2016

Application Services

NETCENTS-2

Version 2.1

23 September 2016

Table of Contents

Summary of Changes

Date	Change	Name
9/23/2016	Pages 8 & 9 – Changed paragraph names to better define RFQ	T. Bergeron
9/23/2016	Pages 10 - 13 – Updated CLIN structure language for Application Services Small Companion Contract	T. Bergeron
9/23/2016	Pages 34 Changed IA Language to Cyber Security.	T. Bergeron
9/23/2016	Deleted several Contracting Appendices -Application Services Sample Performance Parameters -Application Services Task Order Data Item Description Deliverables -Scope Analysis and Mapping Template -Multi-Functional Team Template -Market Research Report Template -Quality Assurance Surveillance Plan (QASP) Template -Fair Opportunity Exception (FOE) Justification Template	T. Bergeron

	-Fair Opportunity Exception (FOE) Coordination & Approval Template -DD Form 254, Contract Security Classification Specification -Inherently Government Functions (IGF) Memo Template -Government Furnished Property Determination & Findings Template -New Start Validation Template -Independent Government Cost Estimate (IGCE) -Evaluation Guidelines -Ozone Depleting Substance (ODS) Certificate Template -NETCENTS-2 Requirements Approval Documentation (RAD) -Application Services Customer Survey -Customer Ordering Guide Using AFWay – now a standalone document -Example FAR 16 RFP with Evaluation Criteria -Department of Defense Warranty Memorandum -Vendor POC lists for SB and Full and Open – now standalone documents	

NETCENTS-2 APPLICATION SERVICES

1. Scope

The NETCENTS-2 Application Services acquisition provides a vehicle for customers to access a wide range of services such as sustainment, migration, integration, training, help desk support, testing and operational support. Other services include, but are not limited to, exposing data from Authoritative Data Sources (ADS) to support web-services or Service Oriented Architecture (SOA) constructs in AF enterprise environments. Through this vehicle, the contractor shall develop content delivery and presentation services and new mission applications that operate in netcentric enterprise environments that exploit SOA infrastructures. This contract shall support legacy system sustainment, migration and the development of new mission capabilities and applications. The focus of this contract is to provide application services support to mission areas, as overseen by portfolio managers, Communities of Interest (COIs), project offices and program offices.

For work that clearly falls within the scope of this contract, Contracting Officers (COs) are not required to do scope determinations. However, if the CO has any question as to whether the work to be performed on the task order (TOs) falls within the scope of this Indefinite Delivery/Indefinite Quantity (ID/IQ) contract, then the CO should do a scope determination and place it under the appropriate tab in the TO contract file. If you would like scope analysis assistance from the NETCENTS-2 team, review the instructions at A6 – Scope Analysis and Mapping Template and the team will provide a recommendation to the CO.

A Market Research Report is available on the web site (http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp) that describes the overall evaluation process that was performed during source selection to ensure each vendor was qualified to meet the Application Service requirements. COs utilizing the ID/IQ contracts can accelerate their acquisition processes using this document as part of their Market Research required by FAR Part 10.   Re-validation of the contract holder's qualifications need not be conducted.

NOTE: If you do not understand the scope of the Application Services contract, please read the Application Services Performance Work Statement (PWS) to get an overview of the contract.

2. Authorized Users

In addition to the Air Force, DoD and other Federal Agencies may employ the contract when the requirement:

- Relates to requirements for interoperability with Air Force capabilities,
- Supports Air Force IT infrastructure, applications or operation,
- Supports host-tenant arrangements involving Air Force units, or
- Supports joint operations or solutions.

The Air Force reserves the right to restrict use of this contract and to disallow DoD and other Federal Agencies from using this contract.

3. How to Order

This guide does not replace MAJCOM or local contracting procedures. In the event of conflict, COs will use their local procedures. Appendix A1, *Application Services Checklist*, identifies the information necessary for procurement packages. Please complete the required documents and supplementary templates referenced in Appendix A1, *Application Services Checklist*, and submit to your local CO for final approval.

3.1 Full & Open vs. Small Business Companion

The Application Services procurement vehicle includes both full and open and small business (also known as “Companion Contracts”) ID/IQ contracts. **See Clause H137 (5) of the ID/IQ contract to determine whether the Companion Contracts are appropriate. The ordering CO must prepare DD Form 2579, “Small Business Coordination Record,” for procurements exceeding $10,000 to document consideration of small business and incorporation of the FAR 19.7 subcontracting plan where appropriate. The CO should coordinate his/her decisions or recommendations on a particular acquisition with the Office of Small & Disadvantaged Business Utilization (OSDBU) and ensure a Small Business Specialist has reviewed the DD Form 2579.**

Please note guidance may differ for Full & Open and Companion contracts.

Ordering activities should perform sufficient market research to justify the selected contract pool.

3.2 Fair Opportunity Exception (FOE)

The CO will provide all contractors a “fair opportunity” to be considered for each order in excess of $3,500 unless a justifiable condition applies. **See Clause H137 (6) (c) of the ID/IQ contract for applicable exceptions to the fair opportunity process.**

3.3 Decentralized Ordering – NETCENTS e-ordering tool

The local contracting office supporting the requiring activity will award, administer and close out the TO.

Decentralized ordering authority is granted within the AF, and may be granted to DoD and other Federal Agencies, on a non-interference basis with AF ceiling requirements. No decentralized orders shall be placed without an assigned NETCENTS-2 Program Management Office (PMO) control number. AFWay generates the NETCENTS-2 PMO control number for each Request for Proposals/Request for Quote (RFP/RFQ), the CO has successfully submitted to the Application Services vendors. Customers may use this number for tracking purposes throughout the procurement. For in-depth instruction on how to submit a RFP/RFQ in AFWay, refer to *AFWay User’s Guide for App Svs on the Application Services Documents Page on our website*.

3.4 Requests for Proposals (RFP)

Once the CO assembles a complete requirements package, he or she may solicit NETCENTS-2 Application Services vendors for solution proposals through AFWay, the e-Ordering tool for all NETCENTS-2 ID/IQ contracts. The CO should initiate and process a RFP, and receive vendor responses to the RFP, through AFWay. After evaluating and selecting the best vendor solution, the CO should then award through AFWay. Instructions and guidance for this entire process is available on the AFWay User's Guide for App Svs on the Application Services Documents Page on our Website. If the number or size of attachments poses an issue to processing an RFI through AFWay, **use the AMRDEC SAFE ACCESS FILE EXCHANGE (SAFE) website to post documentation. Directions of the use of SAFE can be found in Appendix 5.**

3.5 Requests for Information (RFI)

Customers can post an RFI to solicit vendors for assistance in the development of their Performance Work Statement (PWS), to see if the vendors can meet the requirements of the PWS or to determine whether to use the small business or the full and open pool of contract holders. Draft RFPs can also be used to gather this information. The RFI should describe the requirements and solicit interested vendors for capability statements or other relevant information. However, the RFI **should not** be used to find out if the vendors have the capabilities that have already been determined in the overarching ID/IQ vehicles. Submit RFIs, through AFWay observing the same process for submitting a RFQ with "RFI" at the beginning of the title. Refer to the AFWay User's Guide for App Svs on the Application Services Page of our Website for instructions. If the number or size of attachments poses an issue to processing an RFI through AFWay, **use the AMRDEC SAFE ACCESS FILE EXCHANGE (SAFE) website to post documentation. Directions of the use of SAFE can be found in Appendix A3.**

3.6 Classified TO Procurement

Customers and COs who have CLASSIFIED requirements within scope of Application Services are able to compete their requirements using the following procedure:

- Post a notice on AFWAY that your organization has a CLASSIFIED requirement. This will generate an AFWAY RFQ # that will be included in the RFP. Have the vendor respond to the CO with the name(s) of any offeror representative(s) who should receive the CLASSIFIED RFP along with their classification level and contact information.
- Validate the classification information provided by the offeror(s).
- Distribute the CLASSIFIED RFP through secure channels ONLY to the appropriate offeror representatives. Include the AFWAY RFQ # in the RFP.
- Receive the CLASSIFIED proposal through secure channels.
- Proceed with evaluation and award of the TO.

AFWay is an UNCLASSIFIED system and cannot process or compete any RFPs/RFQs that contain classified information.

3.7 TO Requiring Hardware/Software Products

TOs that require hardware or software products shall be purchased by the Application Services vendors from the NETCENTS-2 Products vendors. Customers should carefully review the PWS template in Appendix A2 and ensure applicable products standards are written into the PWS to ensure compatibility and compliance with AF network standards. A minimum of two estimates with each RFP/RFQ solution response is required.

4. ID/IQ Ordering Period

TOs may be issued at any time during the ordering period. The Application Services ID/IQ contract has a 7-year ordering period which consists of a 3-year base period and four 12-month options.

4.1 Full & Open

The Full & Open Application Services ID/IQ was awarded 31 March 2015. AFWAY is accepting RFQs as of 22 April 2015.

