DATE:
25June2019

Re: **GSA Schedule 84 SIN 246-54**

Dear Sir or Madam:

The Department of Homeland Security, U.S. Customs and Border Protection (CBP), has an anticipated requirement for Transportation and Security Guard Services in support of the US Border Patrol, along the Southwest Border. This is a streamlined solicitation under FAR Part 8.405-2(b)(2). CBP intends to enter into a single Blanket Purchase Agreement (BPA) with a General Services Administration (GSA) Federal Supply Schedule (FSS) vendor to fulfill these recurring requirements. It is requested that your company submit a response for this effort.

Your emailed response is requested to be received by Matt Russell at the following address no later than July 10th, 2019 5:00 P.M. local time (EST): matthew.j.russell@cbp.dhs.gov. Any questions shall also be directed to the above-mentioned email address no later than July 2nd, 2019 5:00 P.M. local time (EST).

Sincerely,

Shaun G. Saad
Contracting Officer

Attachments:

1. Evaluation Instructions (Pages 2-11)
2. Corporate Experience Questionnaire (pages 12-14)
3. Performance Work Statement (PWS)/Transportation Plan (page 15)
4. Pricing Worksheet/ Sample Task Order (page 16)
5. Quality Assurance Surveillance Plan (QASP) (page 17)
6. Blanket Purchase Agreement [template] (BPA) (pages 18-46)

ATTACHMENT 1

EVALUATION INSTRUCTIONS

I.1 INTRODUCTION

U.S. Customs and Border Protection (CBP) plans to establish a single award Blanket Purchase Agreement (BPA) for the *Southwest Border – Ground Transportation and Security Guard Services* with a General Services Administration (GSA) Federal Supply Schedule (FSS) vendor. Contractor teaming arrangements (CTAs) may be proposed; however, all team participants must be a current GSA FSS contractor under Schedule 84, SIN 246-54.

I.2 GENERAL INSTRUCTIONS FOR THE PREPARATION OF QUOTATION

CBP will conduct a streamlined evaluation of FSS contractors currently holding GSA contracts for establishing a BPA. CBP reserves the right to establish a BPA without further communication and exchange; therefore, each response to this request should contain the vendor's best pricing, terms, and conditions. Quotes must be prepared in accordance with these instructions and provide all required information in the format specified. The required format is designed to ensure submission of information essential to the understanding and comprehensive evaluation of the vendor's quote. Failure of a quote to comply with these instructions may be grounds for exclusion of the quote from further consideration. Any exceptions taken with respect to the clauses in the solicitation shall be noted. For the purpose of facilitating exchanges, for every instance where the vendor does not propose to comply with or agree to a requirement, the vendor shall propose an alternative and describe its reasoning therefore.

The Government intends to conduct this acquisition in two phases—

Phase 1-- Phone Interview

Vendors must request to schedule a Phase 1 phone interview and submit Attachment 2 – Corporate Experience Questionnaire prior to the date and time scheduled for the Phone Interview. The Phone Interview will evaluate Factor One –Experience and Risk Awareness/Mitigation. Based on the Government's evaluation of this interview, an advisory down-select will then be issued by the Government, whereby vendors will be advised whether they are invited to participate in Phase 2. **The quoter shall not record the call.** The Government may record the call.

Phase 2-- Oral Presentation—The Technical Quote shall be submitted in the form of an Oral Presentation. There will be no written technical volume. No written technical volume of any sort will be accepted. The only required written submittal for Phase 2 will be the Pricing Worksheet and the Sample Task Order submission.

(1) **FACTOR ONE— Experience and Risk Awareness/Mitigation (Phase 1)**

(a) Method: Phone Interview.
(b) Duration: 30 minute estimate.

(c) Process:

(i) By the date and time set in this RFQ for Phase 1, the quoter shall submit Attachment 2- Corporate Experience Questionnaire.

(ii) In the phone call, the quoter shall identify a maximum of three (3) past contracts/orders that are most similar in size (i.e. the # of estimated FTEs performing the requirement and/or the estimated dollar value of the contract) and scope to the work of this RFQ. For each of these, the quoter shall describe (A) its own experiences in providing similar services in circumstances similar to CBP's, (B) the similarities and the differences, (C) the value it brought to those experiences, (D) its lessons learned from those experiences, (E) the value to the Government that comes with its experiences, (F) the risks both the Government and the Contractor will face in accomplishing the work and achieving successful task order performance, and (G) its approach to managing those risks as our contractor so that the CBP Ground Transportation and Guard services effort will be successful.

(iii) The quoter's participation is limited to three persons, all of whom must be current employees of the prime schedule contractor. The experience discussion is limited to the prime schedule contractor's own experience, unless the vendor is submitting under a Contractor Teaming Arrangement (CTA), in which case at least two of the experience discussions must be the prime schedule contractor's own experience and no more than one may be a CTA partner's experience.

(d) Advisory Down-Select Decision:

(i) Based on its evaluation of Factor One, the Government intends to advise up to three schedule contractors who are most highly rated for Factor 1 (based on the confidence rating system described in section I.5) to proceed to Phase 2.

