APR 2003) 38](#_Toc122634919)

[III.7 QUESTIONS/CLARIFICATIONS REGARDING THIS SOLICITATION 39](#_Toc122634920)

[III.8 SELECT BEST-SUITED, THEN NEGOTIATE 39](#_Toc122634921)

[III.9 INSTRUCTIONS FOR THE PREPARATION AND SUBMISSION OF QUOTATIONS (OCT 2008) 39](#_Toc122634922)

[III.10 GENERAL QUOTATION INFORMATION 45](#_Toc122634923)

[III.11 EVALUATION CRITERIA 45](#_Toc122634924)

[III.12 BASIS OF AWARD (TRADEOFF ANALYSIS) (JUN 2007) 48](#_Toc122634926)

1. SCHEDULES
   1. SCHEDULE OF SUPPLIES/SERVICES

**[TO BE INSERTED UPON AWARD]**

**See Attachment 2 – Pricing Template Tab 1 (Pricing Schedule)**

* 1. DELIVERY SCHEDULE

**[TO BE INSERTED UPON AWARD/SEE DELIVERABLE SCHEDULE]**

1. CONTRACT CLAUSES
   1. 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

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):

www.acquisition.gov

I. FEDERAL ACQUISITION REGULATION (48 CHAPTER 1) CLAUSES

NUMBER TITLE

* 1. 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)
  2. 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (NOV 2021)
  3. 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)
  4. 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)
  5. 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

1. The Government may extend the term of this agreement by written notice to the Contractor within any time prior to BPA ordering period expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the agreement expires. The preliminary notice does not commit the Government to an extension.
2. If the Government exercises this option, the extended agreement shall be considered to include this option clause.
3. The total duration of this agreement, including the exercise of any options under this clause, shall not exceed five (5) years.

(End of clause)

* 1. Basic Safeguarding of Covered Contractor Information Systems (Nov 2021)

      (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 websites) 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](http://uscode.house.gov/browse.xhtml;jsessionid=114A3287C7B3359E597506A31FC855B3)).

           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 products or commercial services, 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.

(End of clause)

* 1. 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (DEVIATION 20-05) (DEC 2020)

(a) Definitions. As used in this clause—

“Backhaul” means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

“Covered foreign country” means The People’s Republic of China.

“Covered telecommunications equipment or services” means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

“Critical technology” means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

“Interconnection arrangements” means arrangements governing the physical connection of two or more networks to allow the use of another’s network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

“Reasonable inquiry” means an inquiry designed to uncover any information in the entity’s possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

“Roaming” means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

“Substantial or essential component” means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(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. The Contractor is prohibited from providing to the Government 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, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(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, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. 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.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer’s Representative, and the Network Operations Security Center (NOSC) at [NDAA\_Incidents@hq.dhs.gov](mailto:NDAA_Incidents@hq.dhs.gov), with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at [https://dibnet.dod.mil](https://dibnet.dod.mil/). For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer’s Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at [https://dibnet.dod.mil](https://dibnet.dod.mil/).

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e)and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

[End of Clause]

* 1. 52.204-23 – PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KAPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 20-05)

1. Definitions. As used in this clause --

“*Covered article*” means any hardware, software, or service that –

* 1. Is developed or provided by a covered entity;
  2. Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or
  3. Contains components using any hardware or software developed in whole or in part by a covered entity. “*Covered entity*” means --

1. Kaspersky Lab;
2. Any successor entity to Kaspersky Lab;
3. Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
4. Any entity of which Kaspersky Lab has a majority ownership.
5. *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from --
   1. Providing any covered article that the Government will use on or after October 1, 2018; and
   2. Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.
6. *Reporting requirement*.
   1. In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer’s Representative, and the Enterprise Security Operations Center (SOC) at [NDAA\_Incidents@hq.dhs.gov,](mailto:NDAA_Incidents@hq.dhs.gov) with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at [https://dibnet.dod.mil.](https://dibnet.dod.mil/) For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Page 5 of 8 Officer(s) and Contracting Officer’s Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.
   2. The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:
      1. Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
      2. Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(c) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

* 1. 52.227-14 RIGHTS IN DATA—GENERAL (MAY 2014)

1. *Definitions.* As used in this clause--

*Computer database or database* means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

*Computer software--* (1) Means (i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation. Computer software documentation means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

*Data* means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

*Form, fit, and function data* means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

*Limited rights* means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

*Limited rights data* means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

*Restricted computer software* means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

*Restricted rights*, as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

*Technical data*, means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 116).

*Unlimited rights* means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

1. *Allocation of rights.* (1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in--
   1. Data first produced in the performance of this contract;
   2. Form, fit, and function data delivered under this contract;
   3. Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and
   4. All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to--

1. Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;
2. Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;
3. Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and
4. Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.
5. *Copyright--* (1) *Data first produced in the performance of this contract.* (i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.
6. When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17

U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

1. For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.
2. *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor--
   1. Identifies the data; and
   2. Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.
3. *Removal of copyright notices*. The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.
4. *Release, publication, and use of data*. The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except--
5. As prohibited by Federal law or regulation (e.g., export control or national security laws or regulations);
6. As expressly set forth in this contract; or
7. If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.
8. *Unauthorized marking of data*. (1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g)
9. if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.
   1. The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;
   2. If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.
   3. If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.
10. The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.
11. Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.
12. *Omitted or incorrect markings*. (1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.
13. If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor--
    1. Identifies the data to which the omitted notice is to be applied;
    2. Demonstrates that the omission of the notice was inadvertent;
    3. Establishes that the proposed notice is authorized; and
    4. Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.
14. If data has been marked with an incorrect notice, the Contracting Officer may--
    1. Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or
    2. Correct any incorrect notices.
15. *Protection of limited rights data and restricted computer software*. (1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and
    1. of this clause. As a condition to this withholding, the Contractor shall--
       1. Identify the data being withheld; and
       2. Furnish form, fit, and function data instead.
16. Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.
17. [Reserved]

*Subcontracting*. The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

1. *Relationship to patents or other rights*. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

* 1. Rights in Data-Special Works (Dec 2007)

      (a) Definitions. As used in this clause-

      Data means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

      Unlimited rights means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

      (b) Allocation of Rights.

(1) The Government shall have-

                (i) Unlimited rights in all data delivered under this contract, and in all data first produced in the performance of this contract, except as provided in paragraph (c) of this clause.

                (ii) The right to limit assertion of copyright in data first produced in the performance of this contract, and to obtain assignment of copyright in that data, in accordance with paragraph (c)(1) of this clause.

                (iii) The right to limit the release and use of certain data in accordance with paragraph (d) of this clause.

           (2) The Contractor shall have, to the extent permission is granted in accordance with paragraph (c)(1) of this clause, the right to assert claim to copyright subsisting in data first produced in the performance of this contract.

      (c) Copyright-

(1) Data first produced in the performance of this contract.

(i) The Contractor shall not assert or authorize others to assert any claim to copyright subsisting in any data first produced in the performance of this contract without prior written permission of the Contracting Officer. When copyright is asserted, the Contractor shall affix the appropriate copyright notice of [17 U.S.C. 401 or 402](http://uscode.house.gov/browse.xhtml;jsessionid=114A3287C7B3359E597506A31FC855B3) and acknowledgment of Government sponsorship (including contract number) to the data when delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. The Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license for all delivered data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

                (ii) If the Government desires to obtain copyright in data first produced in the performance of this contract and permission has not been granted as set forth in paragraph (c)(1)(i) of this clause, the Contracting Officer shall direct the Contractor to assign (with or without registration), or obtain the assignment of, the copyright to the Government or its designated assignee.

           (2) Data not first produced in the performance of this contract. The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract and that contain the copyright notice of [17 U.S.C. 401 or 402](http://uscode.house.gov/browse.xhtml;jsessionid=114A3287C7B3359E597506A31FC855B3), unless the Contractor identifies such data and grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

      (d) Release and use restrictions. Except as otherwise specifically provided for in this contract, the Contractor shall not use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.

      (e) Indemnity. The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor’s consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies.

(End of clause)

* 1. 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

1. The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of (DEVIATION) after the date of the clause.
2. The use in this solicitation or contract of any [www.acquisition.gov/hsar](http://www.acquisition.gov/hsar) clause with an authorized deviation is indicated by the addition of (DEVIATION) after the name of the regulation.

(End of clause)

* 1. 3052.209-72 ORGANIZATIONAL CONFLICT OF INTEREST (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting: There could be concerns that the Contractor could occupy an influential and responsible position in recommending Cloud Service Providers (CSP) and software for use in CSPs. Thus, the ECIS Contractors could potentially be able to influence decisions favoring its own or partners’ products or capabilities.