4.2 Small Business Companion

Base Period:	June 21, 2012 – June 20, 2015
*Option Period One:	June 21, 2015 – June 20, 2016
*Option Period Two:	June 21, 2016 – June 20, 2017
*Option Period Three:	June 21, 2017 – June 20, 2018
*Option Period Four:	June 21, 2018 – June 20, 2019

4.3 Full & Open

Base Period:	March 31, 2015 – March 30, 2018
*Option Period One:	March 31, 2018 – March 30, 2019
*Option Period Two:	March 31, 2019 – March 30, 2020
*Option Period Three:	March 31, 2020 – March 30, 2021
*Option Period Four:	March 31, 2021 – March 30, 2022

5. Task Order Period of Performance

The TO shall identify the period of performance. **See Clause F002 of the basic ID/IQ contract.**

The total duration of any TO issued under this basic contract shall not exceed 5 years, including all option periods. The period of performance for any TO shall not extend more than 3 years beyond the last day of the basic contract ordering period (e.g., a TO issued on the last day of the ordering period of the basic contract could have a 1-year base period and two 1-year option periods). **See Clause 52.216-22 (OCT 1995) of the basic ID/IQ contract.**

6. Prime Contractor Information

6.1 Full & Open

Refer to the App Svs Full and Open Vendor POC List under the Application Services Support Documents window of the Application Services Document page on our website, http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp

6.2 Small Business Companion

Refer to the App Svs Small Business Companion Vendor POC List under the Application Services Support Documents window of the Application Services Document page on our website, http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp

7. CLIN / Pricing Structure

7.1 Full & Open

Base Period (3-yr)	Option Period 1 (1-yr)	Option Period 2 (1-yr)	Option Period 3 (1-yr)	Option Period 4 (1-yr)	Description	Pricing
0100	1100	2100	3100	4100	Network Centric Solutions	Firm Fixed Price (FFP)
0200	1200	2200	3200	4200	Network Centric Solutions	Cost
0300	1300	2300	3300	4300	Network Centric Services	Labor Hour –10% cap
0400	1400	2400	3400	4400	Data	NSP
0500	1500	2500	3500	4500	Warranty	(FFP)
0600	1600	2600	3600	4600	Other Direct Costs (ODC)	Cost
0700	1700	2700	3700	4700	Travel	Cost
0800	1800	2800	3800		NetCents-2 Post Award Conference	(FFP) – One Time Use

Contract Line Item Numbering (CLIN) shall be IAW DFARS 204.71 and PGI 204.71. When multiple contract line items are required the CLIN structure shall maintain compliance with the basic NETCENTS-2 Full and Open CLIN structure. For example, all requirements using CLIN 0100 shall contain a "0" in the first digit and a "1" in the second digit and maintain the contract type, Fixed Price and all requirements using CLIN 0200 shall contain a "0" in the first digit and a "2" in the second digit and maintain the contract type, Cost. This compliance shall be the same for the following CLINs: 0300, 0400, 0500, 0600 and 0700.

Any TO issued during the ID/IQ Base Period must use the Base Period CLIN Structure. Once an Option Period has been *exercised*, any TO issued during that Option Period must use the CLIN structure from that Option Period.

Contracting activities may use multiple contract line items and subcontract line items when appropriate as long as the "root" CLIN is compliant with the NETCENTS ID/IQ contract.

Each number identified in the CLIN represents a specific element of the ID/IQ Contract. For example, the base year period CLIN 0100 is broken down into four (4) distinct components:

- **The first digit represents the Ordering Period of the ID/IQ.**
- **The second digit represents the Contract Type.**
- **The third digit is reserved for the Small Business CLIN Structure.**
- **The fourth digit can be modified for use in multiple CLINs.**

Examples:
CLIN 0100 - NETCENTRIC Total Solution - Base Year
CLIN 0101 - NETCENTRIC Total Solution - Option Year One
CLIN 0102 - NETCENTRIC Total Solution - Option Year Two
CLIN 0103 - NETCENTRIC Total Solution - Option Year Three
CLIN 0104 - NETCENTRIC Total Solution - Option Year Four

OR,
CLIN 0100 - NETCENTRIC Total Solution
Sub-CLIN 0100AA - NETCENTRIC Total Solution - Base Year
Sub-CLIN 0100AB - NETCENTRIC Total Solution - Option Year One
Sub-CLIN 0100AC - NETCENTRIC Total Solution - Option Year Two
Sub-CLIN 0100AD - NETCENTRIC Total Solution - Option Year Three
Sub-CLIN 0100AE - NETCENTRIC Total Solution - Option Year Four

If that TO had a second FP CLIN it would appear as follows:
CLIN 0105 - NETCENTRIC Total Solution - Base Year
CLIN 0106 - NETCENTRIC Total Solution - Option Year One
CLIN 0107 - NETCENTRIC Total Solution - Option Year Two
CLIN 0108 - NETCENTRIC Total Solution - Option Year Three
CLIN 0109 - NETCENTRIC Total Solution - Option Year Four

OR,
CLIN 0011 - NETCENTRIC Total Solution
Sub-CLIN 0101AA - NETCENTRIC Total Solution - Base Year
Sub-CLIN 0101AB - NETCENTRIC Total Solution - Option Year One
Sub-CLIN 0101AC - NETCENTRIC Total Solution - Option Year Two
Sub-CLIN 0101AD - NETCENTRIC Total Solution - Option Year Three
Sub-CLIN 0101AE - NETCENTRIC Total Solution - Option Year Four

7.2 7.2 Small Business Companion

Base Period (3-yr)	Option Period 1 (1-yr)	Option Period 2 (1-yr)	Option Period 3 (1-yr)	Option Period 4 (1-yr)	Description	Pricing
0010	1010	2010	3010	4010	Network Centric Solutions	Firm Fixed Price (FFP)
0020	1020	2020	3020	4020	Network Centric Solutions	Cost
0030	1030	2030	3030	4030	Network Centric Services	Labor Hour –10% cap
0040	1040	2040	3040	4040	Data	NSP
0050	1050	2050	3050	4050	Warranty	(FFP)
0060	1060	2060	3060	4060	Other Direct Costs (ODC)	Cost
0070	1070	2070	3070	4070	Travel	Cost
0080	1080	2090	3090		NetCents-2 Post Award Conference	(FFP) – One Time Use
		2080**	3080**		Small Business Graduate Data Submission	Included in CLIN 2010, 2020, 2030, 3010, 3020 or 3030

****** This **ONE-TIME USE CLIN** is established for small business companion contractors who are unable to recertify as a small business concern **as stated in Clause H139** and who elect to transition into the UNRESTRICTED multiple award ID/IQ contract pool for Application Services. This **ONE-TIME USE CLIN** provides small business companion contractors the opportunity to be considered for award of CLINs 3100-3700 and/or 4100-4700 **as stated in Clause H139 of this ID/IQ contract.**

CLIN shall be IAW DFARS 204.71 and PGI 204.71. When multiple contract line items are required the CLIN structure shall maintain compliance with the basic NETCENTS-2 Application Services SB CLIN structure. Currently in option year 2, 21 June 2016 – 20 June 2017, for example, all requirements using CLIN 2010 shall contain a "2" in the first digit and a "1" in the third digit and maintain the contract type, Fixed Price; all requirements using CLIN 2020 shall contain a "2" in the first digit and a "2" in the third digit and maintain the contract type, Cost. This compliance shall be the same for the following CLINs: 1030, 1040, 1050, 1060 and 1070. Any TO issued during that Option Period must use the CLIN structure from that Option Period.

Contracting activities may use multiple contract line items and subcontract line items when appropriate as long as the "root" CLIN is compliant with the NETCENTS ID/IQ contract.

Each number identified in the CLIN represents a specific element of the ID/IQ Contract. For example, the option year 2, CLIN 2010 is broken down into four distinct components:

- The first digit represents the Ordering Period of the ID/IQ.
- The second digit is reserved for the Full and Open CLIN Structure.
- The third digit represents the Contract Type.
- The fourth digit can be modified for use in multiple CLINs.

Examples:
CLIN 2010 - NETCENTRIC Total Solution - Base Year
CLIN 2011 - NETCENTRIC Total Solution - Option Year One
CLIN 2012 - NETCENTRIC Total Solution - Option Year Two
CLIN 2013 - NETCENTRIC Total Solution - Option Year Three
CLIN 2014 - NETCENTRIC Total Solution - Option Year Four

OR,

CLIN 2010 - NETCENTRIC Total Solution
Sub-CLIN 2010AA - NETCENTRIC Total Solution - Base Year
Sub-CLIN 2010AB - NETCENTRIC Total Solution - Option Year One
Sub-CLIN 2010AC - NETCENTRIC Total Solution - Option Year Two
Sub-CLIN 2010AD - NETCENTRIC Total Solution - Option Year Three
Sub-CLIN 2010AE - NETCENTRIC Total Solution - Option Year Four

If that TO had a second FP CLIN it would appear as follows:

CLIN 2015 - NETCENTRIC Total Solution - Base Year
CLIN 2016 - NETCENTRIC Total Solution - Option Year One
CLIN 2017 - NETCENTRIC Total Solution - Option Year Two
CLIN 2018 - NETCENTRIC Total Solution - Option Year Three
CLIN 2019 - NETCENTRIC Total Solution - Option Year Four

OR,

CLIN 2011 - NETCENTRIC Total Solution
Sub-CLIN 2011AA - NETCENTRIC Total Solution - Base Year
Sub-CLIN 2011AB - NETCENTRIC Total Solution - Option Year One
Sub-CLIN 2011AC - NETCENTRIC Total Solution - Option Year Two
Sub-CLIN 2011AD - NETCENTRIC Total Solution - Option Year Three
Sub-CLIN 2011AE - NETCENTRIC Total Solution - Option Year Four

8. North American Industry Classifications System (NAICS) Code

The North American Industry Classification System (NAICS) code for the NETCENTS-2 Application Services ID/IQ contract is 541511, Custom Computer Programming Service; cannot be changed at the TO level. If there are any questions, please contact the Procuring Contract Officer (PCO) or send an e-mail to NETCENTS-2 Customer Support at netcents@us.af.mil.

9. Contractor Certification

9.1 Full & Open

Each contractor is required to maintain a Capability Maturity Model Integration (CMMI)-DEV Level 3.

9.2 Small Business Companion

The prime contractor shall be appraised at Level 2 or higher for Capability Maturity Model (CMM), CMMI, or CMMI Development using the Software Engineering Institute's (SEI) Standard CMMI Appraisal Method for Process Improvement (SCAMPI) (Method A) by an SEI-authorized lead appraiser, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the organizational level performing the contract. If not SEI appraised, acceptable comparable Systems Engineering (SE) processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance.