(ii) After the Government completes evaluation of Factor 1, quoters will receive an advisory notification via e-mail from the Contracting Officer. This notification will advise the Quoter of the Government's advisory recommendation to proceed or not to proceed with Phase 2 submission. Quoters who are rated most highly for Factor 1 will be advised to proceed to Phase 2 of the quote submission process. Quoters 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 the Government's advisory recommendation. The intent of this advice is to minimize quote development costs for those Quoters with little to no chance of receiving an award. Quoters should note that Phase 1 evaluation criteria are more important than Phase 2 evaluation criteria.

(iii) The notices will provide the date and time by which quoters who wish to participate in Phase 2 must submit the Phase 2 quotation.

(2) **FACTOR TWO – Technical/Management Approach (Oral Presentation, Phase 2 only)**

(a) Method: Oral Presentation.

(b) Duration: 4 Hours.

The Technical Quote shall be made in the form of an Oral presentation. The presentation may be recorded by the Government. The only written technical volume of any sort that will be accepted is the Pricing and Sample Task Order responses.

During the Oral Presentation, the quoter shall not make any reference to cost or price; however, resource information (such as data concerning labor hours and categories, materials or supplies required for performance, subcontracts, etc.) may be discussed so that the quoter's understanding of the requirements may be evaluated. The same confidence rating methodology used in Phase 1 will be used for evaluation purposes of Phase 2.

The Oral Presentation will be conducted in such a manner as to enable the Government reviewers to make a thorough evaluation and arrive at a sound determination of whether the quoter understands the technical requirements. Presentations which merely offer to perform in accordance with the Government's requirements or which merely paraphrase the requirements document, or use phrases such as, "standard engineering practices will be employed," or "well established techniques will be employed," etc. may not provide confidence to the Government evaluators. The Contractor must present an explanation of its proposed technical approach in conjunction with the tasks to be performed in achieving the program objectives.

(c) Process:

(i) By the date and time set in the Phase 1 notice for receipt of Phase 2 quotations, the quoter shall submit (A) a one-page document that summarizes the points it intends to make in its oral presentation, (B) a list of attendees at the oral presentation (including name, employer, title, proposed role in performance, and citizenship).

(ii) The oral presentation will occur in a conference room in a Government building. A whiteboard and/or flipchart pad with markers will be provided.

(iii) The quoter is limited to five attendees. The attendees must include the proposed program manager, a proposed sector manager, and a proposed transportation officer.

(iv) The quoter's attendees may not access phones, computers, or other electronic devices during the oral presentation.

(v) The Government intends to evaluate the oral presentation immediately after it occurs. At that time, the whiteboard will be erased and any flipchart pages will be destroyed.

(vi) During the oral presentation, the quoter will have up to 60 minutes to answer all questions listed below, and up to 60 additional minutes to answer any "challenge" questions that may be asked after the 5 questions below have been answered.

(vii) The first question the quoter shall answer is—

Question 1: Summarize your approach to fulfill the requirements outlined in the PWS (if presenting under a CTA, quoters shall summarize the CTA structure and explain how the agreement will allocate work under the PWS tasks.

(viii) The four additional questions the quoter shall answer are—

Question 2: Outline the challenges you expect to encounter with the PWS requirements.

Question 3: Describe how you plan to ensure that the Operational Requirement of 95% will be consistently met.

Question 4: Describe your plan to provide the required vehicles for the sectors, and how you intend to ensure they are always available per the PWS.

Question 5: How do you plan to ensure adequate numbers of trained and qualified Transportation/Detention Officerss, including BI's both initially, and throughout the contract?

(ix) Sample Task Order submission: complete the Sample Task Order and, when asked for it, submit it during the Oral Presentation.

(x) The Government will inform the quoter of the time and date for its oral presentation. The Government assumes no responsibility for any attendee's inability to pass through security.

(xi) The schedule will be as follows—

Hour	**Activity**
1st	Presenting team arrives, introductions, contracting officer (CO) gives questions, Government staff depart the room and presenting team prepares its responses.
2nd/3rd	Government staff returns, presenting team makes its presentation.
4th	Government staff retires to a caucus to see if any further questions need to be asked (1/2 hour); if so, presenting team answers them (1/2 hour).

(d) The Government will evaluate the oral presentation based on its confidence that the quoter understands the Government's need and will be successful in task order performance.

(3) **FACTOR THREE (PRICE)**

Sample Task Order (submitted at the conclusion of the Oral Presentation, Phase 2 only)

(a) Method: written submission (see Attachment 4).

(b) Process: The sample task order shall not deviate from the supplied format. The sample task order will remain with the Government at the completion of the oral presentation.

Pricing Worksheet (submitted at the conclusion of the Oral Presentation, Phase 2 only).

(a) Method: Written submission (see attachment 4 Pricing Worksheet/ Excel Spreadsheet).

(b) Process: Price quotation shall be submitted on the date of the Oral Presentation. Price proposals shall be broken down into sectors, and further by labor rates and vehicle rates (see Attachment 4). The quoter shall identify any exceptions it takes to any portion of the RFQ or its attachments.