(b) If any such conflict of interest is found to exist, the Contracting Officer may

(1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

\_(1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

\_(2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this clause.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this clause do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this clause.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of clause)

* 1. 3052.209-73 LIMITATION OF FUTURE CONTRACTING (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5 - Organizational Conflicts of Interest.

(b) The nature of this conflict is: There could be concerns that the Contractor could occupy an influential and responsible position in recommending Cloud Service Providers (CSP) and software for use in CSPs. Thus, the ECIS Contractors could potentially be able to influence decisions favoring its own or partners’ products or capabilities.

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this BPA, or through the performance of tasks pursuant to this BPA, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this BPA.

(2) To the extent that the work under this BPA requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

* 1. 3052.209-75 PROHIBITED FINANCIAL INTERESTS FOR LEAD SYSEMS INTEGRATORS (JUL 2010)

(a) Definitions. As used in this clause -

(1) “Direct financial interest,” for the purpose of this clause and contract, and subject to exceptions set forth 6 U.S.C. 396(b) as implemented, means:

(i) Developing or constructing any individual system or element of any system of systems for which the Contractor is the lead system integrator;

(ii) Owning or being in a position to exert corporate control over a subcontractor at any level under the prime contract;

(iii) Owning, or being in a position to exert corporate control over an entity that either -

(A) Is a subcontractor at any level under the prime contract, or

(B) Owns or is in a position to control another entity that is a subcontractor at any level under the prime contract; and

(iv) Participating or sharing in the profits of another firm's development or construction of any individual system or element of any system of systems for which the Contractor is the lead system integrator or agreeing to participate in the profits of the firm from such development or construction.

(2) “Lead system integrator” includes “lead system integrator with system responsibility” and “lead system integrator without system responsibility.”

(3) “Lead system integrator with system responsibility” means a prime contractor for the development or production of a major system, if the prime contractor is not expected at the time of award to perform a substantial portion of the work on the system and the major subsystems.

(4) “Lead system integrator without system responsibility” means a prime contractor under a contract for the procurement of services, the primary purpose of which is to perform acquisition functions closely associated with inherently governmental functions (see section 7.503(d) of the Federal Acquisition Regulation) with regard to the development or production of a major system.

(5) The phrase “substantial portion of the work,” as used in the definition of “lead system integrator with system responsibility,” may relate to the dollar value of the effort or to the criticality of the effort performed.

(b) Limitations. The Contracting Officer has determined that the Contractor meets the definition of lead system integrator with [ ] without [X ] system responsibility. Unless an exception is granted, the Contractor shall not have any direct financial interest in the development or construction of any individual system or element of any system of systems while performing lead system integrator functions in the acquisition of a major system by the Department of Homeland Security under this contract.

(c) Agreement. The Contractor agrees that during performance of this contract it will not acquire any direct financial interest as described in paragraph (b) of this clause, or, if it does acquire or plan to acquire such interest, it will immediately notify the Contracting Officer. The Contractor further agrees to provide to the Contracting Officer all relevant information regarding the change in financial interests so that the Contracting Officer can determine whether an exception applies or whether the Contractor will be allowed to continue performance on this contract. If an organizational conflict of interest in the performance of this contract that is attributable to the Contractor's direct financial interest cannot be avoided, eliminated, or mitigated to the Contracting Officer's satisfaction, the Contracting Officer may terminate this contract for default or may take other remedial measures as appropriate in the Contracting Officer's sole discretion.

(d) Notwithstanding any other clause of this contract, if the Contracting Officer determines that the Contractor misrepresented its financial interests at the time of award or has violated the agreement in paragraph (c) of this clause, the Government may terminate this contract for default or may take other remedial measures as appropriate in the Contracting Officer's sole discretion.

(e) This clause implements the requirements of 6 U.S.C. 396, as added by Section 6405 of the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, And Iraq Accountability Appropriations Act, 2007 (Pub. L. 110-28).

(End of clause)

* 1. 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(a) Provisions.

[ ] 3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

[ ] 3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

[ ] 3052.247-70 F.o.B. Origin Information.

[ ] Alternate I

[ ] Alternate II

[ ] 3052.247-71 F.o.B. Origin Only.

[ ] 3052.247-72 F.o.B. Destination Only.

(b) Clauses.

[X ] 3052.203-70 Instructions for Contractor Disclosure of Violations.

[ ] 3052.204-70 Security Requirements for Unclassified Information Technology Resources.

[X ] 3052.204-71 Contractor Employee Access.

[X ] Alternate I

[X ] 3052.205-70 Advertisement, Publicizing Awards, and Releases.

[X ] AlternateI

[ ] 3052.209-72 Organizational Conflicts of Interest.

[ ] 3052.209-73 Limitation on Future Contracting.

[ ] 3052.215-70 Key Personnel or Facilities.

[ ] 3052.216-71 Determination of Award Fee.

[ ] 3052.216-72 Performance Evaluation Plan.

[ ] 3052.216-73 Distribution of Award Fee.

[ ] 3052.219-71 DHS Mentor Protégé Program.

[ ] 3052.228-70 Insurance.

[ ] 3052.236-70 Special Provisions for Work at Operating Airports.

[X ] 3052.242-72 Contracting Officer’s Representative.

(End of clause)

* 1. NON-PERSONAL SERVICE (MAR 2003)

1. The Government and the contractor agree and understand the services to be performed under this contract are non- personal in nature. The Contractor shall not perform any inherently Governmental functions under this contract as described in Office of Federal Procurement Policy Letter 92-1
2. The services to be performed under this contract do not require the Contractor or his employees to exercise personal judgment and discretion on behalf of the Government, but rather, the Contractor's employees will act and exercise personal judgment and discretion on behalf of the Contractor.
3. The parties also recognize and agree that no employer-employee relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees. Contractor personnel under this contract shall not:
   1. Be placed in a position where there is an appearance that they are employed by the Government or are under the supervision, direction, or evaluation of any Government employee. All individual employee assignments any daily work direction shall be given by the applicable employee supervisor.
   2. Hold him or herself out to be a Government employee, agent or representative or state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as such and specify the name of the company of which they work.
   3. Be placed in a position of command, supervision, administration or control over Government personnel or personnel of other Government contractors, or become a part of the government organization. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to change the contract in any way. If the other Contractor believes this communication to be direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.
4. If the Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the Contractor shall promptly notify the CO of this communication or action.
5. Rules, regulations directives and requirements which are issued by U.S. Customs & Border Protection under their responsibility for good order, administration and security are applicable to all personnel who enter U.S. Customs & Border Protection installations or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

[End of Clause]

* 1. CONTRACT TYPE (OCT 2008)

This is a hybrid Firm-Fixed-Price (FFP), Time and Materials (T&M), and Labor Hour Blanket Purchase Agreement.

[End of Clause]

* 1. PERIOD OF PERFORMANCE (MAR 2003)

The base Ordering Period will be twelve (12) months from date of award with four (4) 12-month option periods. Services will be provided within the United States.

[End of Clause]

* 1. CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this BPA. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the BPA, or to modify any term or condition of the BPA. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed BPA can be incurred before receipt of a fully executed Task Order or specific authorization from the Contracting Officer.

[End of Clause]

* 1. POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2014)

1. Contractor Performance Evaluations

Interim and final performance evaluation reports will be prepared on this contract or order in accordance with FAR Subpart 42.15. A final performance evaluation report will be prepared at the time the work under this contract or order is completed. In addition to the final performance evaluation report, an interim performance evaluation report will be prepared annually to coincide with the anniversary date of the contract or order.

Interim and final performance evaluation reports will be provided to the contractor via the Contractor Performance Assessment Reporting System (CPARS) after completion of the evaluation. The CPARS Assessing Official Representatives (AORs) will provide input for interim and final contractor performance evaluations. The AORs may be Contracting Officer’s Representatives (CORs), project managers, and/or contract specialists. The CPARS Assessing Officials (AOs) are the contracting officers (CO) or contract specialists (CS) who will sign the evaluation report and forward it to the contractor representative via CPARS for comments.

The contractor representative is responsible for reviewing and commenting on proposed ratings and remarks for all evaluations forwarded by the AO. After review, the contractor representative will return the evaluation to the AO via CPARS.