10. Contract Data Requirements List (ID/IQ Level)

Section J, Exhibit A, A005 Contractor Manpower Reporting

In order to implement FY11 NDAA Section 8108, Contractor Inventory, the contractors are required to report all contractor labor hours (including subcontractor labor hours) required for performance of all services provided under the Application Services ID/IQ contracts. The reporting will be done for each TO awarded in the Contractor Manpower Reporting Application at http://www.ecmra.mil.

Each TO should provide the contractor with your organization's Requiring Activity Code (RA UIC).

11. Points of Contact

Customer Support (CS) – For all Application Services CS issues, please email CS at netcents@us.af.mil. Please ensure **"Application Services"** is noted in the subject line for appropriate distribution and review. If you require immediate assistance, the CS can be reached at 334-416-5070, option 1.

12. NETCENTS-2 Document Updates

In order to be aware of changes to this and other NETCENTS-2 documents, please follow the instructions in Appendix A6 NETCENTS-2 RSS Feed Instructions.

Appendix A1 – Application Services Requirements Package Checklist

Instructions: Use this checklist as a guide to complete your requirements package. Submit your resulting requirements package to your CO to continue the process towards TO issuance. If your local contracting squadron has their own checklist, you may use that. Please ensure it includes the items listed here if needed.

#	DOCUMENTATION	REFERENCE	STATUS
1.	**TASK ORDER INFORMATION**		
a.	Agency/Department: Organization Office Symbol: Organization Address:		□
b.	Task Order Title: Brief Description:		□
c.	Customer Requiring Activity POCs Primary POC Name: Title: Email: Phone: Secondary POC Name: Title: Email: Phone:		□
d.	Period of Performance:	Application Services Users Guide, Section 5	□
2.	**SCOPE ANALYSIS & DETERMINATION**		
a.	Complete a Scope Analysis by mapping your proposed requirements to the Application Services ID/IQ requirements contained in the Application Services PWS, available at http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp." This action ensures proposed requirements fall within scope of the Application Services ID/IQ.	A2: Application Services TO PWS Template	□

#	DOCUMENTATION	REFERENCE	STATUS
b.	You may request that the NC-2 Application Services Team provide an analysis of your Mapping in support of the Contracting Officer's Scope Determination. If this is needed send your PWS to NETCENTS@us.af.mil with "Scope Analysis Request" in the subject line.		□
3.	**MULTI-FUNCTIONAL TEAM**		
	Appoint a Multi-Functional Team (MFT) of key stakeholders to ensure that this acquisition integrates the needs of the mission with the requirement to procure a performance-based service acquisition. If needed, a MFT template is provided.		□
4.	**MARKET RESEARCH**		
	Perform and document market research in a manner adequate to support acquisition decisions. As part of the initial award for the Application Services ID/IQ contract, the Government found contract holders qualified to perform under the general PWS.		□
5.	**ACQUISITION PLANNING**		
a.	Some larger and more complex acquisitions may require an Acquisition Plan.	FAR 7.103 – 7.107 AFFARS 5307.104 – 92(b)(3)	□
b.	Provide Acquisition Strategy Panel (ASP) Briefing Charts and ASP Minutes, if applicable.	AFFARS 5307.104 – 90	□
c.	Multi-Functional Independent Review Teams (MIRTs) are required for Acquisitions greater than $50M. There are five (5) reviews required that make up the MIRT process that will significantly add to the duration of the schedule, if not waived. Determine whether all reviews composing the MIRT process are required.	AFFARS 5301.90 MP 5301.9001(b)	□
6.	**NAICS CODE**		
	The **NAICS** code for the Application Services ID/IQ has already been determined to be: **541511, Custom Computer Programming Service**. This cannot be changed at the Task Order level.		□
7.	**SERVICES DESIGNATED OFFICIAL (SDO)**		

#	DOCUMENTATION	REFERENCE	STATUS
	Appoint a SDO to coordinate with AFPEO/CM for all requirements with an estimated value of $100 M or greater, and for coordination with OSD of IT requirements over $500M and other requirements over $1B.	AFI 63-101, Chapter 4, Section 4.4	□
8.	**QUALITY ASSURANCE**		
a.	Appoint a Contracting Officer Representative (COR) if not already identified as part of the Multi-Functional Team.	COR Appointment Letter Template	□
b.	Retain a copy of the COR's Phase 1 Training Certificate. **Must be completed before release of the RFP.**	OUSD (AT&L) Memo, 29 Mar 2010	□
c.	Provide a Quality Assurance Surveillance Plan (QASP).		□
9.	**REQUIREMENTS**		
a.	Is this a Sole Source Task Order? Contractor:	FAR 6.302 FAR 8.405-6	□Yes □No
b.	If this is a Sole Source, provide Justification for a Fair Opportunity Exception (FOE). If Justification is approved, use the appropriate FOE Coordination & Approval template, which is based on the Task Order amount.	FAR 16.505(b)(2)	□
c.	Use the Application Services TO PWS Template to provide a Performance Work Statement with attention to the following sections: - Services Delivery Summary - Data Item Deliverables - Standards & References	A2: Application Services TO PWS Template	□
d.	If classified information necessitates contractual security specifications, complete and include a DD 254.	AFI 31-601, Chapter 4	□
e.	Are there any supplementary attachments that need to be provided (i.e., software design plans, testing and integration plans, etc.)?		□Yes □No
f.	Are there any requirements which are Mission Essential Requirements? If yes, they must be identified as such.	DoDI 1100.22	□Yes □No
g.	Complete certification that Contractor will not perform Inherently Governmental Functions (IGF).		□Yes □No

#	DOCUMENTATION	REFERENCE	STATUS
h.	Complete **Government Furnished Property (GFP) and Space** that the GFP or space is available (as applicable).		□
i.	Provide justification if any consolidated contract requirements; i.e., two or more requirements previously acquired separately now consolidated into a single requirement applicable to actions greater than $5M.	DFARS 207.170-2 AFFARS 5307.170-3	□Yes □No
j.	If a new start program/project, provide supporting file documentation, including appropriate congressional notification/approvals.		□Yes □No
10.	**INDEPENDENT GOVERNMENT COST ESTIMATE (IGCE)**		
	Provide a copy of an Independent Government Cost Estimate (IGCE) to include costs for option years.		□
11.	**TASK ORDER AWARD EVALUATION**		
a.	Use the Evaluation Guidelines to outline selection criteria for Task Order award for ordering CO approval.		□
b.	Prepare an **Instruction to Offerors** for ordering CO approval.		□
12.	**FUNDING DOCUMENTS**		
a.	Provide funding documents (i.e., MIPR, PR, etc.) and ensure sufficient funds are available for the effort and funding appropriation properly matches the services being procured.	FAR 32.702 DFARS 204.7103 DoD 7000.14R	□
b.	Are the services being requested **severable or non-severable**? Severable services cannot exceed one year.	DoD 7000.14R, Vol. III, Chapter 8	□
c.	Confirm within 5 days of contract award, the Wide Area Workflow Inspector Code.	DFARS 252.232-7003	□
13.	**CLIN / PRICING STRUCTURE**		
	Provide a CLIN / Pricing Structure.	Application Services Users Guide Section 7	□
14.	**OZONE DEPLETING SUBSTANCE (ODS)**		
	Provide either a certification that there is no Class I ODS or a copy of the GO/SES approval for use of Class I ODS.		□
15.	**REQUIREMENTS APPROVAL DOCUMENTATION (RAD)**		

#	DOCUMENTATION	REFERENCE	STATUS
	A NETCENTS-2 RAD was accomplished. Local Contracting and MAJCOM's should be consulted to determine if a TO RAD is required. If a RAD is required you can use the NETCENTS-2 RAD as a starting point.		□
16.	**TASK ORDER POST AWARD TASKS**		
a.	The **Contractor Performance Assessment Reporting System (CPARS)** is required for NETCENTS-2 Task Orders that exceed $1M. Provide a CPAR point of contact, which is normally the Contracting Officer Representative (COR). CPAR Focal Point Name: E-mail: Phone:		□
b.	If the Task Order is projected to be less than $1M, a Customer Survey is required instead of a (CPAR).		□
c.	**Public Disclosure of Information** Does the PWS contain information that, if released, would be harmful to the government? FOIA Coordinator Name: E-mail: Physical Address:		□

Appendix A2 – Application Services Task Order PWS Template

(NOTE: This is the broad based USAF Application Services Template. If you are in PEO BES and need the AF PEO BES System Sustainment template, please download it from the NETCENTS-2 website under Application Services Documents Templates. http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp)

INSTRUCTIONS:

1. **You may use this format for your Application Services PW S. Using a standard template helps offerors know where to look for requirements and can decrease the time required to solicit proposals for the TOs.**

2. **Save a copy of this template and modify it according to your requirements. Each time a PWS is accomplished, come back to the User's Guide and download the PWS template. The language, standards and references will be updated over time.**

3. **All bold italic text within brackets [ ] is instructional information specific to the section.**

4. **Text not within brackets is information that you are HIGHLY ENCOURAGED to keep in your PWS; only apply modifications, introduce additional information or include updates in the event that standards or instructions change, or when deemed necessary by your specific program's or organization's policies.**

5. **All citations to policies, directives, instructions and reference material are included in *Application Services Standards & References on the Application Services Documents Page on our website*.**

6. **If you need assistance in writing your specific requirements, you may use the DAU Service Acquisition Mall (SAM) website, http://sam.dau.mil/. Within this link you will find Sample Task Statements, http://sam.dau.mil/Content.aspx?currentContentID=sample_task_statements and Sample Performance Standards, http://sam.dau.mil/Content.aspx?currentContentID=sample_performance_standards. There is a further link in the mall that includes a video on how to write a PWS/SOO, http://sam.dau.mil/Content.aspx?currentContentID=pws_soo. Assistance in building your evaluation factors can be addressed with this link, http://sam.dau.mil/Content.aspx?currentContentID=arrt_evaluation_factors.**

7. **Before submitting your completed PWS, REMEMBER TO DELETE all instructional text contained within brackets. It is shown here for instructional purposes only and must not remain in the final document.**

NETCENTS-2 SOLUTIONS
Application Services – Full & Open / Small Business Companion
[Add Your Own Task Order Title]
Task Order Performance Work Statement (PWS)

Name:	
Organization:	
Address:	***[physical mailing address]***

Executive Summary

[*Provide a <u>short</u> description of the work to be performed.*]

NETCENTS-2 Application Services TO PWS
[Requesting Agency TO Title]

1. PURPOSE

[In this paragraph, define the overall purpose and objectives of the TO.]