The quoter shall submit the following that shall comprise its price quotation for this solicitation.

(1) **Direct Labor Base.** The quoter shall offer the largest possible reduction on its GSA schedule contract rates for direct labor. Quoter shall show the GSA labor category descriptions, estimated hours, unit hourly rates, and extended amounts for each category of labor. It is understood that the GSA rates are fully loaded (i.e., with all indirect expenses, G&A, fringes, etc.). A direct labor total shall be shown as a result of the extended amounts. Where specific individuals are proposed for particular labor categories, so indicate as a matrix. The quoter must include a statement that these rates are applicable for the period(s) of performance of the BPA. Quoters must appropriately map their corresponding GSA labor categories to the labor categories described in the PWS.

(2) **Travel, Fuel, and Surge.** A pre-populated line item for Travel and Fuel is provided and must be used by quoters. This is a Not-To-Exceed (NTE) line item. These costs will be treated as direct reimbursable under GSA schedule special ordering procedures. The Government will reimburse the contractor's approved actual direct costs for travel and fuel, with no indirects or other mark-ups. The vendor exceeds at its own risk. Any travel under subsequent task orders must be pre-approved by the Contracting Officer's Representative (COR.) Surge will have an NTE amount of hours and that specific number of NTE hours must be used for calculating potential surge. The Quoter is only required to fill in its Surge rates.

(3) **Total: Time-and-Materials Estimate**

(4) Quoter shall include information to explain the estimating process used, including judgmental and assumption factors applied.

NOTE: The quoter shall submit a separate breakdown of the above for each period of performance stated below:

(a) Base Performance Period: **08/01/2019 – 07/30/2020**

(b) Optional Performance Period I: **08/01/2020 – 07/30/2021**

(c) Optional Performance Period II: **08/012021 – 07/30/2022**

(d) Optional Performance Period III: **08/01/2022 – 07/30/2023**

(e) Optional Performance Period IV: **08/01/2023 – 07/30/2024**

I.3 ORAL PRESENTATIONS GUIDELINES AND SUBMISSION RULES

GENERAL

Oral presentations will be used for this solicitation. Quotations must be prepared in accordance with the GENERAL INSTRUCTIONS FOR THE PREPARATION OF QUOTATIONS and these instructions, and provide all required information in the format specified.

PROCEDURES:

The order and scheduling of oral presenters will be determined by a drawing by the Contracting Officer within 5 days after Phase 1 is completed, with notification of presentation time given as soon as reasonably possible thereafter. All vendors should be prepared to give oral

presentations within 20 days after receipt of the notice to continue to Phase 2. Vendors must be available for the presentation at their scheduled time. Requests for a different time period are discouraged but the Government reserves the right to reschedule a presentation at the discretion of the Contracting Officer.

Presentations will be held in the Washington, DC Metropolitan Area (Bldg and room to be determined). The key presenters shall be the primary presenters and represent those individuals responsible for the performance of specified functions under the BPA. This excludes marketing reps, proposal consultants (individuals giving the presentation not working on the effort) and professional presenters. Offering a movie, videotape or other means of demonstration in lieu of the oral presentation is not permitted. If all of the quoter's presenters fail to attend the scheduled oral presentation then they will be eliminated from further consideration for award.

The oral presentation may be video recorded by the Government for documentation purposes.

TIMING AND PRESENTATION

It is the vendor's responsibility to ensure their team members arrive at the briefing site on-time. Vendors must allow adequate time for clearing visitor control and security processes. Vendors will be given a private 30 minute preparation time prior to the presentation. Time not used in preparation cannot be added to the presentation time. Total time of preparation and presentation shall not exceed 4 and a half hours. After the presentation, a 30-minute break (maximum) will be given prior to the question and answer session (Q & A), which shall not exceed 30 minutes. It is anticipated that to conduct the entire oral presentation process, a total of 4 hours may be required by the parties.

The 2 hour limit on the briefing portion of the oral presentation is not a requirement that a vendor fill 2 hours with a presentation. Vendors shall present a briefing that fits within the overall time limit but the order and exact times for each section are up to the vendor. The time spent on each area is relevant only to the extent to which it may exclude other areas to be addressed during the overall time frame; therefore, there are no specific time limits for individual sections. The Contracting Officer (or representative) will moderate the time and verbally signal when scheduled breaks are needed and when the end of the overall presentation time is near. If a vendor fails to complete the presentation or does not address all topics, communications may be used to address the issues during the Q&A session. However, neither the briefing materials nor the Q&A session shall be used to cure the inability of the vendor to complete its presentation. The evaluators' obligation is simply to rate the vendor based on the oral presentation, including the Q&A session and any communications that take place. Unused time for the briefing cannot be applied to achieve a longer Q&A session.