The contractor representative will be given up to fourteen (14) days to submit written comments or a rebuttal statement. Within the first seven (7) calendar days of the comment period, the contractor representative may request a meeting with the AO to discuss the evaluation report. The AO may complete the evaluation without the contractor representative’s comments if none are provided within the fourteen (14) day comment period. Any disagreement between the AO/CO and the contractor representative regarding the performance evaluation report will be referred to the Reviewing Official (RO) within the division/branch the AO is assigned. Once the RO completes the review, the evaluation is considered complete and the decision is final.

Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file and may be used in future award decisions.

1. Designated Contractor Representative

The contractor must identify a primary representative for this contract and provide the full name, title, phone number, email address, and business address to the CO within 30 days after award.

1. Electronic Access to Contractor Performance Evaluations

The AO will request CPARS user access for the contractor by forwarding the contractor’s primary and alternate representatives’ information to the CPARS Focal Point (FP).

The FP is responsible for CPARS access authorizations for Government and contractor personnel. The FP will set up the user accounts and will create system access to CPARS.

The CPARS application will send an automatic notification to users when CPARS access is granted. In addition, contractor representatives will receive an automated email from CPARS when an evaluation report has been completed.

[End of Clause]

* 1. HOLIDAYS AND ADMINISTRATIVE LEAVE (OCT 2021)

U.S. Customs & Border Protection (CBP) personnel observe the following days as holidays:

New Year’s Day Labor Day

Martin Luther King’s Birthday Columbus Day

President’s Day Veteran’s Day

Memorial Day Thanksgiving Day

Juneteenth National Independence Day Christmas Day Independence Day Inauguration Day**\***

**\*** Unless otherwise specified, Inauguration Day is a holiday for federal employees only in the District of Columbia, Montgomery and Prince George's counties in Maryland, Arlington and Fairfax counties in Virginia, and the cities of Alexandria and Falls Church in Virginia. It is also a holiday for district employees in Washington DC.

CBP observes any other day as a federal holiday designated by Federal statute, by Executive Order or by the President's proclamation.

When any such day falls on a Saturday, the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule or period of performance or adjustment to the price, except as set forth in the contract.

Except for designated around-the-clock or emergency operations, and/or as defined within the statement of requirements, contractor personnel will not be able to perform on site under this contract with CBP on the holidays set forth above. The contractor will not charge any holiday as a direct charge to the contract. In the event Contractor personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

In the event CBP grants administrative leave to its Government employees at the site, on-site contractor personnel shall also be dismissed if the site is being closed. However, the Contractor shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the Contracting Officer or her/his duly appointed representative. In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances; the Contractor will direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the Contractor for the period of any such site closure are a reimbursable item of direct cost under the contract for employees whose regular time is normally a direct charge if they continue to perform contract work; otherwise, costs incurred because of site closure are reimbursable as indirect cost in accordance with the Contractor's established accounting policy.

[End of Clause]

* 1. ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (AUG 2022)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U.S. Department of the Treasury's Invoice Processing Platform System (IPP).

"*Payment request*" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice [*CO to edit and include the documentation required under this contract*]*:*

-See FAR 52.232-7\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

[End of Clause]

* 1. GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

* 1. SECURITY PROCEDURES (AUG 2022)

**I. PERSONNEL SECURITY**

**A. CBP Suitability Requirements**

1. All Contractor Employees requiring access to CBP facilities and its information technology networks and systems must undergo an investigation to determine suitability for employment. Based on the position sensitivity designation, OPR/Personnel Security Division initiates either a T4 or T5 Background Investigation in accordance with CBP Personnel Security Handbook, HB 1400-07A.

2. Contractor Employees who require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with DHS Instruction 121-01-007-01, Revision 1, Chapter 2, Personnel Security Program Standards, § 13, and Citizenship Requirements, § 13F. (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01, Revision 01.

3. Provided the requirements of DHS Instruction Handbook 121-01-007-01 are met as outlined in paragraph I.B.1, below, Contractor Employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated Tier 4 (T4) or Tier 5 (T5) background investigation (U.S. Office of Personnel Management (OPM), Suitability Executive Agent and the Director of National Intelligence (DNI), Security Executive Agent, Federal Investigative Standards, December 2012, or its successor), prior to commencing work on this contract, as outlined in the applicable requirements document, such as a Statement of Work (SOW) or Performance Work Statement (PWS). Exceptions shall be approved on a case-by-case basis with the Contractor Employee’s access to facilities, systems, and information limited until the Contractor Employee receives a favorably adjudicated T4 or T5. A favorably adjudicated T4 or T5 shall include various aspects of a Contractor Employee’s life, including employment, education, residences, police, and court inquires, credit history, and national agency checks.

4. For contracts requiring Contractor Employees to possess a CBP suitability upon contract inception, the following is applicable: The Contractor shall submit, within ten (10) working days after award of the contract, a list containing the full legal name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated T4 or T5 background investigations that meet federal investigation standards (as mandated in the SOW/PWS). These individuals will be considered for “reciprocity” as applicable (reference CBP Form 78 – BIRD). For contracts not requiring Contractor Employees to possess a CBP suitability upon contract inception, the following is applicable: The Contractor shall require Contractor Employee candidates, needing a T4 or T5 background investigation for the contract, to submit information and documentation requested by CBP to initiate the background investigation process immediately upon request by CBP.

5. Background Investigation information and documentation are submitted by proper completion of standard federal and agency forms provided by the COR, such as Electronic Questionnaires for Investigations Processing (e-QIP), Electronic Fingerprint Submission, CBP Form 78-Background Investigation Requirements Determination (BIRD) Form, Fair Credit Reporting Act (FCRA), Non-Disclosure Agreement (NDA), a Contractor Employee initial Background Investigation Form (CBP Form 77) (Sections A and B), and relevant “clearance” documents (if applicable), etc. The Contractor is responsible for ensuring all Contract Employee candidates complete the Electronic Questionnaire for Investigations Processing (e-QIP) and Electronic Fingerprints using their full legal name, correct SSN and ensuring these actions are completed in a timely manner, within 30 days of e-QIP initiation. The Contractor is also responsible for ensuring all Contract Employee candidates respond to phone calls and check their emails regularly for communications from the CBP Security Office and/or the field investigator for any necessary actions. The appropriate forms, to include “clearance” documents if applicable, must be submitted to the COR assigned to the contract, and the COR shall forward the completed forms to the CBP security official that will review the information for completeness and begin the adjudication and “clearance” (if applicable) process. Any Contract Employee candidate who fails to comply after multiple requests and attempts to reach them will be discontinued from the Background Investigation process. The Contractor shall then propose a qualified replacement employee candidate to the CO and COR within 30 days after being notified of the discontinued Contract Employee candidate.

6. CBP cannot provide a standard completion time for a T4 or T5 background investigation as many scenarios affect CBP’s ability to process an individual. During the term of this contract, the Contractor is required to provide the names of its employees who successfully complete the CBP T4 or T5 process to the CO and COR. Failure of any Contractor Employee to obtain and maintain a favorably adjudicated T4 or T5 shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel Contractor Employees, the Contractor shall propose a qualified replacement employee candidate to the COR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COR shall approve or disapprove replacement employees. For contracts requiring Contractor Employees to possess a CBP suitability per SOW/PWS requirements, continuous failure to provide Contractor Employees who meet CBP T4 or T5 requirements may be cause for termination of the contract (refer #4).

**B. Security Clearance Requirements**

1. Contractor Employees who require access to classified information must be U.S. citizens or have Lawful Permanent Resident (LPR) status in accordance with DHS Instruction Handbook 121-01-007-01, Rev. 01, the Department of Homeland Security Personnel Security, Suitability and Fitness Program, Chapter 2, Personnel Security Program Standards, § 13, Citizenship Requirements. A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.

2. For contracts requiring Contractor Employees to possess a security clearance *upon contract inception*, the following is applicable: The Contractor shall submit, within ten (10) working days after award of the contract, a list containing the full legal name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated T5 background investigations that meet federal investigation standards (as mandated in the SOW/PWS). These individuals will be considered for “reciprocity” as applicable (refer to CBP Form 78 – BIRD). For contracts not requiring Contractor Employees to possess a security clearance *upon contract inception*, the following is applicable: The Contractor shall require Contractor Employee candidates, needing a T4 or T5 background investigation for the contract, to submit information and documentation requested by CBP to initiate the background investigation process immediately upon request by CBP.