2. SCOPE

[In this paragraph, summarize the specific type(s) of support your organization/program office is seeking and who the work supports – what organization(s) or domain(s). Context is very important here. Some items that may be helpful could be organizational charts, discussion of geographic locations requiring support and clearly defined stakeholders.]

3. REQUIREMENT(S)/DESCRIPTION OF SERVICE(S)

[In this paragraph, describe the broad level of service(s) required under the TO, not each specific activity. It should be consistent with the outcomes defined in the Services Delivery Summary and linked to Air Force/organizational requirements. The objective is to state, using established industry/government standards, what we need (objective) not how we need each task accomplished (methodology). Tailor the following to meet required Systems Sustainment services. To make your requirement(s) contractually binding the PWS must state, "The Contractor shall," for each requirement. Call out "as-is" and "to-be" artifacts to assist offerors in understanding the requirement. Place links or instructions on how to access these system artifacts, sometimes known as the bidder's library. This includes Architecture Views, ISPs, Design Documents, Installation Plans, Users Guide, ConOps, etc.]

[Any dependencies known that are outside the control of the Program Office and of the vendor should be clearly stated. For example, if the operational environment is managed by DISA and the test environment and processes by the CIE and/or RTO, this needs to be stated. Must they prepare packages to be deployed through AFCEDS? If the contractor must use the government help desk tracking system, this needs to be explained. The vendors must understand the existing development, test and operational environments in detail. If you expect the vendor to modify (tech refresh, etc.) any of those environments or components as part of system sustainment, this must be clearly stated.]

Factor	**Data**
Code and data complexity	Include the following types of information: Number of code modules by type (i.e. C, Java, JSP, PL/SQL, TCL/TK, C#, COBOL, 4GL, Pearl, etc.) Number of reusable modules (i.e. COBOL copy book elements, C library modules, Java utility classes/libraries, Screen/HTML templates, XML modules, JCL, Unix scripts, Screen resource elements, Stored Procedures, SOA web services, etc.)

Factor	**Data**
	Number of online screens. Number of report programs (if using COTS BI/Ad Hoc Reporting tools, provide the number and types of each module including database table views, joins, Cubes, etc.). Database definitions (i.e. number of tables, number of data elements, number of primary keys, foreign keys, number of table joins, etc.). This can be provided in the form of logical and physical data models.
Stability	Provide the Mean Time to Repair on the legacy code. Provide the defect density (the number of defects/DIREPS/SCRs average per Function Point or 1000 Lines of code). This is preferred by the type of code listed in the first row of this table. The average (in FP or SLOC) number of modifications/improvements per period (quarterly, annually, etc.) per Baseline Change Request.
Number of concurrent users	
Application age	
Function Points Inputs External Inputs	
External Outputs	
Logical Internal Files	
External Interfaces	
External Inquiries	
Initial response time	Provide the current average response time for online applications and/or web services. Provide the expected/desired response time for online applications and/or web services.

Factor	Data
	If there are throughput requirements on batch/background updates or reports, provide the current average and the desired goal/objective.
Life expectancy	
Operating system	Provide a complete list of the OS and all COTS/GOTS utilities including Development Tools along with the version numbers of each.
Platform	Provide the list of the HW baseline for servers along with capacity, model numbers, etc.
Programming Languages	See first row above. Also provide the programming language versions being used (i.e. Java 1.6, TCL/TK 8.4.x, COBOL 85, Oracle 11G, etc.)
Programs	See row 1 above. This need to be expanded to show the profile of all the types of development components (i.e. copy books, libraries, JCL, scripts, screen definitions, etc.) and not just the number of programs.
Database	See row 1 above on the database information needed.
COTS	Provide complete list and version numbers. Also provide any licensing restrictions/limitations that my prohibit exploitation by a bidder on the use of a product that is limited for that application/project.
Avg transactions per day	This needs to be by type (i.e. updates, inquiries, web services, etc.).
Interfaces	Provide ICDs or equivalent information about the nature and design of the interface (i.e. frequency, data definitions, triggers, mechanism such as ftp or web service, etc.).
Upgrades	Planned as well as past history for both COTS and the applications.
Average help desk call volume	Provide by severity levels and the numbers that have passed from level 1 to 2 to 3.

[TO that require hardware or software products shall be purchased by the Application Services vendors from the NETCENTS-2 Products contract vendors. Customers should carefully review and include any products standards and requirements in Section 9 of this TO PWS to ensure applicable products standards are written into the PWS to ensure compatibility and compliance with AF network standards.]

3.1 Systems Sustainment

Systems sustainment requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

The contractor shall design, develop, test and package systems and software changes as well as provide problem resolutions for the existing system. The contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as required. The contractor shall provide to the government all developed, modified or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to develop each approved systems change request. Specific tasks may include the following:

- Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases and interfaces in compliance with applicable AF/DoD standards.

- Support system sustainment activities to include maintaining existing legacy systems and environments and to sustain applications, databases and interfaces.

- Provide application services to support, maintain and operate systems or services.

[NOTE: Remove entire section if not applicable or modify to meet your requirements.]

3.2 Systems Development, Migration and Integration

Systems development, migration and integration requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

- Conduct software development, software security, web services development, web services testing, smart phone or other IT device applications and testing, security layer integration, database clean-up, data wrapping and data conversion.

- Develop, operate and maintain prototype applications, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. Develop schedules and implementation plans, including parallel operations, identification of technical approaches and a description of anticipated prototype results.

- Perform system performance tuning, system re-hosting and integration services.

- Migrate legacy systems to an Enterprise Resource Planning (ERP) system or an existing standard infrastructure such as the Global Combat Support System (GCSS) or DoD Enterprise Computing Center (DECC).

- Utilize Government-Off-The-Shelf (GOTS) or approved Commercial-Off-The-Shelf (COTS) tools for systems design and development.

- Ensure all mobile applications being developed comply with DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) section (3f) and they must be developed to be device agnostic. Ensure compliance with the DoD Mobile Development Strategy V2.0 dated May 2012.

- If applicable, ensure compliance with the USAF Implementation Baseline (IB). The IB is applicable to IT programs, new systems/applications, major increments and/or applications migrating to new infrastructure environments as identified in the baseline documentation.

  (For the latest IB version: IB version 2.1 documents are available on the RESTRICTED DTIC site (http://www.dtic.mil). Because the documents are marked "Distribution D," it precludes them being made available on the public DTIC site. Once a publicly releasable version is accomplished, it will be available on the NETCENTS-2 web site. Anyone needing the IB documents must first register for an account on DTIC. Once account registration is completed and approved, the user must select the "DTIC Online Access Control (DOAC)" link on the right side of the DTIC homepage and then click, "Connect Now." Keep in mind that the public DTIC site is BLUE and the restricted side is GREEN. Searching "Technical Reports" using the title, 'Implementation Baseline V2.1,' seems to be the most efficient method for returning the documents. There are six IB V2.1 documents in total; the main IB with five addenda (ERP, DEAMS Migration, .NET for STAX, ELS Use Cases, Enterprise Claims Service). For some reason, the documents are not all returned together; the user needs to scroll through the first 1 to 12 hits to locate all 6.

[NOTE: Remove entire section if not applicable or modify to meet your requirements.]

3.3 Information Services

Information services requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

The contractor shall provide application and content presentation services that identify and exploit existing services, create new Service-Oriented Architecture applications and data services, create presentation services, define, align and register vocabularies, expose information assets for discovery in the Metadata Environment (MDE) for COI, provide wrapping services and provide data layer connectivity.

3.3.1 Development of New SOA Applications and Data Services

- Expose authoritative data, as defined, by re-engineering a business process, identifying the sources for the authoritative data and establishing user roles and permissions for information access as directed by COI.

- Support life-cycle management of new SOA-based applications that encapsulate business logic to provide new functional/operational mission capabilities.

[NOTE: Remove entire section if not applicable.]

3.3.2 Create Aggregation Services

- Create aggregation services that deliver capabilities by coupling multiple core data services to construct new information assets.

- Avoid duplication of data available from other authoritative sources, performance permitting.
- Invoke enclave security services to mitigate security issues from aggregating data from multiple Authoritative Data Sources (ADS).
- Create repositories for new authoritative data generated from aggregation services.
- Create services through which content can be creatively combined, searched and/or correlated.

[NOTE: Remove entire section if not applicable.]

3.3.3 Create Presentation Services

- Create presentation services that are required to display information unique to a specific set of users and to deliver specific mission capabilities.
- Develop these presentation services to be available from the SOA infrastructure to provide content on-demand.

[NOTE: Remove entire section if not applicable.]

3.3.4 Specify Information Assets for Exposure

- Generate specification for exposing authoritative data as information asset payloads.
- Create semi-automated services that enable the specification of information assets by editing, sorting, filtering and translating.
- Utilize applicable data definitions and standards for information assets to be exposed.
- Create schema/documentation for organizations to register for use throughout the DoD enterprise.

[NOTE: Remove entire section if not applicable.]

3.3.5 Registering Services

Support the registration of ADS exposure services, aggregation services and presentation services.