In order to make the oral presentations as flexible as possible, evaluators are authorized and encouraged to use the question and answer session for a full exchange of information, as needed, to evaluate a specific presentation. It is not anticipated that there will be a need for any dialogue during the vendor's briefing, except for normal personal exchange between individuals. Dialogue between the parties during the briefing may actually detract from the overall presentation and cause delays in the time needed for the presentation. Therefore, unless absolutely needed, exchanges will be reserved for the Q&A session. Vendors are advised that the Q&A session is not an opportunity for a debate. Vendors will also not be allowed to respond to questions by saying they will provide the information at a later date.

Each offeror shall provide an oral presentation demonstrating their technical and management approach and capabilities. They shall demonstrate an understanding of planning, risk management and the relationship between financial and resource allocation necessary to execute the program and partner with the Government. One individual representing a Key Personnel category shall be present and shall demonstrate their knowledge, skills and abilities of specific core expertise. That individual shall actively participate in the presentation and is encouraged to give an oral version of their resume. He/she shall demonstrate an understanding of the requirements and his/her capabilities. The Key Personnel categories are found in the PWS, as follows: Program Manager, Sector Manager.

The material content of the presentation is up to the vendor, provided it substantively addresses the information set forth below. Only the vendor's initial presentation shall be evaluated and rated - - changes or resubmissions are not permitted. The presentation shall not address any pricing information. When the Oral Presentation is completed, then the Pricing portion shall be submitted and then the parties will caucus and any pricing information may be clarified during the Q&A session that follows.

Vendors shall give their oral presentation in a briefing format specifically addressing their Technical and Management Approach, which consists of answering the 5 questions previously listed under Factor Two (2). At the conclusion of the Oral Presentation, Vendors will be asked to submit their formal written Price quote which consists of the Pricing Worksheet (Excel spreadsheet) and the Sample Task Order for Factor 3 (Price). [see Attachment 4]

QUESTION AND ANSWER SESSIONS

After completion of the Oral Presentation, the Government evaluation team members shall have the opportunity to ask questions in order to clarify any points addressed which are unclear and may ask for elaboration from the presenters on any topics addressed in the Oral Presentation. To the extent that a dialogue takes place between the parties, any such interchange between the vendor and the Government will be for clarifications only. The information supplied in the Oral Presentation is intended for evaluation purposes and are considered clarifications and will not obligate the Government to determine a competitive range, conduct exchanges, or solicit or entertain revised quotations.

At the conclusion of the Q&A session, the presenters will be escorted out of the area.

ACTIONS AT THE CONCLUSION OF ORAL PRESENTATIONS

Statements made by the vendor during the oral briefing or the question and answer session will not become part of any contract resulting from this RFQ, unless the Government and the vendor agree in writing. The Government does not plan to solicit revisions to the oral presentations or to the answers given during the question and answer session but reserves the right to do so if the Government decides to conduct further exchanges. If during either the briefing and/or during the question and answer session the vendor makes a promise to which the Government wishes to bind the vendor, the promise will be reduced to writing and the vendor will be asked to confirm the promise during further exchanges, if opened. Any binding promise that has the potential to result in a revision to the vendor's presentation/submission will be confirmed only during further exchanges, if opened.

AWARD ON INITIAL RESPONSES

The Government anticipates selecting the best-suited quoter from initial responses, without engaging in exchanges with quoters. Quoters are strongly encouraged to present their best technical solutions and pricing/sample task order submissions in response to this RFQ. However, the Government reserves the right to communicate with any or all vendors submitting a technical and price quote, if it is determined advantageous to the Government to do so.

I.4 BASIS OF AWARD (TRADE-OFF ANALYSIS)

The Government anticipates establishing a single-award BPA with the schedule contractor whose quote 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 trade-off analysis among price and non-price factors.

The basis for the establishment of a BPA as a result of this RFQ will be a detailed, integrated evaluation by the Government on the basis of how well the presentations satisfy the evaluation criteria contained in the provision entitled "Evaluation Criteria" in this solicitation. Accordingly, the Government may award the BPA to other than the lowest priced offeror or other than the offeror with the highest technical merit rating. Where quotes are determined to be substantially equal in technical merit, price will be become the predominating factor.

Award will be made to the responsible offeror whose quote provides the best overall value to the Government.

For this solicitation, the evaluation factors are:

Factor One (Non-Price/Cost): Experience and Risk Awareness/Mitigation.

Factor Two (Non-Price/Cost): Oral Presentation

Factor Three (Price): Pricing Spreadsheet and Sample Task Order Submission

All "Non-Price/Cost" factors when combined, are significantly more important than Cost/Price. The Government is more concerned with obtaining superior technical performance capability (represented by the non-cost evaluation categories) than with making an award at the lowest overall evaluated cost/ price. The determination that technical/performance aspects are essentially equal is within the discretion of the Source Selection Authority (SSA).

Award of a BPA can only be made to a vendor:

1. Whose technical presentation and pricing represents the best value; and

2. Whose proposed price is determined to be fair and reasonable.

The Government will perform a cross-walk of the technical presentation and pricing submissions to ensure the price approach is in line with the technical approach. This cross-walk will affirm

the vendor's price is fair and reasonable with respect to the vendor's technical approach (i.e. level-of effort/labor mix).