3. Background Investigation information and documentation are submitted by proper completion of standard federal and agency forms provided by the COR, such as Electronic Questionnaires for Investigations Processing (e-QIP), Electronic Fingerprint Submission, CBP Form 78-Background Investigation Requirements Determination (BIRD) Form, Fair Credit Reporting Act (FCRA), Non-Disclosure Agreement (NDA), a Contractor Employee Initial Background Investigation Form (CBP Form 77) (Sections A and B), and relevant “clearance” documents (if applicable), etc. The Contractor is responsible for ensuring all Contract Employee candidates complete the Electronic Questionnaire for Investigations Processing (e-QIP) and Electronic Fingerprints using their full legal name, correct SSN and ensuring these actions are completed in a timely manner, within 30 days of e-QIP initiation. The Contractor is also responsible for ensuring all Contract Employee candidates respond to phone calls and check their emails regularly for communications from the CBP Security Office and/or the field investigator for any necessary actions. The appropriate forms, to include “clearance” documents if applicable, must be submitted to the COR assigned to the contract, and the COR shall forward the completed forms to the CBP security official that will review the information for completeness and begin the adjudication and “clearance” (if applicable) process. Any Contract Employee candidate who fails to comply after multiple requests and attempts to reach them will be discontinued from the Background Investigation process. The Contractor shall then propose a qualified replacement employee candidate to the CO and COR within 30 days after being notified of the discontinued Contract Employee candidate.

4. CBP cannot provide a standard completion time for a T4 or T5 background investigation as many scenarios affect CBP’s ability to process an individual. During the term of this contract, the Contractor is required to provide the names of its employees who successfully complete the CBP T4 or T5 process to the CO and COR. Failure of any Contractor Employee to obtain and maintain a favorably adjudicated T4 or T5 shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel Contractor Employees, the Contractor shall propose a qualified replacement employee candidate to the COR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COR shall approve or disapprove replacement employees. Continuous failure to provide Contractor Employees who meet CBP T4 or T5 requirements may be cause for termination of the contract.

**C. Contractor Tracking System**

1. All Contractor Employees must be entered into the current agency Contractor Tracking System (CTS) database by the COR or Alternate COR. Additionally, the COR/ACOR shall maintain current, accurate and complete data for Contractor Employees during their performance on the contract. The Contractor Project Manager (CPM) shall provide timely start information to the CO/COR or designated government personnel to initiate the CTS entry. Other relevant information will also be needed for Contractor Employee record submission in the CTS database such as, but not limited to, the Contractor Employee’s legal name, brief job description, labor rate, Hash ID, schedule, and location. The CO/COR or designated government personnel shall provide the CPM with instructions for providing required information.

2. The CO/COR may designate responsibility for out-processing to the CPM. The CPM must have an active CBP Background Investigation (BI) and an Active Directory (AD) account (i.e., email, etc.) within the agency. CPM shall provide Contactor Employee departure/separation date and reason for leaving to the CO/COR in accordance with CBP Directive 1210-007B, Tracking of Contractor Employees. Failure by the CPM to provide timely notification of Contractor Employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel complete a Contractor Performance Report (under Business Relations) or other performance related measures.

**II. CONTROLS**

A. Access Controls.

1. The Contractor Employee shall comply with the U.S. Customs and Border Protection’s (CBP) administrative, physical, and technical security controls to ensure that the Government’s security requirements are met.

2. All Contractor Employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor Employees’ departure/separation, all badges, valid HSPD-12 compliant Personal Identity Verification (PIV) card, building passes, parking permits, keys, and pass cards must be returned to the Contracting Officer’s Representative (COR). The COR shall immediately notify the cognizant Physical Security official to ensure that access to all buildings, and facilities, and network are revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Professional Responsibility, Security Management Division (OPR/SMD) shall be notified immediately, if building access is revoked.

3. Contractor Employees in possession of a valid HSPD-12 compliant PIV card are authorized to access Department Headquarters and DHS Component Headquarters while on official business, in accordance with DHS Instruction Manual # 121-01-011-01, Revision # 00.

4. Contractor Employees may be subject to random security screening upon entering certain CBP facilities.

5. Contractor Employees who do not have their PIV cards must sign-in at lobby guard desk, and show a federal, state, or local government-issued photo identification (e.g., driver’s license that meets the requirements of the REAL ID Act of 2005, US passport, US military ID card, Tribal ID, or Permanent Residence card).

B. Visitor Security Management.

1. Visitors accessing any DHS Headquarters or DHS Component Headquarters facilities are subject to a criminal history check utilizing the National Crime Information Center (NCIC) system, except as stipulated elsewhere in DHS Instruction Manual # 121-01-011-01, Revision # 00.

2. All visitors requesting access to CBP facilities are required to sign-in at designated visitor location, depending on the facility’s resources. Visitors are required to show a federal, state, or local government-issued photo identification (e.g., driver’s license that meets the requirements of the REAL ID Act of 2005, US passport, US military ID card, Tribal ID, or Permanent Residence card), unless otherwise directed by the Facility Security Manager (FSM) or CBP Assistant Technical Representative (ATR).

3. Visitors must be escorted to their intended CBP destination by CBP employees or CBP contractors with a valid CBP-issued PIV card capable of operating the turnstiles. Supplemental access cards cannot be used for escorting purposes without a valid CBP-issued PIV card.

4. Visitor passes will be issued only at designated locations and/or entrances. All visitors are required to pass through screening at the designated entrances. All visitors must be escorted back to the security desk by a CBP employee or CBP contractor.

**III. INFORMATION SECURITY REQUIREMENTS**

A. Managing Sensitive Security Information.

1. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor Employee shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.

2. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract.

3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Sensitive Systems Policy Directive 4300A, v.13.1, DHS Sensitive Systems Handbook 4300A, v.12.0, or latest available version, and CBP Information Security Handbook (HB 1400-04A).

4. Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

● Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

● Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, “Protection of Sensitive Security Information,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

● Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

● Any information that is designated “sensitive” or subject to other controls, safeguards, or protections in accordance with subsequently adopted homeland security information handling procedures.

B. Managing Classified Information.

1. Contracts requiring contractor employees to access Classified National Security Information, completion of the DD Form 254 (Contract Security Classification Specification) is necessary for the Contractor (the company) to establish and have on record. Additionally, FAR Clause 52.204-2, Security Requirements, must be included in the solicitation and contract. If desired, a Solicitation DD Form 254 can be added to the solicitation package. Contact the Security Management Division (SMD) for assistance at: [cbpsecurity@cbp.dhs.gov](mailto:cbpsecurity@cbp.dhs.gov).

2. For additional information about the National Industrial Security Program (NISP) please visit the Defense Counterintelligence and Security Agency website and search for The NISPOM Rule.

**IV. GENERAL SECURITY RESPONSIBILITIES**

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable Contractor Employees shall be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

2. The CO/COR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public’s interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.

3. Upon completion of this contract, the Contractor Employee shall return all sensitive information used in the performance of the contract to the CO/COR. The Contractor shall certify, in writing, that all sensitive and non-public information have been purged from any Contractor-owned system.

4. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor Employee shall comply with all security policies contained in CBP Handbook 1400-05D, v.7.0, Information Systems Security Policies and Procedures Handbook, or latest available version.

**V. NOTIFICATION OF CONTRACTOR EMPLOYEE CHANGES**

1. The Contractor or CPM shall notify the CO/COR via phone or electronic transmission, immediately after a personnel change becomes known or no later than five (5) business days prior to departure of the Contractor Employee. Telephone notifications must be immediately followed up in writing. CPM’s notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

2. The CPM shall notify the CO/COR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change.

**VI. NON-DISCLOSURE AGREEMENTS**

As part of the background investigation package, Contractor Employees are required to execute and submit a Non-Disclosure Agreement (DHS Form 11000-6) as a condition to perform on any CBP contract.

[End of Clause]

* 1. SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (AUG 2022)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Homeland Security (DHS) contract by pre-screening the person/candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirement is considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months, illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

a. Felony convictions within the past 36 months: An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).

b. Pending/open/unresolved criminal charges of any nature: An acceptable means of obtaining information related to unresolved criminal charges is through employee self-certification, by public records check, or other reference checks conducted in the normal course of business.

c. Illegal drug use within the past 12 months: An acceptable means of obtaining information related to drug use is through employee self-certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.

d. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months: An acceptable means of obtaining information related to misconduct is through employee self-certification, by public records check, or other reference checks conducted in the normal course of business.

2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username, and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

* 1. ADDITIONAL CONTRACTOR PERSONNEL REQUIREMENTS (OCT 2007)

The Contractor will ensure that its employees will identify themselves as employees of their respective company while working on U.S. Customs & Border Protection (CBP) contracts. For example, contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.