[NOTE: Remove entire section if not applicable.]

3.3.6 Web Services

Create and maintain web services using standards as defined within the Enterprise Architecture to enable sharing of data across different applications in an enterprise.

[NOTE: Remove entire section if not applicable.]

3.3.7 Service Life-cycle Management

Generate necessary design and implementation artifacts that will support life-cycle management, defined as service development, testing, certification, registration, sustainment and evolution aligned with defined requirements. These artifacts will include the metadata needed for service life-cycle management IAW the current version of the DoD Discovery

Metadata Specification (DDMS). The design and implementation artifacts for Top Secret network systems and applications, as well as ISR mission systems, are owned by the government and provided to the government representative prior to the end of the TO at no additional cost to the government unless otherwise stated in the TO.

[NOTE: Remove entire section if not applicable.]

3.3.8 Vocabulary Management

- Support the development of vocabularies.
- Create and maintain Web Ontology Language (WOL) vocabularies and schemas.
- Verify vocabularies do not overlap and/or contradict other ADS vocabularies.
- Resolve discrepancies and eliminate redundancies of vocabularies.

[NOTE: Remove entire section if not applicable.]

3.3.9 Register Vocabularies

Support the alignment, articulation and registration of vocabulary artifacts.

[NOTE: Remove entire section if not applicable.]

3.3.10 Data Stores

- Create and maintain data stores.
- Provide services such as data cleansing, redundancy resolution and business rule validation.
- Monitor and maintain these data stores to ensure data availability, accuracy, precision and responsiveness.

[NOTE: Remove entire section if not applicable.]

3.3.11 Information Exposure Services

- Provide application services.
- Prepare and standardize data retrieved from legacy information sources.
- Modify the information source's interface, data and/or behavior for standardized accessibility.
- Transform communication interfaces, data structures and program semantic alignment
    - Provide standardized communication/program wrapping services, data language translation, etc.
- Employ configuration management plan of existing legacy baseline code and data exposure code.

[NOTE: Remove entire section if not applicable.]

3.4 Systems Operations

Systems operations requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

The contractor shall provide operational support services including, but not limited to, database administration, systems administration, customer training and help desk support of both legacy and new applications and systems in accordance with AFI 33-115 Network Operations and DoD 8570.01M Information Assurance Workforce Improvement Program.

3.4.1 Database Administration

- Create and test backups of data, provide data cleansing services, verify data integrity, implement access controls.
- Assist developers of data exposure services with engagement of the database.

[NOTE: Remove entire section if not applicable.]

3.4.2 Systems Administration

- Install, support and maintain computer systems.
- Plan and respond to service outages.
- Diagnose software and hardware failures to resolution.
- Implement and ensure security preventive measures are fully functioning.
- Monitor and enhance system performance.

[NOTE: Remove entire section if not applicable.]

3.4.3 Customer Training

- Provide on-site training at government and contractor locations.
- Develop, maintain and/or update student and instructor training programs and materials.
- Ensure training stays current with the services offered throughout the life of the TO.

[NOTE: Remove entire section if not applicable.]

3.4.4 Help Desk Support

Provide Help Desk Tier 1, Tier 2 and/or Tier 3 support for technical assistance, order processing, support of multiple software versions, training, warranty and maintenance, 24-hours a day, 7-days a week, 365 days a year.

- Tier 1 – Basic application software and/or hardware support.
- Tier 2 – More complex support on application software and/or hardware.
- Tier 3 – Usually subject matter experts, support on complex hardware and OS software issues.

[NOTE: Remove entire section if not applicable.]

3.5 Agent of the Certifying Authority (ACA) Support Services

ACA support services requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

The contractor shall provide support services for those customers seeking assistance in obtaining Information System Certification & Accreditation. Capabilities include both testing and validating functions of implemented IA controls, functions that may potentially overlap with existing IAM/IAO personnel functions assigned to Information Systems (ISs).

- ACA support **with** IAM/IAO functions seeking an authority independent of the program to perform both **testing** and **validating** of any existing IS security controls put in place by the IS developers. If mitigations to remaining IS vulnerabilities are required, the ACA possesses the necessary skills to recommend additional security controls for program personnel to implement so that the ACA could subsequently re-test and validate.

- ACA support **without** IAM/IAO functions seeking an authority independent of the program to perform **validation** of security controls implemented and tested by IAM/IAO personnel before the AF-CA can certify the IS for accreditation at the appropriate Designated Accrediting Authority (DAA).

[NOTE: Remove entire section if not applicable.]

3.6 [Next Requirement]

4. ENGINEERING REQUIREMENTS

4.1 Systems Engineering

[If applicable, insert additional MAJCOM or organization Business and Enterprise Systems (BES) Process Directory policy, requirements or guidelines. Include any special Process Directory instructions for Top Secret/TS SCI systems or applications. Tailor this section to applicable policies and practices for program office requirements.]

4.1.1 Life-Cycle Systems Engineering

[Keep this section unless organizational specific language is inserted.]

The contractor shall employ disciplined systems engineering processes including, but not limited to, requirements development, technical management and control, system/software design and architecture, integrated risk management, configuration management, data management and test, evaluation, verification and validation practices throughout the period of performance of TOs in accordance with AFI 63-1201, *Life Cycle Systems Engineering*.

4.1.2 Business and enterprise Systems (BES) Process Directory

If applicable, the contractor shall follow and refer to the Air Force Program Executive Office (AFPEO) Business Enterprise Systems (BES) Process Directory website https://acc.dau.mil/bes for common plans, procedures, checklists, forms and templates that support system life-cycle management and systems engineering processes as it applies to Defense Acquisition, Technology and Logistics tailored to Capability Maturity Model Integrated (CMMI) disciplines, or be able to demonstrate comparable processes and artifacts.

The contractor shall develop solutions that employ principles of open technology development and a modular open systems architecture for hardware and software as described in the DoD Open Technology Development Guidebook and Net-Centric Enterprise Solutions for Interoperability (NESI) body of knowledge. The contractor's systems engineering plan and design activities shall also adhere to the DoD Information Sharing and Net-Centric Strategies published by the DoD CIO, and the engineering body of knowledge and lessons-learned accumulated in NESI.

4.2 Architecture and System Design

[Tailor this section or provide additional considerations that will have an effect on the target date of deployment for systems or applications, particularly those that reflect current or target architectures and any test environments. These may include the dependencies the customer has outlined in the above Requirements, Section 3.]

The contractor shall support the design and development of systems and applications and their integration into the overarching enterprise architecture. The contractor shall provide all required design and development documents and supporting architectural documentation, for any frameworks as identified in this TO.

4.2.1 Department of Defense Architectural Framework (DoDAF) Guidance

The contractor shall provide all required design and development documents and supporting architectural documentation in compliance with the latest DoD Architectural Framework (DoDAF) Enterprise Architecture guidance http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf.

4.2.2 Global Combat Support System (GCSS) Developer's Guide

The contractor shall follow and comply with GCSS guidelines for developing systems and applications that will be deployed to the GCSS environment.

4.2.3 Capabilities Integration Environment (CIE)

The contractor shall make considerations for any development, integration and testing that needs to successfully complete the CIE process for information technology solutions and standardized DoD target infrastructures. The CIE provides a compliant capability with a set of enterprise services in support of proofs of concept, development, integration and test activities in an accredited environment.

4.2.4 DoD Mobility Strategy

For any systems or applications that have requirements for deployment on mobile technology, contractors shall follow and comply with the DoD Mobility Strategy.

4.2.5 Federal Desktop Core Configuration (FDCC)

All services provided under this TO shall function and be in compliance with the Federal Desktop Core Configuration (FDCC).

4.3 Configuration Management

The contractor shall accomplish Configuration Management (CM) activities as described in the TO. CM activities include baseline identification, change control, status accounting and auditing.

4.4 Testing

[If applicable, insert additional test requirements for Top Secret/TS SCI systems or applications.]

The contractor shall conduct rapid testing and deployment of Core Data Services and Aggregation and Presentation Layer Services using distributed testing environments. The contractor shall develop dynamic testing environments to support C&A and functional testing. The contractor shall perform testing of Top Secret and/or TS SCI systems and applications IAW standards, policies and guidelines identified in the TO.

4.4.1 Test Lab

When requested and specified in the TO, the contractor shall establish and maintain a system integrated test lab that is capable of supporting a full range of integration test activities for both the currently fielded system as well as maintenance/modernization releases. The currently fielded system includes the most current version and up to three previous versions for products that have not yet been declared ‘end of life.’ The contractor shall support test activities in areas which include, but are not limited to, product testing (regression testing and new capability testing), operational scenarios (real world simulation testing considering system topology and concept of operation, disaster recovery, clustering and load balancing), stress and longevity (throughput, speed of service and duration), interoperability, security (VPN, Firewall, security configuration of products and operating systems, and CAC Middleware testing), usability, transition (upgrade paths) and packaging/installation.

4.4.2 Regression Testing

The contractor shall establish and maintain a production environment that mirrors the operational environment in order to perform regression testing of the entire system for each upgrade or patch installed to ensure continuing functionality. The development environment shall include tools, test suites, support databases, a software test lab, configuration management, hardware spares, process and procedure documentation and delivered source code. If a test fails, the contractor shall analyze and document test data for each component and rework the system to establish functional equilibrium. Testing shall be performed in two steps: operational testing, then system acceptance testing and be performed IAW AFI 99-103, *Capabilities-Based Test and Evaluation*. The contractor shall provide a logical test process that minimizes interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing. The contractor shall develop scripts and conduct testing for the application, database and operating system IAW test plans.