I.5 EVALUATION CRITERIA

TECHNICAL (NON-PRICE) (FACTORS 1 and 2)

Evaluation of the "Technical (Non-Price)" portion of the quote will be based on a Two-Phased approach, the first phase is an advisory down-select based on Factor 1 –Prior Experience and Risk Awareness/Mitigation. The second phase is based on Factor 2 –Technical/Management Approach that is submitted via the Oral Presentation. Factor 2 focuses on the Government's questions and the vendor's answers during the Oral Presentation to establish a confidence level rating for the vendor's technical solution, approach, capabilities, labor-mix/level-of-effort, and general understanding of the requirement to assess how the technical quote satisfies the Performance Work Statement (PWS) provided by the Government in this solicitation (Section I.2 above outlines the Oral Presentation in detail). This group of non-price factors will be assessed on High Confidence, Some Confidence, or Low Confidence, as follows:

Rating System for Evaluation of Technical (Non Price) Factors	
High Confidence	The Government has *high confidence* that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with little or no Government intervention.
Some Confidence	The Government has *some confidence* that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with some Government intervention.
Low Confidence	The Government has *low confidence* that the Offeror understands the requirement, proposes a sound approach, or will be successful in performing the contract even with Government intervention.

PRICE (FACTOR 3)

Separately and apart from the technical evaluation, the Government will conduct a price evaluation of the vendor's price quote. A price analysis will be conducted to determine fairness and reasonableness in accordance with FAR 8.405-3(b)(2)(vi) and if proposed prices accurately and adequately reflect the work to be performed.

The Offeror's proposed price will also be considered in the context of price risk and affordability. In this context, price risk is the Government's level of confidence in the Offeror's ability to perform the work as proposed based on the following:

1. The price information provided by the Offeror and/or from the applicable GSA schedule
2. The completeness of the Offeror's price documentation proposed in the Excel spreadsheet entitled "Pricing Schedule".

3. The completeness of the Offeror's pricing in response to the Sample Task Order

Failure to comply with Pricing Worksheet Instructions requirements may result in vendor's elimination from consideration

For the Base Period evaluation, the bottom line price will be evaluated by combining the bottom line price for all CLINs including the NTE amounts for (Travel- Direct Reimbursable) and Fuel. The equivalent CLINs in each of the Option Periods will be combined to develop a bottom line price for each of the Option Periods. The Government will then combine the bottom line price of the base period and the bottom line price of each of the option periods to determine a total evaluated price.

I.6 PERIOD OF PERFORMANCE

(a) Base Performance Period: **09/01/2019 – 08/31/2020**
(b) Optional Performance Period I: **09/01/2020 – 08/31/2021**
(c) Optional Performance Period II: **09/01/2021 – 08/31/2022**
(d) Optional Performance Period III: **09/01/2022 – 08/31/2023**
(e) Optional Performance Period IV: **09/01/2023 – 08/31/2024**

I.7 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.

ATTACHMENT 2

Corporate Experience Questionnaire
Ground Transportation and Security Guard Services

Please complete the Corporate Experience Questionnaire by providing the demographic and corporate experience information for your firm below. Vendors may provide up to three (3) reference projects for ongoing projects or projects completed within the last three (3) years of the date of this RFQ demonstrating relevant experience performing projects similar in size, scope, and complexity to this BPA requirement. A project is considered a single contract or task/delivery order, or a collection of orders under a BPA or IDIQ contract. The vendor's response must provide a clear, specific, and concise description of its relevant corporate experience. Any state, local, or private sector experience can be considered. Extraneous narrative, elaborate brochures, public relations (PR) material, etc. shall not be submitted. If vendors choose to submit as a prime/sub team or under a contractor teaming arrangement (CTA), please indicate which firm's experience is being demonstrated. Vendors may choose only to submit as a prime. The Government will assess the collective experience in each vendor's submittal. The Corporate Experience Questionnaire must be submitted to the Contract Specialist - Matt Russell at *Matthew.J.Russell@cbp.dhs.gov* prior to the date and time for the vendor's scheduled Phone Interview.

1. Firm Information

_____
Firm's Name and Address:

Name and Title of Representative:

Phone:
Fax:
E-mail Address:
_____
Labor Categories provided under projects:

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

If teaming with another firm(s), list their name(s) and address(es):
Firm 1 - Name:
Address:

Firm 2 - Name:
Address:

(**NOTE: If more than two partners are proposed, add the remaining information on a separate sheet of paper.)**

Has this team worked together previously: □ Yes □ No

GSA Contract #:
FSS Schedule #:
Contract Period:

2. List up to three *[3]* projects which demonstrate the firm's or team's prior experience performing work similar to that required by the PWS using the format below:

Project Name and Location	
Nature of the work performed	
Customer Name and Address	
The Firm's Project Manager's Name and Phone Number	
Period of Performance and Percentage Complete	
Estimated or Final Value	

Project Name and Location	
Nature of the work performed	
Customer Name and Address	

The Firm’s Project Manager's Name and Phone Number	
Period of Performance and Percentage Complete	
Estimated or Final Value	

Project Name and Location	
Nature of the work performed	
Customer Name and Address	
The Firm’s Project Manager's Name and Phone Number	
Period of Performance and Percentage Complete	
Estimated or Final Value	

Submitted by:

_____ _____

Signature Date

ATTACHMENT 3

Performance Work Statement (PWS)

PWS RFQ
03C19Q0067_Groun

Transportation Plan (this is for informational purposes only in addition to the PWS)

ALL-2019 Contract
Transportation Plan.