The contractor will ensure that their personnel use the following format signature on all official e-mails generated by CBP computers:

[Name]

(Contractor)

[Position or Professional Title] [Company Name]

Supporting the XXX Division/Office

U.S. Customs & Border Protection

[Phone]

[FAX]

[Other contact information as desired]

[End of Clause]

* 1. SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

*“Personally Identifiable Information (PII)”* means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

*“Sensitive Information”* is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

*“Sensitive Information Incident”* is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

*“Sensitive Personally Identifiable Information (SPII)”* is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status

(4) Ethnic or religious affiliation

(5) Sexual orientation

(6) Criminal History

(7) Medical Information

(8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer’s Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor’s invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government’s acceptance of the ATO does not alleviate the Contractor’s responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor’s system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor’s facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole).  If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information.  These measures may include restricting access to sensitive information on the Contractor IT system under this contract.  Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer’s email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor’s use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

[End of Clause]

* 1. DISCLOSURE OF INFORMATION

1. General

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.

1. Technical Data Rights

The Contractor shall not use, disclose, reproduce, or otherwise divulge or transfuse to any persons any technical information or data licensed for use by the Government that bears any type of restrictive or proprietary legend except as may be necessary in the performance of the contract. Refer to the Rights in Data clause for additional information.

1. Privacy Act

In performance of this contract the Contractor assumes the responsibility for protection of the confidentiality of all Government records and/or protected data provided for performance under the contract and shall ensure that (a) all work performed by any subcontractor is subject to the disclosure restrictions set forth above and (b) all subcontract work be performed under the supervision of the Contractor or their employees.

[End of Clause]

* 1. INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer’s Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

[End of Clause]

* 1. SPECIFICATIONS, STATEMETN OF WORK, STATEMENT OF OBJECTIVES OR PERFORMANCE WORK STATEMENT ATTACHED (JUN 2013)

The Specifications, Statement of Work, Statement of Objectives or Performance Work Statement which describe the work to be performed hereunder, although attached, is incorporated and made a part of this document with the same force and effect of “specifications” as described in the clause, Order of Precedence, FAR 52.212-4(s) incorporated herein by reference.

[End of Clause]

* 1. TERM OF THE CONTRACT

The Ordering term of this Blanket Purchase Agreement (BPA) includes a base period of ttwelve (12) months from date of award with four (4) 12-month option periods.

[End of Clause]

* 1. BPA ORDERING

**ORDERING PERIOD**

Orders may be issued from the date of award of this BPA through five (5) years, if all options are exercised. Orders may extend twelve (12) months beyond the BPA term.

**MINIMUM AMOUNT/EXTENT OF OBLIGATION**

The Government is obligated only to the extent of authorized Orders made under the BPA. There is no guaranteed minimum quantity of supplies or services the Government agrees to order under this solicitation.

The anticipated BPA does not obligate any funding. The individual Task Orders placed against the contract will obligate the funding.

**AUTHORIZED TO USE THE BPA**

Only CBP Contracting Officers are authorized to place Orders under the BPA.

**INSTRUCTIONS FOR SUBMITTING DELIVERABLES**

Submission of deliverables shall be coordinated with the ordering CBP Contracting Officer or Contracting Officer designated representative.

[End of Clause]

**I.35 PRICING PROVISIONS FOR TASK ORDER OR BLANKET PURCHASE AGREEMENT ISSUED UNDER A FEDERAL SUPPLY SCHEDULE (JUN 2005)**

This Blanket Purchase Agreement (BPA) is placed under the terms and conditions of the GSA Federal Supply Schedule contract identified herein. The contractor warrants that, throughout performance, the prices charged the Government shall be as low as, or lower than, those charged the contractor's most favored customers and that the Government shall never be charged more under this order than the offeror/contractor’s current GSA schedule rates, or the rates contained in the BPA Price Schedule, whichever are lower.

If this order contains options for additional periods of performance, U.S. Customs & Border Protection (CBP) will invoke the option only if the offeror/contractor maintains a current GSA schedule. Unilateral options will not be invoked if the rates indicated in the task order schedule for the option are higher than current GSA schedule rates, but may be invoked bilaterally at the offeror/contractor's current GSA rates. The contractor shall provide notice to the Government of any proposed and/or approved change to the GSA schedule rates. Failure to comply with the provisions of this price warranty may be cause for termination of the order and the offeror/contractor may be required to adjust their billing and/or reimburse the Government for any charges invoiced in violation of the price warranty."

[End of Clause]

**I.36 ORDERING PROCEDURES - SERVICES (OCT 2007)**

Ordering of services under this BPA shall be accomplished by the issuance of written task orders specifying the services being ordered. All task orders issued under this BPA shall conform to the provisions of the BPA ordering procedures.

The only office(s) authorized to issue task orders under this contract are: CBP

**CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS**

I.37 LIST OF ATTACHMENTS

## Attachment No. Attachment Title

Attachment 1 – Statement of Objectives (SOO)

Attachment 2 – Pricing Template

Attachment 3 – Performance Work Statement Template

Attachment 4 – Sample Task Order Statement of Work (SOW)

1. SOLICITATION PROVISIONS
   1. 52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIOSN AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)

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.

1. *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.

1. *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--
   1. 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
   2. 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--

1. 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
2. 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.
3. *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.''
4. *Representations*. The Offeror represents that--
5. 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

1. 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.

1. *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:

* 1. For covered equipment--
     1. 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);
     2. 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
     3. 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.
  2. For covered services--
     1. 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
     2. 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:

1. For covered equipment--
   1. 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);
   2. 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

* 1. 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.

1. For covered services--
   1. 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
   2. 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]

* 1. 52.204-26 COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES-REPRESENTATION (OCT 2020)

1. *Definitions*. As used in this provision, ‘‘*covered telecommunications equipment or services*’’ and "*reasonable inquiry*" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.
2. *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’’.
3. *Representations*. (1) 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]

* 1. 52.216-1 TYPE OF CONTRACT (APR 1984)

The Government contemplates award of a single-award Blanket Purchase Agreement resulting from this solicitation.

[End of Provision]

* 1. 52.216-31 Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Acquisition (Nov 2021)

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

  (b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by-  (1) The offeror; (2) Subcontractors; and/or  (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

(End of provision)

* 1. 52.217-5 EVALUATION OF OPTIONS (JUL 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

[End of Provision]

* 1. AGENCY LEVEL PROTEST NOTICE (APR 2003)

Offerors are notified that per FAR 33.103(d)(4), an independent review of the grounds for a protest is available at a level above the contracting officer as an alternative to the protest to the agency contracting officer, not as an additional appeal after the protest to the agency contracting officer has been resolved. A choice to protest to the agency contracting officer therefore relieves the U.S. Customs & Border Protection of any further internal review or appeal after the contracting officer's decision.

[End of Provision]

* 1. QUESTIONS/CLARIFICATIONS REGARDING THIS SOLICITATION

All questions or clarifications regarding this solicitation must be submitted via Email to: Aaron Lacy (Contract Specialist) at [aaron.s.lacy@cbp.dhs.gov,](mailto:aaron.s.lacy@cbp.dhs.gov) **and**

Todd Frye (Contracting Officer) at [todd.frye@cbp.dhs.gov](mailto:todd.frye@cbp.dhs.gov)

**Phase I Questions shall be submitted no later than [TBD]**. Vendors shall place “70B02C23Q00000004 Question” in the subject line of the email. The Government is not obligated to provide responses to all questions and clarifications. A deadline for Phase II questions will be established in the Phase II advisory notification(s).

[End of Provision]

* 1. SELECT BEST-SUITED, THEN NEGOTIATE

Once the Government determines that a quoter is the best-suited (i.e., the apparent successful quoter) from Phase II submissions, the Government reserves the right to communicate with only that quoter to address any remaining issues, if necessary, and finalize a BPA with that quoter. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the Government, the Government reserves the right to communicate with the next best-suited quoter based on the original analysis and address any remaining issues. Once the Government has begun communications with the next best-suited quoter, the Government intends to cease communications with the previous quoter until after the BPA has been awarded. This process shall continue until an agreement is successfully reached and a BPA is awarded.

[End of Provision]

* 1. INSTRUCTIONS FOR THE PREPARATION AND SUBMISSION OF QUOTATIONS (OCT 2008)

This Request for Quote (RFQ) is being issued to all GSA IT MAS Subcategory Special Item Number (SIN) 518210C – Cloud and Cloud-Related IT Professional Services (NAICS 518210) and GSA IT MAS Subcategory SIN 54151S – IT Professional Services under FAR 8.405-3. Offerors must hold either or both SINs. All labor categories quoted must be included in the offeror’s relevant GSA schedule within the SIN. If a Contract Teaming Agreement (CTA) in which two or more GSA Schedule contractors team together is proposed, the offeror must submit the CTA with its quote. In the case of a CTA, each team member must have a GSA Schedule contract within one or both of the SINs identified.