4.4.3 Product/System Integration Testing

The contractor shall perform testing and inspections of all system services to ensure the technical adequacy and accuracy of all work, including reports and other documents required in support of that work. The contractor shall conduct on-site testing when requested. When specified by the government, the contractor shall participate with the government in testing the complete system or application which may include premise equipment, distribution systems or any additional telecommunications equipment or operating support systems identified in the TO. After appropriate corrective action has been taken, all tests including those previously completed related to the failed test and the corrective action shall be repeated and successfully completed prior to government acceptance. Pre-cutover audits will consist of verification of all testing completed by the contractor such that the system is deemed ready for functional cutover. As part of this audit, any engineered changes or approved waivers applicable to the installation will be reviewed and agreed upon between the contractor and the government. Post-cutover audits will verify that all post-cutover acceptance testing has been performed satisfactorily IAW the standard practices and identify those tests, if any, which have not been successfully completed and must be re-tested prior to acceptance. Testing shall be performed in two steps: operational testing, then system acceptance testing. The contractor shall provide a logical test process that minimizes interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing.

4.4.4 Simulated Operational Testing

The contractor shall conduct testing ranging from data entry and display at the user level combined with system loading to represent a fully operational system. The contractor shall accomplish operational testing IAW the government-approved test plan as specified in the TO. The plan shall consist of a program of tests, inspections and demonstrations to verify compliance with the requirements of this TO. The contractor shall document test results in the test report(s). The contractor shall furnish all test equipment and personnel required to conduct operational testing. During the installation/test phase, the government reserves the right to perform any of the contractor performed inspections and tests to assure solutions conform to prescribed requirements. The contractor shall be responsible for documenting deficiencies and tracking them until they are resolved. The government will not be expensed for correcting deficiencies that were the direct result of the contractor’s mistakes.

4.4.5 Acceptance Testing

The contractor shall provide on-site support during the acceptance-testing period. Acceptance testing shall be initiated upon acceptance of the operational test report and approval of the acceptance test plan. If a phased installation concept is approved in the Systems Installation Specification Plan (SISP), acceptance shall be based on the increments installed IAW the SISP. This on-site support shall be identified in the acceptance test plan.

4.4.6 System Performance Testing

[Establish system or application availability and performance parameters, thresholds and/or incentives.]

The contractor shall provide system performance testing. The acceptance test will end when the system or application has maintained the site-specific availability rate specified in this TO. In the event the system or application does not meet the availability rate, the acceptance testing shall continue on a day-by-day basis until the availability rate is met. In the event the system or application has not met the availability rate after 60 calendar days, the government reserves the right to require replacement of the component(s) adversely affecting the availability rate at no additional cost.

4.5 Cyber Security

[Modify Information Assurance requirements as they relate to a system or application.]

The contractor shall ensure that all system or application deliverables meet the requirements of DoD and AF Information Assurance (IA) policy. Furthermore, the contractor shall ensure that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications.

4.5.1 System IA

For those solutions that will not inherit existing network security controls, and thus integrate an entirely new application system consisting of a combination of hardware, firmware and software, system security assurance is required at all layers of the TCP/IP DoD Model.

The contractor shall ensure that all the requirements meet the DoD Cyber Security Risk Management Framework (RMF) and DoDI 8500.2, Intelligence Community Directive (ICD) 503, or the most current standards and guidance that are applicable. This includes Certification and Accreditation (C&A) activities. The contractor shall provide application services that are in compliance with and support DoD, USAF or IC Public Key Infrastructure (PKI) policies as applicable. The contractor shall support activities to make applications PK-enabled (PKE) in order to achieve standardized, PKI-supported capabilities for digital signatures, encryption, identification and authentication. The contractor shall assist in defining user and registration requirements to Local Registration Authorities (LRAs). The contractor shall provide solutions that meet confidentiality, data integrity, authentication and non-repudiation requirements. Contractor solutions shall comply with National Institute for Standards and technologies (NIST) and Federal Information Processing Standards (FIPS) and applicable IC standards.

As specified by the TO, the contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products IAW AFI 33-200, Cyber Security or other specified guidance. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Cyber Security Partnership (NCSP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP) or IC standards as applicable.

The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND), which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.5.2 Application Cyber Security

For those solutions that will be deployed to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments and thus inherit existing network security controls, application security assurance is required at the Application layer of the TCP/IP DoD Model.

The contractor shall provide security and information assurance support, protecting information and information systems, and ensuring confidentiality, integrity, authentication, availability and non- repudiation. The contractor shall provide application services support for C&A processes, RMF processes, SISSU processes, Enterprise Information Technology Data Repository (EITDR) certification or ICD 503.

IAW DFARS 239.7103(b), Information Assurance Contractor Training and Certification (JAN 2008):

(a) The contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating systems certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the government, the contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

4.5.3 Personnel Cyber Security

Personnel performing Cyber Security activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005 (with all current changes).

5. CONTRACTUAL REQUIREMENTS

[This section is here to capture all the requirements that do not logically fit or are not specifically covered in any of the other sections. Modify as needed to meet your requirement. This section may include such things as required physical security, emergency or special events, environmental or hazardous requirements, security requirements and specific training requirements. Modify each section IAW your requirements. Delete those that do not apply.]

5.1 Contractors Use of NETCENTS-2 Products Contract

The contractor shall obtain all products and associated peripheral equipment required of this TO from the NETCENTS-2 Products contract as stipulated in Section H Clause H098 of the ID/IQ contract.

5.2 Place of Performance

[The place of performance will be designated in each TO. Work shall be performed at either the customer (government) or contractor site. Travel to other government or contractor facilities may be required and will be specified in each TO. Exercise and deployment support will be identified in applicable TOs.]

5.3 Normal Hours of Operation

[Identify customer specific hours that are applicable to this TO, i.e., 7-4, 8-5, 24 x 7 x 365. Sample language is provided below.]

The average work week is 40 hours. The average workday is 8 hours and the window in which those 8 hours may be scheduled is between 6:00 AM and 6:00 PM, Monday through Friday or as specified in this TO, except for days listed in Clause G021, Contract Holidays, in the overarching ID/IQ contract. Billable hours are limited to the performance of services as defined in the TO. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Work in excess of the standard 40 hour work week requires prior written approval by the Quality Assurance Personnel (QAP).

5.4 Government Furnished Property

[Identify any Government Furnished Equipment (GFE) and/or Government Furnished Information (GFI) and any limitations that will be provided to the contractor. For GFE, provide serial numbers and all identifying information. Note, if GFE is a sizable list, indicate for example, "50 PC Pentium IVs" and state that serial numbers will be provided at TO award, along with location and delivery method. For GFI, list by document number and title, date, etc. Include standards, specifications and other reference material required to perform the TO. Include any facilities the government may need to provide to contractor personnel for project performance. Sample language is provided below.]

When this TO requires the contractor to work in a government facility, the government will furnish or make available working space, network access and equipment to include:

- Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
- Telephone (local/long distance calls authorized as dictated by TO performance requirements)
- Facsimile
- Copier
- Printer

Copies of required government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the TO will be provided to the contractor in hard copy or soft copy. All materials will remain the property of the government and will be returned to the responsible government QAP upon request or at the end of the TO period of performance.

Equipment purchased by the contractor with the approval of the government and directly charged to this TO shall be considered government owned-contractor operated equipment. The contractor shall conduct a joint inventory and turn in this equipment to the COR upon request or completion of the TO.

5.5 Billable Hours

[Modify as required for TO requirements. Sample language is provided below.]

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the TO PWS. In the course of business, situations may arise where government facilities may not be available for performance of the TO requirements (i.e., base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services will be provided and no charges will be incurred and/or billed to any TO. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as government employees. Participation in such events is not billable to the TO and contractor employee participation should be IAW the employees, company's policies and compensation system.

5.6 Non-Personal Services

[Modify as required for TO requirements. Sample language is provided below.]

The government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the contractor feels that any actions constitute or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the TO CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the government. These operating procedures may be superseded by Theater Commander's direction during deployments.

5.7 Contractor Identification

[Modify as required for TO requirements. Sample language is provided below.]

All contractor/subcontractor personnel shall be required to wear AF-approved or provided picture identification badges so as to distinguish themselves from government employees. When conversing with government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their government program customer should identify their work space area with their name and company affiliation. ***Refer to Clause H063 of the overarching ID/IQ contract.***

5.8 Performance Reporting

The contractor's TO performance will be monitored by the government and reported in Contractor Performance Assessment Reports (CPARs) or a Customer Survey, depending on the dollar amount of the TO. Performance standards shall include the contractor's ability to provide or satisfy the following:

- Provide satisfactory solutions to requirements with the necessary customer support.
- Provide solutions and services that meet or exceed specified performance parameters.
- Deliver timely and quality deliverables to include accurate reports and responsive proposals.
- Ensure solutions to requirements are in compliance with applicable policy and regulation.

5.9 Program Management/Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this TO, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to.

5.9.1 Services Delivery Summary

Reference Section 6,* Services Delivery Summary*, of this TO PWS for specific performance objectives.

The contractor's performance at the contract level will be assessed quarterly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary will be in accordance with AFI 63-101, Acquisition and Sustainment Life Cycle Management, AFI 10-601, Capabilities-Based Requirements Development and FAR Subpart 37.6, Performance-Based Acquisition.

5.9.2 TO Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/TO order manager who will oversee all aspects of the TO. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and solutions, support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature and continuously improving processes for administering all contract and TO efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high-quality delivery. The contractor shall provide transition plans as required.

5.9.3 Documentation and Data Management

The contractor shall establish, maintain and administer an integrated data management system for collection, control, publishing and delivery of all program documents. The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters and TO Proposals. The contractor shall provide the government with electronic access to this data, including access to printable reports.