ATTACHMENT 4

Pricing Worksheet/ Sample Task Order

RFQ
03C19Q0067_PRICIN

Sample Task
Order_03C19Q0067_

ATTACHMENT 5

QUALITY ASSURANCE SURVEILLANCE PLAN

QASP_RFQ
03C19Q0067_QASP.c

ATTACHMENT 6

BEST VALUE

BLANKET PURCHASE AGREEMENT

FEDERAL SUPPLY SCHEDULE

(US Customs and Border Protection)

In the spirit of the Federal Acquisition Streamlining Act _____(Agency)_____ and _____(Contractor)_____ enter into an agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s) _____.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: the search for sources; the development of technical documents and solicitations; and the evaluation of bids and offers. Contractor Team Arrangements are permitted with Federal Supply Schedule contractors in accordance with Federal Acquisition Regulation (FAR) Subpart 9.6.

This BPA will further decrease costs, reduce paperwork and save time by eliminating the need for repetitive, individual purchases from the Schedule contract. The end result is to create a purchasing mechanism for the **Government that works better and costs less.**

Signatures:

_____		_____	
AGENCY	DATE	CONTRACTOR	DATE

BPA NUMBER _____

U.S. CUSTOMS AND BORDER PROTECTION
BLANKET PURCHASE AGREEMENT

Pursuant to a General Services Administration (GSA) Federal Supply Schedule (FSS) Contract Number(s) _____, a Blanket Purchase Agreement (BPA) is hereby established between _____ and the U.S. Customs and Border Protection under the terms and conditions of the above stated contract and the following terms and conditions incorporated in this BPA.

ADMINISTRATIVE DATA

Primary Point of Contact: _____

(Complete name, title, _____

corporate address, electronic _____

mail address and phone number) _____

_____

Alternate Point of Contact _____

_____

_____

_____

Contracting Officer to complete the following:

North American Industry Classification (NAIC) Code: _____

Description: _____

Size Standard: _____

The BPA Holder represents that (check all that apply):

It is ☐ is not ☐ a small business concern

Complete the following only if a small business concern:

It is ☐ is not ☐ a small disadvantaged business concern

It is ☐ is not ☐ a women-owned small business concern

It is ☐ is not ☐ a veteran-owned small business concern

It is ☐ is not ☐ a service-disabled veteran-owned small business

It is ☐ is not ☐ a Hub-Zone small business co

(1) AUTHORITY - The authority to establish this BPA is FAR 8.405-3

(2) DESCRIPTION OF AGREEMENT

Under this agreement, the BPA Holder shall provide to U.S. Customs and Border Protection (CBP) southwest border transportation security guard services in support of the US Border Patrol's and Office of Field Operations requirements. These services will be provided when requested by the Contracting Officer. This BPA may include requirements for any organization within Customs and Border Protection, but will primarily focus on support for the Border Patrol.

(3) SERVICES AVAILABLE UNDER THIS BPA

{see the attached Performance Work Statement}

(4) DELIVERY REQUIREMENTS

Delivery requirements will be specified in each task order.

(5) PRICING

The GSA Schedule pricing has been determined to be fair and reasonable by the GSA. Prices to CBP shall be no greater than those charged to the BPA Holder's most favored customer for comparable quantities under similar terms and conditions, in addition to any discounts for quantity, prompt payment, etc. The prices listed on the BPA list that are in effect on the date of the order shall govern that order, unless more favorable pricing is negotiated. [CBP *will seek price reductions from the BPA Holder for all orders.*

The BPA Holder shall update the BPA price list when modifications are made to GSA FSS prices. Price reductions may be offered at any time.

Other Direct Costs (ODC) or non-FSS items ("open market") may be needed on a direct reimbursable or fixed price basis. These will be identified by the individual task order. In addition, in accordance with FAR 8.402(f):

All applicable acquisition regulations pertaining to the purchase of the items not on the FSS have been followed (e.g., publicizing (FAR Part 5), competition requirements

(FAR Part 6), acquisition of commercial items (FAR Part 12), contracting methods (FAR Parts 13, 14, and 15) and small business programs (FAR Part 19);

(b) The ordering activity contracting officer has determined the price for the items on FSS is fair and reasonable;

(c) The items are clearly labeled on the order as items not on the FSS; and

(d) All clauses applicable to items not on the FSS are included in the order.

[*Attach pricing*.]