1. **A multi-phase advisory selection process will be used in conducting this competition.** **The Government intends to conduct the evaluation process in two (2) Phases:**
2. Phase I Request for Past Experience. This step requires the following written submission:

* Factor 1 – Demonstrated Relevant Experience

The RFQ will invite interested GSA IT MAS Subcategory SIN 518210C and SIN 54151S contractors to provide a written submission presenting their relevant Past Experience. The RFQ will identify the information that must be submitted for initial Phase I evaluation, which should provide a basis for making a determination as to which offerors are most likely to submit the highest value technical solutions in response to the Phase II RFQ (i.e., the viability determination).

CBP will evaluate all Phase I RFQ responses in accordance with the criteria stated and shall advise each Offeror in writing either that it appears to be a viable competitor and is encouraged to participate in the acquisition through the release of the Phase II RFQ or, based on the information submitted, that it is unlikely to be a viable competitor. No ratings will be disclosed and no brief explanations to Offerors will otherwise be provided at the conclusion of the Phase I evaluation. All Phase I Offerors, notwithstanding the advice provided by the Government in response to their submissions, may participate in Phase II.

Details are in solicitation provision III.8 (d)-I below.

2. Phase II RFQ: This step requires the following submissions:

* Factor–2 - Technical
  + Element 1 – Performance Work Statement
  + Element 2 – Technical Approach to Scenarios
* Factor–3 - Staffing Plan
* Factor–4 - Price
* Factor–5 - Small Business Utilization Plan

Under Phase II of the competition, any GSA IT MAS Subcategory SIN 518210C and SIN 54151S contractors who participated in Phase I may respond to the Phase II RFQ, including those who choose to participate despite the Government’s advisory feedback that they are unlikely to be viable competitors. The RFQ will be issued to all offerors who have participated in Phase I and have requested to participate in Phase II regardless of the Government’s advisory decision.

Phase II Quotes will be evaluated in accordance with the RFQ evaluation criteria and the Government may make an award without exchanges with offerors.

Details are in solicitation provision III.8 (f)-(k) below.

1. **Notional Procurement Schedule:**

|  |  |
| --- | --- |
| **Event** | **Date** |
| Draft RFQ Released | 12/2022 |
| Industry comments/questions open period, analysis of responses | 2 weeks after Draft RFQ release |
| Revisions to RFQ | 1/2023 |
| Solicitation Released | 1/10/2023 |
| Phase I – Written Quotes Due (Demonstrated Relevant Experience) | 1/24/2023 (2 weeks after RFQ release) |
| Phase–I - Advisory Down Select Notifications Sent | 2/23/2023 |
| Phase II – Written Quotes (Technical (PWS and Technical Approach to Scenarios, Staffing Plan, Price, Small Business Utilization) Due | 3/9/2023 (2 weeks after Advisory Down Select Notifications Sent) |
| Award | 5/8/2023 |

*\*Quoters shall note the schedule above is not firm and subject to change.*

1. **Overall Instructions to Offerors**

The Offeror must respond to all of the requirements in the solicitation and must include in its quote all information specifically required in all sections of the solicitation. Each Offeror’s quote submitted in response to this solicitation shall be prepared in seven volumes as delineated in the table below. Each of the volumes and parts shall be separate and complete. The solicitation will be conducted in two phases.

|  |  |  |  |
| --- | --- | --- | --- |
| **RFQ Phase** | **Volume Number** | **Volume Title** | **Page Limit\*** |
| Phase 1 | 1 | Transmittal Letter  (Cover Page, Certification Page, Table of Contents) | 3 pages total |
| Phase 1 | 2 | Demonstrated Relevant Experience | 2 pages per project |
| Phase 2 | 3 | Transmittal Letter  (Cover Page, Table of Contents) | 2 pages total |
| Phase 2 | 4 | Performance Work Statement | 5 pages total |
| Phase 2 | 5 | Technical Approach to Scenarios | 10 pages per scenario |
| Phase 2 | 6 | Staffing Plan | 15 pages total (including QASP) |
| Phase 2 | 7 | Price Quote | N/A. No limit. |
| Phase 2 | 8 | Subcontracting Plan | N/A. No limit. |

Offerors are required to provide electronic copies of their proposals as stated in the table above. Electronic copies of the submissions and any modifications or revisions, are to be delivered to:

[Todd.Frye@cbp.dhs.](mailto: Todd.Frye@cbp.dhs.)gov

All electronic submissions must be delivered in Microsoft® Word 2013 (or higher versions when available) format for text submissions, and Microsoft® Excel 2010 or 2013 (or higher versions when available) for spreadsheet submissions. Offerors shall not submit PDF documents, with the exception of the Volume I.

**NOTE: There is a 10 MB size limitation for all individual incoming email transmissions.** Offerors may want to consider sending more than one email to ensure size limitations will not hinder transmission; however, the complete quote for each Phase (including all required submissions) must be received by the due date and time identified. Offerors should not submit .zip files as these may be stripped by CBP’s email system. For each volume of the quote submission, the respondent must identify the RFQ number in the Subject Line of the email and should include “# of #” if multiple emails are required for submission of the entire quote. All incoming files are scanned so there may be a delay between the time the file is submitted and the time it is received. Therefore, offerors must ensure they submit quotes with sufficient time to reach the required destination no later than the response due date and time identified.

The term “Offeror” as used herein refers to the single legal entity submitting the Quote to U.S. Customs and Border Protection. The work performed by the offeror shall be conducted by a corporate entity, or corporate entities in the case of a CTA, that will be totally responsible for all Blanket Purchase Agreement activities.

No classified information shall be included in the respondent’s written quote.

The Government reserves the right to award a Blanket Purchase Agreement without further exchanges. Therefore, the Offeror’s submission must contain its best terms. However, the Government reserves the right to seek clarification of the Offeror’s quote or to enter into discussions, if the Contracting Officer determines them to be necessary.

The respondent shall include the point of contact (name, telephone number, and e-mail address) that can assist the Contracting Officer with either clarification or discussions, if necessary.

The quote shall be clearly indexed and logically assembled. Each volume shall be clearly identified and shall begin at the top of a page. All pages of each volume shall be appropriately numbered and identified by the complete company name, date and solicitation number in the header and/or footer.

MS Word files shall use the following page setup parameters:

• Margins – Top, Bottom, Left, Right - 1”

• Gutter – 0”

• From Edge – Header, Footer - 0.5”

• Page Size, Width – 8.5”

• Page Size, Height – 11”

The following additional restrictions apply:

Each paragraph shall be separated by at least one blank line. A standard, 12-point minimum font size applies. Arial or New Times Roman fonts are required. Spacing shall be single spaced. Tables and illustrations may use a reduced font size not less than 9-point and may be landscape.

**Cover/Title Pages, certification pages, table of contents, illustrations, indexes and glossaries outside of Volumes 1 and 3 WILL count toward page limitations.** A qualifying page partially used will be counted as one qualifying page.

Every page of each volume shall contain a volume number and a page number. Blank pages shall contain the marking “Page Intentionally Left Blank”. It is the offeror’s responsibility to ensure data considered sensitive is marked as such. Only these markings may appear in the margins. A standard non-disclosure statement is allowed in the footer of each page.

Quotes must be prepared in accordance with these instructions and provide all required information in the format specified. The Offeror is responsible for including sufficient details to permit a complete and accurate evaluation of the Quote.

The required format is designed to ensure submission of information essential to the understanding and comprehensive evaluation of the Offeror’s quote. Pages in excess of the maximum will be removed from the end of the quote volume by the Contracting Officer without being evaluated.

1. **Phase 1, Factor 1: Submission Instructions.**

Phase 1 of the acquisition is initiated upon the release of the RFQ to all GSA IT MAS Subcategory Special Item Number (SIN) 518210C – Cloud and Cloud-Related IT Professional Services (NAICS 518210) and GSA IT MAS Subcategory SIN 54151S – IT Professional Services contractors through GSA eBuy. In response to the Phase 1 RFQ, Offerors shall submit only Volume 1 and Volume 2 of their quotes on or before the due date and time specified in the RFQ for Phase 1. Participation in Phase 1 is mandatory to participate in Phase 2. Phase 1 of the evaluation shall be concluded with an advisory notification to all RFQ Offerors of their viability for award based on CBP’s evaluation of Phase I submissions.