5.9.4 Records, Files, and Documents

All physical records, files, documents and work papers provided and/or generated by the government and/or generated for the government in performance of this PWS, maintained by the contractor which are to be transferred or released to the government or successor contractor, shall become and remain government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the government or the contractor with respect to patents, data rights, copyrights or any other intellectual property or proprietary information as set forth in any other part of this PWS or the Application Services contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

5.9.5 Personnel Security

Individuals performing work under these TOs shall comply with applicable program security requirements as stated in the TO. NETCENTS-2 will support the following levels of security: Unclassified; Unclassified, But Sensitive; Secret (S); Secret Sensitive Compartmented Information (S/SCI); Top Secret (TS) and Top Secret Sensitive Compartmented Information (TS/SCI).

This TOs may require personnel security clearances up to and including Top Secret, and may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed TO. The TOs may also require access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the TO. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and TO level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The types of Personnel Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon requirements of the government and/or conditions of the TO. In cases where access to systems such as e-mail is a requirement of the government, application/cost for the PSI shall be the responsibility of the government. In cases where access to systems is as a condition of the TO, application/cost for the appropriate PSI shall be the responsibility of the contractor. In such instances, the contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active TO. Acquisition planning must consider Anti-Terrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in-transit forces), information systems and communications systems IAW DoD Instructions 2000.16 Anti-Terrorism Standards.

5.9.5.1 Transmission of Classified Material

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in this TO.

5.9.5.2 Protection of System Data

[Modify as required for TO requirements. Sample language is provided below.]

Unless otherwise stated in the TO, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation 5400.7-R and DoD Manual 5200.01(v1-v4) to include latest changes and applicable service/agency/combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by the contractor for these protections shall be DoD or IC approved PKI certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

5.9.5.3 System and Network Authorization Access Requests

[Modify as required for TO requirements. Sample language is provided below.]

For contractor personnel who require access to DoD, DISA or Air Force computing equipment or networks, the contractor shall have the employee, prime or subcontracted, sign and submit a System Authorization Access Report (SAAR), DD Form 2875.

5.9.6 Travel

The contractor shall coordinate specific travel arrangements with the individual CO or COR to obtain advance, written approval for the travel about to be conducted. The contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel in accordance with the basic contract clause H047.

If any travel arrangements cause additional costs to the TO that exceed those previously negotiated, written approval by CO is required prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use economy class or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid.

5.9.7 Other Direct Cost (ODC)

The contractor shall identify ODC and miscellaneous items as specified in each TO. No profit or fee will be added; however, DCAA approved burden rates are authorized.

5.10 Training

Contractor personnel are required to possess the skills necessary to support their company's minimum requirements of the labor category under which they are performing. Training necessary to meet minimum requirements will not be paid for by the government or charged to TOs by contractors.

5.10.1 Mission-Unique Training

In situations where the government organization being supported requires some unique level of support because of program/mission-unique needs, then the contractor may directly charge the TO on a cost reimbursable basis.   Unique training required for successful support must be specifically authorized by the TO CO.   Labor expenses and travel related expenses may be allowed to be billed on a cost reimbursement basis. Tuition/Registration/Book fees (costs) may also be recoverable on a cost reimbursable basis if specifically authorized by the TO CO.   The agency requiring the unique support must document the TO file with a signed memorandum that such contemplated labor, travel and costs to be reimbursed by the government are mission essential and in direct support of unique or special requirements to support the billing of such costs against the TO.

5.10.2 Other Government-Provided Training

The contractor's employees may participate in other government provided training, on a non-discriminatory basis as among contractors, under the following circumstances:

- The contractor employees' participation is on a space-available basis,
- The contractor employees' participation does not negatively impact performance of this TO,
- The government incurs no additional cost in providing the training due to the contractor employees' participation, and
- Man-hours spent due to the contractor employees' participation in such training are not invoiced to the TO.

5.11 Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017, the contractor shall disclose to the ordering CO and ordering office in any proposal for a TO, or after award of a TO if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the TO. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the TO and its CDRL requirements and any cost/price associated with delivery. This disclosure requirement also applies to segregable routines of non-commercial software that may be developed exclusively at government expense to integrate commercial software components or applications provided under a commercial software license or developed to enable commercial software to meet requirements of this TO. Performance of this disclosure requirement shall be considered a material performance requirement of any TO under which such technical data or non-commercial computer software is developed exclusively at government expense.

5.12 Software Support and Data Rights

Unless specified otherwise in the TO, the contractor shall fully support all unique software developed to support integrated solutions on this contract. The contractor shall be able to support all software revisions deployed or resident on the system and sub-systems. The data rights ownership/licensing guidance is specified in Section I, Clause 252.227-7013 and 252.227-7015 in the overarching contract section B, Defense Federal Acquisition Regulation Supplement Contract Clauses.

5.13 COTS Manuals and Supplemental Data

The contractor shall provide documentation for all systems services delivered under this TO. The contractor shall provide COTS manuals, supplemental data for COTS manuals and documentation IAW best commercial practices (i.e., CD-ROM, etc.). This documentation shall include users' manuals, operators' manuals, maintenance manuals, and network and application interfaces if specified in the TO.

5.14 Enterprise Software Initiative

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular TO, the contractor shall use available existing enterprise licenses. If enterprise licenses are unavailable, then products will be obtained via the DoD Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). If products are unavailable from ESI, then products will be acquired through the NETCENTS-2 Products contract. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at http://www.esi.mil.

5.15 Software License Management

If developing and/or sustaining a system that requires and/or contains COTS, the contractor shall provide maintenance and support of that software license to manage its relationship to the overall system life-cycle in accordance with AFMAN 33-153, Communications and Information, which would include applications, license agreements and software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment and configuration control, to include the procurement of supporting software licenses.

5.16 Transition and Decommissioning Plans

The contractor shall create transition and decommissioning plans that accommodate all of the non-authoritative data sources (non-ADS) interfaces and ensure that necessary capabilities are delivered using approved ADSs.

5.17 Section 508 of the Rehabilitation Act

The contractor shall meet the requirements of the Access Board's regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use information technology to access the information on an equal footing with people who do not have disabilities.

5.18 Continuation of Essential Contractor Services During Crisis Declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander

The performance of these services may be considered mission-essential functions during time of crisis. Should a crisis be declared by the Secretary of Defense, the CO or representative will verbally advise the contractor of the revised requirements, followed by written direction. When a crisis is declared, all services identified in this PWS are considered mission-essential functions during a crisis. The contractor shall continue providing service to the requesting organization 24-hours a day until the crisis is over. The contractor shall ensure enough skilled personnel are available during a crisis for any operational emergency. A crisis management plan shall be submitted IAW A-TE-3, A04, which states that the contractor shall "Submit an essential personnel list within 10 days after the contract start date." The list shall contain the employee's name, address, home phone number, beeper number (or cell phone number), social security number, security clearance and duty title. This list shall be updated annually or as changes occur. It must include the language spelled out in DFARS 237.76 – Continuation of Essential Contractor Services to identify services determined mission-essential functions during a crisis situation IAW DODI 1100.22. **Note: It is the responsibility of the Combatant Commander to determine mission-essential functions and to establish procedures to ensure that these standard support requirements and any additional requirements are met.**

5.19 Anthrax Information

[If applicable, include the following statement as part of this TO.]

"In accordance with the Air Force Anthrax Vaccine Immunization Program (AVIP), 18 Jan 2007, any Mission Essential contractor personnel performing work in the CENTCOM AOR or Korea for greater than 15 consecutive days are required to obtain the Anthrax vaccination."

5.20 Incentives

[Incentives should be used to encourage better quality performance and may be either positive, negative or a combination of both; however, they do not need to be present in every performance-based TO as an additional fee structure. In a fixed price TO, the incentives would be embodied in the pricing and the contractor could either maximize profit through effective performance or have payments reduced because of failure to meet the performance standard.

Positive Incentives - Actions to take if the work exceeds the standards.

Negative Incentives - Actions to take if work does not meet standards.

The definitions of standard performance, maximum positive and negative performance incentives, and the units of measurement should be documented here. They will vary from TO to TO and are subject to discussion during a source selection. It is necessary to balance value to the government and meaningful incentives to the contractor. Incentives should correlate with results. Follow-up is necessary to ensure that desired results are realized, i.e., ensuring that incentives actually encourage good performance and discourage unsatisfactory performance.]

6. SERVICES DELIVERY SUMMARY

[Modify to fit TO requirements. Make sure the services required have measurable outcomes.]

7. SECURITY REQUIREMENTS

[NOTE: Contact your local Security Office to determine which requirements may not be applicable to your TO, or which additional security requirements may need to be included. For the sake of readability of your PWS, it may be preferable to move this language to a separate document and include that document as an attachment to your RFP. It is recommended to include this language, as modified to meet TO requirements, in that attachment if your unit prefers to remove this section from the PWS itself.]

7.1 Security Facility Clearance Requirements

[Modify as required for TO requirements. Sample language is provided below.]

The contractor must possess or obtain an appropriate facility security clearance as identified below prior to performing work on a classified government contract: **(SELECT ONE)**

(   )   Top Secret

(   )   Secret

If the contractor does not possess a facility clearance the government will request one. The contractor shall notify the 42d Security Forces Squadron, Plans and Programs Flight, Information Protection (42 SFS/S5X/IP) before on-base performance of the service. The notification shall include:

a. Name, address and telephone number of company representatives;

b. The contract number and contracting agency;

c. The highest level of classified information which contractor employees require access to;

d. The location(s) of service performance and future performance, if known;

e. The date service performance begins;

f. Any change to information previously provided under this paragraph.

*** See Section 7.4 on how to complete this action***

7.2 Personnel Security Clearance Requirements

[Modify as required for TO requirements. Sample language is provided below.]

Some or all of the personnel performing work on this contract will require a security clearance as identified below: **(SELECT ONE)**

( ) Top Secret

( ) Secret

The contractor shall request security clearances for personnel requiring access to classified information within 15 business days after receiving a facility clearance or, if the contractor is already cleared, within 15 business days after service award. Due to costs involved with security investigations, contractor security clearances shall be kept to an absolute minimum necessary to perform service requirements.