(6) TERM OF THE BPA

This BPA expires on [*indicate the end date of the BPA Holder's current GSA FSS contract period].* This BPA may be renewed by the CBP Contracting Officer for option year(s) remaining in the BPA Holder's GSA FSS contract, if exercised by GSA. However, this BPA may not exceed a total of 1 years in length (not including any option years). [*Note: A single-award BPA shall not exceed one year. It may have up to four one-year options.]*

If the BPA Holder fails to perform in a manner satisfactory to the Contracting Officer, this BPA may be canceled with 30 days written notice to the BPA Holder by the CO.

(7) EXTENT OF OBLIGATION/VOLUME/PURCHASE LIMITATION

This BPA does not obligate any funds. Funds will be obligated by the placement of task orders.

The Government estimates, but does not guarantee, that the volume of purchases through this agreement will be approximately $291,500,000 ($291.5M).

(8) AUTHORITIES

Only a CBP Contracting Officer may authorize changes in the terms of the BPA during the effective period; renew the BPA for additional periods; or terminate the BPA.

8.1 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 and any issued task order. In the event the BPA Holder 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 task order price to cover any increase in costs incurred as a result thereof. The

Contracting Officer shall be the only individual authorized to accept non-conforming work, waive any requirement of the task order, or to modify any term or condition of the task order. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to a proposed task order can be incurred before receipt of the fully executed task order or specific authorization from the Contracting Officer.

A CBP Contracting Officer's Representative (COR) will be appointed for each task order issued under this BPA. The clause below is applicable to individual task orders. Where the term "contract" is used, "task order" should be substituted.

8.2 HSAR 3052.242-72 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Representative (COR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COR under the contract.

(b) The Contracting Officer cannot authorize the COR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer. [End of Clause]

(9) PREVAILING TERMS AND CONDITIONS

[9.] PRICING PROVISIONS FOR TASK ORDER OR BLANKET PURCHASE AGREEMENT ISSUED UNDER A FEDERAL SUPPLY SCHEDULE (JUN 2005)

This task order/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 task order 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]

[9.2] OPTION TO EXTEND THE TERM OF THE BPA

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the BPA expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended BPA shall be considered to include this option clause.

(c) The total duration of this BPA, including the exercise of any options under this clause, shall not exceed 5 Years.

(End of clause)

[9.3] SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

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 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 requirements are 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 or 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. 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.

c. 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]

[9.4] PREVENT, DETECT AND RESPOND TO SEXUAL ABUSE AND ASSAULT IN CONFINEMENT FACILITIES (FEB 2017)

1. As prescribed by the Prison Rape Elimination Act (PREA) of 2003, 44 U.S.C. § 15601 et. seq., the Contractor shall comply with the Department of Homeland Security (DHS) "Standards to Prevent, Detect and Respond to Sexual Abuse and Assault in Confinement Facilities," codified at 6 C.F.R. Part 115 (the Regulations), for preventing, detecting and responding to sexual abuse and assault within U.S. Customs and Border Protection (CBP) holding facilities[1], whether owned, operated or contracted. The contractor shall also comply with all applicable Federal PREA standards and all applicable DHS and CBP policies implementing PREA.

2. In addition to the general requirements of the above PREA standards and policies, the Contractor further acknowledge the following specific roles and responsibilities in complying with the Regulations:

   a. **Detainee Supervision (6 CFR § 115.113)**: Ensure sufficient supervision of detainees to protect detainees against sexual abuse.

   b. **Juveniles and Family Requirements (6 CFR § 115.114)**: Ensure juvenile and family detainees are afforded the appropriate protections.

c. **Cross-Gender Viewing and Searches (6 CFR § 115.115)**: Implement proper procedures for cross-gender viewing and searches.

d. **Accommodations for Limited English Proficient (LEP) Detainees and Those with Disabilities (6 CFR § 115.116)**: Ensure reasonable measures are taken to ensure detainees who are limited English proficient, and those detainees with disabilities, are given equal access to programs and services at the facility.

e. **Hiring and Promotion (6 CFR § 115.117)**: Ensure no contractors are hired or promoted who have a substantiated history of sexual abuse/assault and that all contractors who may have contact with detainees are required to undergo a background investigation prior to hiring.

f. **Training (6 CFR § 115.131)**: Ensure training of all contractors who may have contact with holding facility detainees to be able to fulfill their responsibilities under the Regulations, including training on:

(1) The agency's zero-tolerance policies for all forms of sexual abuse;

(2) The right of detainees and employees to be free from sexual abuse, and from retaliation for reporting sexual abuse;

(3) Definitions and examples of prohibited and illegal sexual behavior;

(4) Recognition of situations where sexual abuse may occur;

(5) Recognition of physical, behavioral, and emotional signs of sexual abuse, and methods of preventing such occurrences;

(6) Procedures for reporting knowledge or suspicion of sexual abuse;

(7) How to communicate effectively and professionally with detainees, including lesbian, gay, bisexual, transgender, intersex, or gender nonconforming detainees; and

(8) The requirement to limit reporting of sexual abuse to personnel with a need-to-know in order to make decisions concerning the victim's welfare and for law enforcement or investigative purposes.