* 1. **Transmittal Letter.** The quotation shall include a cover page, certification page with an authorized official’s signature, and table of contents. The cover page shall include the date, solicitation number, company name and address, Unique Entity ID and CAGE Code, Taxpayer Identification Number (TIN), NAICS code, relevant GSA Schedule Number(s), and points of contact (primary and alternate) names, telephone numbers, and email addresses. The certification page shall certify the Offeror agrees to the terms and conditions of the solicitation.
  2. **Demonstrated Relevant Experience.**

Offerors shall submit a minimum of one **(1)** and a maximum of three **(3)** recent and relevant projects similar in size, scope and complexity to the work described in the SOO. The minimum and maximum limitations apply to the quote and may include the experience of contract teaming arrangement partners or subcontractors. The Offeror must demonstrate relevant experience with managing the topics listed below. Offerors may include projects with the Federal Government, agencies of state and local governments, and commercial customers. Demonstrated Relevant Experience submissions shall be sufficiently robust to allow evaluators to judge relevancy to this SOO within the page limits specified.

The Offeror shall provide the following information in connection with each of the examples of Demonstrated Relevant Experience example:

* Name of Prime Contractor
* Name of Government agency (Federal, state or local) and contracting activity or company name;
* Contract/task order/subcontract number;
* Contract/task order type;
* Dollar value;
* Date of contract/task order award and period of performance (including option periods and award term periods, if applicable);
* Statement as to performance responsibility as either prime contractor or subcontractor;
* Detailed description of work performed to support relevance of the work; and
* Name, mailing address, e-mail address, telephone number, and fax number of the following references:
  + - Contracting Officer or company business manager; and,
    - Contracting Officer’s Representative or company principal technical point of contact (POC).

Topics to be addressed in the Demonstrated Relevant Experience Narrative are designed to provide the Technical Evaluation Panel with information to determine their confidence in the Offeror’s ability to successfully perform various tasks in the SOO. Offerors are encouraged to not simply share what they did and where but focus instead on how they did it, the challenges they faced, and if they overcame those challenges. Offerors are also encouraged to discuss how they would apply their experiences, using tools and infrastructure they would use specifically at CBP.

Demonstrated Relevant Experience evaluation considers each Offeror’s demonstrated recent and relevant record of experience in providing services that are similar in size, scope and complexity to the statement of work requirements. To be recent, all or part of the period of performance of the relevant experience must have occurred within the 36 months prior to the Phase 1 solicitation closing date.

Offerors shall address the requirements of the SOO in the Demonstrated Relevant Experience Narrative.

1. **Advisory Notification/Down Select.** After the Government completes evaluation of Phase 1 submissions (Factor 1), Offerors will receive an advisory notification via email from the Contracting Officer. Offerors who rate most highly for Factor 1 will be advised to proceed to Phase 2. Offerors who were not among the most highly rated will be advised not to proceed to Phase 2. Offerors who were not among the most highly rated, will be advised that they are unlikely to be viable competitors, along with the general basis for that opinion. Offerors will be advised that their Factor 1 evaluation results will carry forward to Phase 2 and will be considered in the best value award decision. The intent of this advice is to minimize quote development costs for those Offerors with little chance of receiving an award. This will be a recommendation only and discontinuing the pursuit of the requirement following the notification is voluntary. The Government does not intend to provide exchanges after the completion of the advisory down select notifications. Failure to participate in Phase 1 precludes further consideration of an Offeror. Phase 2 Offeror submissions will not be accepted from Offerors who have not submitted Phase 1 requirements by the due date and time provided for in this solicitation.

The advisory notification will include the Phase 2 due date. . All Phase 1 Offerors, notwithstanding the advice provided by the Government in response to their submissions, may participate in Phase 2.

1. **Phase II, Factor 2 (Technical – Elements 1 & 2).**

***Element 1: Performance Work Statement (PWS)***

The Offeror shall complete and submit the PWS template (Attachment 3) to describe how it will satisfy all requirements documented in the Statement of Objectives (SOO) for the overall Blanket Purchase Agreement.

***Element 2: Technical Approach to*** **Scenarios 1 and 2**

**Scenario 1 - Unplanned Cybersecurity Support**

Issue: CBP is suddenly affected by a nationwide impacting zero-day vulnerability (**unintended security flaw in a software application or an operating system (OS) unknown to the party or vendor responsible for fixing the flaw**). The originating product’s vendor has suggested limited mitigation options.

* 1. In relation to the support requirements listed in the SOO, describe your role and actions in addressing this scenario.
  2. Include the types of resources, communication, monitoring and other information as appropriate.

**Scenario 2 – Cost Optimization**

Issue: CBP has experienced an unprecedented growth in cloud costs over the last five years. In this scenario, the annual bill across three CSPs increases 30% year over year which is considered unacceptable considering the growth and migration models. CBP’s current cloud cost ranges from $40,000,000 to $50,000,000. CBP believes there are strategies for optimizing costs to reduce the cloud bill. This scenario places the offerors in the position of developing strategies to permit the government to control costs, while also providing insight into the offerors’ ability to assess and optimize ongoing inefficiencies.

* 1. In relation to the support requirements listed in the SOO, describe your role and actions in addressing this scenario.
  2. Include the types of actions that would be taken to identify, implement, control, and monitor cost optimization opportunities.

1. **Phase II, Factor 3 (Staffing Plan).**

The Offeror shall submit a Staffing Plan which encompasses the following:

* An overview of recruitment, training, and retention policies for each labor category offered. Data must be sufficient to demonstrate the overall experience and qualifications of each labor category offered.
* Provide an overview of the strategy for acquiring cleared staff and staff which have a high probability of successfully passing the background investigation.
* Provide an overview/plan to ensure personnel maintain technical expertise and stay current on the ever-changing technical environment.
* Provide an organizational chart that identifies background and qualifications of the management team.
* A high-level composition of the proposed team, which includes an estimated number of personnel mapped to the labor categories per task as provided in the SOO. Include a brief summary of team(s) and the team’s relationships and responsibilities in the execution of the planned work.
* Propose off-site staffing options that improve the level of service and lower costs to the CBP.
* Demonstrate the day 1 staffing model, performance targets, and technology and tools adopted by or deployed by the Offeror.
* Total personnel (FTE) in the Staffing Plan shall be consistent with the number of FTE listed in the submitted Attachment 2 - Pricing Template.
* Quality Assurance Surveillance Plan

1. **Phase II, Factor 4 (Price Quote).**

The offeror shall quote a pricing structure consistent with the proposed technical solution. Offerors shall complete all tabs within “Attachment 2 – Pricing Template” and submit as part of their price quotation. Tab 1 of Attachment 2 shall include all potential labor categories, associated MAS GSA rates, and quoted rates to be included in the BPA. Tab 2 of Attachment 2 shall include all potential labor categories, associated MAS GSA rates, and quoted rates for the Sample Task Order Statement of Work, Attachment 4, for Cloud Modernization Effort – IT Professional Services Quotations shall include a statement that the offeror’s quotation is valid for a minimum of one hundred-twenty (120) calendar days from the date of submission.

The Offeror’s price quote shall be based on the offeror’s current GSA MAS pricing, utilizing all discounts, which are hereby specifically requested. The Offeror’s quote shall provide its GSA MAS pricing rates as a reference and its quoted pricing/rates to meet the requirements of the RFQ. The Offeror’s price portion must include all pre-set columns and include a cumulative summary of pricing to include the total quoted for the Sample Task Order.

1. **Phase II, Factor 5 (Small Business Utilization Plan)**

For Factor 5, offerors shall submit a Small Business Utilization Plan specific to this ECIS requirement that articulates how small businesses will participate through small business subcontracting and/or Contract Teaming Arrangements (CTAs). If a CTA is proposed, the offeror must submit the CTA with its quote. The offeror shall propose goals that meet or exceed CBP’s Small Business Goals, as specified in the solicitation, when proposing their Small Business Utilization Plan. Include a brief description of the efforts the Offeror will make to assure that small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small-disadvantaged business, and women-owned small business concerns have an equitable opportunity to compete for subcontracts.

The following are CBP’s small business subcontracting goals:

* 40.0% Small Business
* 18.8% Small Disadvantaged Business (SDB)
* 5.0% Women Owned Small Business (WOSB)
* 3.0% Service Disabled Veteran Owned Small Business (SDVOSB)
* 3.0% Historically Underutilized Business Zone (HUBZone)

Failure to meet CBP small business plan goals results in a rating of “Fail”.