Confirmation that all contractors who may have contact with holding facility detainees have completed this training must be submitted to the contracting officer, or the contracting officer's designee, and maintained for a least five (5) years.

g. **Risk Assessment (6 CFR § 115.141):** Ensure detainees are assessed for risk of victimization or abusiveness and implement protective measures, as appropriate and available.

h. **Immediate Notification (6 CFR § 115.161)**: Ensure contract staff report immediately to CBP officials any knowledge, suspicion, or information regarding an incident of sexual abuse or assault that occurred; retaliation against individuals who reported or participated in an investigation about such an incident; and any staff neglect or violation of responsibilities that may have contributed to an incident or retaliation.

i. **Corrective Actions (6 CFR § 115.177)**: Contractor personnel suspected of perpetrating sexual abuse shall be prohibited from contact with detainees. Contractors suspected of perpetrating sexual abuse may be removed from all duties requiring detainee contact pending the outcome of an investigation, as appropriate. Contractor shall notify the contracting officer, or contracting officer's designee, identified in the contract within 24 hours of the discipline, removal, termination, or resignation of the suspected employee.

3. The Contractor acknowledges that, in addition to self-monitoring requirements, CBP will conduct third party audits of holding facilities, announced or unannounced, to include on-site monitoring. The Contractor is required to make contract staff available to auditors and agency personnel for interviews, site inspection, and provide relevant documentation to complete a thorough audit of the facility.

4. At all times, the Contractor shall adhere to the standards set forth in the Regulations. Failure to comply with the Regulations may result in termination of the contract.

[1] HOLDING FACILITY: The Regulations define the term "holding facility" as a facility that contains holding cells, cell blocks, or other secure enclosures that are: (1) under the control of the agency; and (2) primarily used for the short-term confinement of individuals who have recently been detained, or are being transferred to or from a court, jail, prison, other agency, or other unit of the facility or agency.

End of Clause

[9.5] 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)

[9.6] 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)

[9.7] STANDARD OF CONDUCT AT GOVERNMENT INSTALLATIONS

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity; and shall be responsible for taking such disciplinary action with respect to its employees, as necessary.

(End of clause)

[9.10] SPECIFICATIONS, STATEMENT 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 52.215-8 incorporated herein by reference.

[End of Clause]

[9.11] PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 9/01/2019 through 8/31/2020.

[End of Clause]

[9.12] ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

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 terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"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.

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)

[9.13] 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]

[9.14] SECURITY PROCEDURES (APR 2019)

A. 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 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.

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 and DHS Sensitive Systems Handbook 4300A, v.12.0, or latest available version.

4. All Contractor Employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Representative (COR). The COR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the

National Capitol Region (NCR), the Office of Professional Responsibility, Security Management Division (OPR/SMD) shall be notified if building access is revoked.

5. All Contractor Employees must be entered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COR. 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 record submission in the CTS database such as, but not limited to, the contractor's legal name, contracting company address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COR or designated government personnel shall provide the CPM with instructions for providing required information.

6. The CO/COR may designate responsibility for out-processing to the CPM. This requires that the CPM have an active CBP Background Investigation (BI) and Active Directory (AD) account. 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 completes a Contractor Performance Report (under Business Relations) or other performance related measures. Additionally, the CO/COR shall immediately notify OPR/SMD of the contractor's departure/separation.

B. Security Background Investigation Requirements

1. 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, Contractor Employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status, § 13E. A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.

2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with 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.

3. Provided the requirements of DHS Instruction Handbook 121-01-007-01 are met as outlined in paragraph 1, above, Contractor Employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope

background investigation (SSBI) prior to commencing work on this contract. 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 BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor Employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).

4. The Contractor Employee shall submit within ten (10) working days after award of this 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 BI or SSBI that meets federal investigation standards. For Contractor employee candidates needing a BI for this contract, the Contractor Employee shall require the applicable Contractor Employees to submit information and documentation requested by CBP to initiate the BI process.

5. Background Investigation information and documentation is usually submitted by proper completion of standard federal and agency forms such as Electronic Questionnaires for investigations Processing (e-QIP), Fingerprint Card, CBP Form 78-Background Investigation Requirements Determination (BIRD), Fair Credit Reporting Act (FCRA) Form, a Contractor Employee Initial Background Investigation (BI) Form (CBP Form 77) (Sections A and B). These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.

6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of its employees who successfully complete the CBP BI or SSBI process to the CO and COR. Failure of any Contractor Employee to obtain and maintain a favorably adjudicated BI or SSBI 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 BI or SSBI requirements may be cause for termination of the contract.

C. 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 personnel will 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. 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.

4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.

5. 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 has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The CPM shall notify the CO/COR via phone, facsimile, 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. If a security clearance is required, the CO/COR will notify OPR/SMD.

E. Non-Disclosure Agreements

As part of the BI 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]

[9.15] 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:

(a) 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.

(b) 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.

(c)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]

[9.16] POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2014)

A. 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.

B. 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.

C. 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)

[9.17] 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]

[9.18] 3052.215-70 KEY PERSONNEL OR FACILITIES (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this Contract:

Program Manager

Sector Manager

(End of clause)