1. **Organizational Conflicts of Interest (OCI)**

Offerors must affirmatively state that they do not have an organizational conflict of interest (OCI) that requires a mitigation plan in accordance with HSAR 3052.209-72 Organizational Conflict of Interest, or otherwise must disclose the potential conflict and offer a mitigation plan, if applicable, with submission of their quote.

1. **Assumptions, Conditions, or Exceptions.**

Offerors must submit all (if any) assumptions, conditions, or exceptions with any of the terms and conditions of this solicitation. The assumptions must be included in the Price Quote (Factor 4). An Offeror’s assumptions, conditions or exceptions may result in their quote being non-compliant and ineligible for award.

If not clearly identified in the Price Quote (Factor 4), it will be assumed that the Offeror proposes no assumptions for award and agrees to comply with all of the terms and conditions as set forth herein in this RFQ. It is not the responsibility of the Government to seek out and identify assumptions, conditions, or exceptions buried within the Offeror’s quote.

* 1. GENERAL QUOTATION INFORMATION

1. Your quotation shall become the property of the Government and will not be returned. If your quotation contains information that you do not wish disclosed to the public or used by the Government for any purpose other than evaluation of your quotation, such restrictions shall be indicated clearly on each sheet containing such information.
2. Prior to the submission of quotations, Quoters are expected to reach an understanding of the requirements of this solicitation. If such a review establishes the need for correction or clarification, such information should immediately be brought to the attention of the Contracting Officer so that the matter can be resolved and/if necessary, official dissemination of such information can be made to all Quoters.
3. The Government reserves the right to request such additional information as may be necessary to determine the Quoter’s qualifications for award of a task order or to clarify and aspects of the quotation. Such information shall be furnished promptly upon the Government’s request.
4. The Contracting Officer is the only person who can legally obligate the Government for the expenditure of public funds. Costs shall not be incurred by recipients of the solicitation document in anticipation of receiving direct reimbursement from the Government; the Government will not reimburse for quotation preparation. This solicitation and resulting task order shall not cover charges for any items which are not specifically provided for by this solicitation. The Quoter is cautioned that if it provides services/supplies not specifically covered during the performance of any subsequent task order, regardless of who requested them (including the COR); payment will not be made. Again, the only person authorized to create financial obligations on behalf of the Government is the Contracting Officer.
   1. EVALUATION CRITERIA

A best value, trade-off analysis will be performed in selecting an awardee. The Government may make an award without discussions. Only one award will be made.

1. Quotations shall be evaluated on the following factors:

**Phase I:**

Factor 1 - Demonstrated Relevant Experience (Written Submission)

**Phase II:**

Factor 2 – Technical Elements 1 and 2 (Written Submission)

Factor 3 - Staffing Plan (Written Submission)

Factor 4 - Price (Written Submission)

Factor 5 - Small Business Utilization Plan (Written Submission)

Each of the above factors are evaluated independent of other factors. This is a multi-phased source selection process. Failure to meet or comply with either the Phase I or Phase II submission requirements may result in a determination of non-responsiveness at each Phase respectively.

See provision “RELATIVE IMPORTANCE OF EVALUATION FACTORS” below for relative order of importance.

1. *Confidence Ratings* – Factors 1, 2, and 3 will each be evaluated with a rating scale of "high confidence," "some confidence," and "low confidence," representing the Government’s confidence that the Offeror understands the requirement and will be successful in performing the work. Additionally, Confidence Ratings will be utilized to make a trade-off selection decision for award.

|  |  |
| --- | --- |
| **CONFIDENCE RATINGS** | |
| **RATING** | **DEFINITION** |
| **High Confidence** | Based on the information provided, the Government has ***high*** ***confidence*** that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the task orders with little or no intervention. |
| **Some Confidence** | Based on the information provided, the Government has ***some*** ***confidence*** that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the task orders with ***some*** Government intervention. |
| **Low Confidence** | Based on the information provided, the Government has ***low*** ***confidence*** that the Offeror understands the requirement, proposes a sound approach, or will be successful in performing the task orders ***even with*** Government intervention. |

1. **Price Evaluation.** The Government will conduct a price evaluation (Factor 4) of the offeror's quotation. Pricing will be evaluated for reasonableness in accordance with FAR 8.405-3. The Government will consider the level of effort and the mix of labor proposed to performto determine price reasonableness and will use the total evaluated amount from the sample Task Order for comparison in the trade off decision.

It is anticipated that pricing and award of this acquisition will be based on adequate price competition. Offerors are strongly encouraged to offer substantial discounts from their GSA MAS rates.

Price volumes failing to meet or comply with price quotation instructions may be deemed noncompliant.

The entire Price quotation will be evaluated for the reasonableness of the overall price. This evaluation will determine if prices contained in the Offeror’s quotation are reasonable given the nature of the work to be performed.

An Offeror’s price quotation must be consistent with the Offeror’s technical approach to both technical scenarios and staffing plan.

Offeror’s quoted rates will be locked in for future Task Orders issued under the BPA.

1. **Pass/Fail Ratings** – Factor 4 will be evaluated by comparing the Offeror’s proposed sourcing plan with subcontracting goals to CBP’s provided subcontracting plan goals with a rating scale of Pass or Fail. If the offeror is a small business concern performing at least 51% of the work, a rating of “Pass” will be assigned without further consideration.

The following are CBP’s small business subcontracting goals:

* 40.0% Small Business
* 18.8% Small Disadvantaged Business (SDB)
* 5.0% Women Owned Small Business (WOSB)
* 3.0% Service Disabled Veteran Owned Small Business (SDVOSB)
* 3.0% Historically Underutilized Business Zone (HUBZone)

Failure to meet CBP small business plan goals results in a rating of “Fail”.

1. **Overall Evaluation Factors and Basis for Award**

For this solicitation, the major evaluation factors are:

**Factor 1** – Demonstrated Relevant Experience (Non-Price; Confidence Rating)

**Factor 2** – Technical (Non-Price; Confidence Rating)

**Factor 3** – Staffing Plan (Non-Price; Confidence Rating)

**Factor 4** – Price

**Factor 5** – Small Business Utilization (Non-Price; Pass/Fail)

A best value source selection using tradeoffs will be conducted in accordance with the policies and procedures in FAR 8.4 and the RFQ. The Government may make an award without discussions. Only one award will be made.

The Government anticipates awarding a single BPA to the Offeror whose quote is the most advantageous to the Government, price and other factors considered. Of the 5 evaluation factors, Demonstrated Relevant Experience (Factor 1) is slightly more important than Technical (Factor 2). Technical (Factor 2) is slightly more important than Staffing Plan (Factor 3). When combined, factors 1-3 are significantly more important than price (Factor 4). Factor 5 will be evaluated on a pass/fail basis. As the non-price factors become more equal, price may become the determining factor. The determination that technical/performance aspects are essentially equal is within the discretion of the Selection Official.

Following receipt of responses, the Government may perform a comparative analysis (comparing contractor responses to one another) to select the contractor that is best value to fulfill the requirements, based on the contractors’ responses to the factors outlined in this RFQ and their relative importance.

Award will be made to that responsible offeror whose quotation provides the combination of criteria offering the best overall value to the Government.

[End of Provision]

# III.12 BASIS OF AWARD (TRADEOFF ANALYSIS) (JUN 2007)

Award shall be made to the quoter whose quotation is determined to best meet the needs of the Government after consideration of all factors-- i.e., provides the "best value". "Best value" is defined here as the procurement process that results in the most advantageous acquisition decision for the Government and is performed through an integrated assessment and tradeoff analysis among price and non-price factors.

The basis for the award of a contract as a result of this Request for Quotation (RFQ) will be a detailed, integrated evaluation by the Government on the basis of how well the proposals satisfy the evaluation criteria contained in the provision entitled "Evaluation Criteria" in this solicitation. Accordingly, the Government may award any resulting task order to other than the lowest priced quoter(s) or other than the quoter(s) with the highest technical merit rating.

The Contracting Officer or Source Selection Official has the right to determine whether two or more technical proposals are "substantially equal" or whether any differences in technical weighing are "significant" for purposes of evaluating the overall merit of proposals. Between quotations of substantially equal technical merit, price will become a more significant factor.

Between competing quotations, the Government is not willing to pay significantly more for a minor technical difference, nor is the Government willing to forego a significant technical difference in exchange for a small price differential.

See the provision entitled "Relative Importance of Evaluation Factors" contained in this solicitation.

[End of Provision]