7.2.1. Additional Investigation Requirements

Anyone working on the contract that does not require a security clearance must have at a minimum a favorably adjudicated National Agency Check with Written Inquiries (NACI) investigation to access a government furnished information system or environment. This investigation must be submitted by the contract company. Note: AFI 31-501, and AFI 31-601 for unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/or sensitive equipment.

7.3 Security Manager Appointment

[Modify as required for TO requirements. Sample language is provided below.]

The contractor shall appoint a security manager for the on base long-term visitor group. The security manager may be a full-time position or an additional duty position. The security manager shall provide contractor employees with training required by DoDM 5200.01, Volume

3, Enclosure 5, *DoD Information Security Program*, AFPD 31-4, *Information Security* and AFI 16-1404, *Air Force Information Security Program*. The contractor security manager shall provide initial and follow-on training to contractor personnel who work in Air Force controlled or restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101, *Air Force Integrated Defense Plan*.

7.4 Visit Requests

Contractors participating in the National Industrial Security Program are authorized to use Joint Personnel Adjudication System (JPAS) in lieu of sending Visitor Authorization Letters (VALs) for classified visit to DoD facilities and military installations. VALs are only required if the contractor isn't using JPAS or if contractor personnel whom access level and affiliation are not accurately reflected in JPAS. However, some agencies may still require VALs to be submitted for access to their facilities. Visit requests must be sent to servicing government's security management office (SMO) code. The SMO code for AFLCMC Des is MG1MFD3Q6. Each contractor performing work on the contract will require a separate SMO Code visit request from the contactor. The visit request must include all prime and subcontract workers on the contract.

7.5 Obtaining and Retrieving Identification Media

As prescribed by the AFFAR 5352.242-9000 Contractor Access to Air Force Installations, AFFAR 5352.242-9001, Common Access Cards (CAC) for Contractor Personnel and FAR 52.204-9, Personal Identity Verification of Contractor Personnel, the contractor must comply with the requirements set forth in these guidance. Contractors requesting a CAC for personnel on the contract will submit on company letterhead the names and all other personnel information as prescribed by the CO to begin the identification processing effort. COs will follow installation specific guidance regarding the issuance and recovery of all identification media issued to the contractors by the government. Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

7.6 Pass and Identification Items

[Modify as required for TO requirements. Sample language is provided below.

NOTE: Contact your local Security Office to determine the appropriate identification for this TO.]

The contractor shall ensure the following identification items as required for contract performance are obtained for employees:

- DoD Common Access Card (AFI 36-3026).
- Base-specific identification as required by local base and/or building security policies.

Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

7.7 Visitor Group Security Agreement (VGSA)

[Modify as required for TO requirements. Sample language is provided below.]

The contractor shall enter into a long-term visitor group security agreement for contract performance on base. This agreement shall outline how the contractor integrates security requirements for contract operations with the Air Force to ensure effective and economical operation on the installation. The agreement shall include:

a. Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, *Industrial Security Regulation,* Air Force Policy Directive 31-6, *Industrial Security,* Air Force Instruction 31-601, *Industrial Security Program Management,* DoDM 5200.01, Volumes 1-4, *DoD Information Security Program,* and AFI 16-1404, *Air Force Information Security Program.*

b. Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

c. On base, the long-term visitor group security agreement may take the place of a *Standard Practice Procedure* (SPP).

7.8 Information Security

The contractors performing duties associated with this TO must adhere to all the standards for protecting classified information as specified in DoDM 5200.01, Volumes 1-4, *DoD Information Security Program*, Air Force Instruction 16-1404, *Air Force Information Security Program* and all applicable supplements and operating instructions.

7.9 Unescorted Entry to Secure Rooms

[Modify as required for TO requirements. Sample language is provided below.]

Contractor personnel requiring unescorted entry to secure rooms designated by the installation commander shall comply with base access requirements and these additional security instructions; DoD 5200.2-R, *DoD Personnel Security Program,* AFI 31-101, *Air Force Integrated Defense Plan* and AFI 31-501, *Personnel Security Program Management* as applicable. Contractor personnel shall be the subject of a favorably adjudicated National Agency Check with Local Agency Check (NACLC) investigation to qualify for unescorted entry to a secure room. Contractor personnel must contact their COR and the appropriate secure room monitor for permission.

7.10 Computer and Network Access Requirements

[Modify as required for TO requirements. Sample language is provided below.]

Contractor personnel working on this contract must be designated in one of the below AIS positions and complete the required security investigation to obtain the required security clearance. This must be accomplished before operating ***government furnished*** computer workstations or systems that have access to ***Air Force*** e-mail systems or computer systems that access classified information. The contractor shall comply with the DoD 5200.2-R, *Personnel Security Program* and AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, requirements. **(Please check one):**

(   )   AIS-II Position - Noncritical-Sensitive Positions. Security Clearance: SECRET based on a NACLC/ANACI background investigation. Responsibility for systems design, operation, testing, maintenance and/or monitoring that is carried out under technical review of higher authority in the AIS-I category, includes, but is not limited to; access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 18 1974 and government-developed privileged information involving the award of contracts.

(   )   AIS-III Position - Nonsensitive Positions. No security clearance required but is a **Trusted Position** based on a favorable NACI background investigation. All other positions involved in U.S. government computer activities.

7.11 Reporting Requirements

The contractor shall comply with requirements from AFI 71-101, Volume-1 and *Criminal Investigations,* and Volume-2 *Protective Service Matters*. Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware may pose a threat to the security of DoD personnel, contractor personnel, resources and classified or unclassified defense information. Contractor employees shall be briefed by their immediate supervisor upon initial on-base assignment and as required thereafter.

7.12 Physical Security

Contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and Operation Security (OPSEC), Emergency Management (EM) and local search/identification requirements. The contractor shall safeguard all government property including controlled forms provided for contractor use. At the close of each work period, government training equipment, facilities, support equipment and other valuable materials shall be secured.

7.13 Wireless Electronic Devices

[Modify as required for TO requirements. Sample language is provided below.]

The following devices are not allowed in areas where classified information is discussed, briefed or processed: cell phones, camera cell phones, cordless telephones, wireless microphones, wireless keyboards, wireless mice, wireless or Infrared Local Area Networks (LANs). The term

"Area" above refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed or processed, wireless pointer/mice devices are allowed for presentations only. This is an acceptable EMSEC risk. All other Personal Electronic Devices (PEDs). All other wireless PEDs not specifically addressed above, that are used for storing and processing and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed or transmitted.

7.14 Operating Instructions

[Modify as required for TO requirements. Sample language is provided below.]

The contractor will adhere to the all Air Force activity Operating Instructions (OIs) and local Security Program Management for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations to include local written OIs.

7.15 Government Authorization

The contractor shall ensure its employees do not allow government issued keys to be used by personnel other than current authorized contractor employees. Contractor employees shall not use keys to open work areas for personnel other than contractor employees engaged in performance of duties, unless authorized by the government functional director.

7.16 Access Lock Combinations

Access lock combinations are "*For Official Use Only"* and will be protected from disclosure to unauthorized personnel. The contractor will adhere to the Air Force activity operating instructions ensuring lock combinations are not revealed to un-cleared /unauthorized persons and ensure the safeguard procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional director.

7.17 Security Combinations

Combinations to security containers, secure rooms or vaults are classified information and must be properly safeguarded. Only contractor employees, who have the proper security clearance and the need-to-know, will be given combinations to security containers, secure rooms or vaults. Contractor employees are responsible for properly safeguarding combinations. Contractor employees will not record security containers, secure rooms or vaults combinations without written approval by the government functional director. Contractors will not change combinations to security containers, secure rooms or vaults without written approval by the security officer and the government functional director.

7.18 Security Alarm Access Codes

Security alarm access codes are "*For Official Use Only*" and will be protected from unauthorized personnel. Security alarm access codes will be given to contractors employees who require entry into areas with security alarms. Contractor employees will adhere to the Air Force activity operating instructions and will properly safeguard alarm access codes to prevent unauthorized disclosure. Contractors will not record alarm access codes without written approval by the government functional director.

7.19 Freedom of Information Act Program (FOIA*)*

The contractor shall comply with DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program,* requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting and safeguarding for *Official Use Only (FOUO)* material. The contractor shall comply with AFI 33-332, *Air Force Privacy Act Program*, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall maintain records in accordance with Air Force manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/.

7.20 Traffic Laws

[Modify as required for TO requirements. Sample language is provided below.]

The contractor and their employees shall comply with all installation traffic regulations.

7.21 Cellular Phone Operation Policy

The contractor shall comply with local base policies regarding cellular phone operation.

7.22 Security Education and Training

[Modify as required for TO requirements. Sample language is provided below.]

The contractors are required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system. Annually, all contractors will complete all required security training. Required annual training includes Force Protection (FP), Information Protection (IP), Cybersecurity and OPSEC. If contract team members will be using the SIPRNet, users will also have to comply with the organizational Derivative Classification Training as a condition of access.

8. DATA DELIVERABLES

[Define deliverables required for individual TOs. This section contains information on data requirements, such as reports or any of those items contained within a CDRL. Strive to minimize data requirements that require government approval and delivery. Only acquire data that are absolutely necessary. The usual rule of thumb is to limit data to those needed by the government to make a decision or to comply with a higher level requirement. Deliverables should relate directly to the Services Delivery Summary in Section 6. Detailed CDRL requirements and formats should be provided IAW DFAR 204.7105 on DD Form 1423-1, FEB 2001. Note, the number and complexity of required

Deliverables need to correlate to the size and complexity of requirements contained in the TO.]

The government reserves the right to review all data deliverables for a period of 10 working days prior to acceptance. No data deliverable will be assumed to be accepted by the government until the 10-day period has passed, unless the government explicitly states otherwise in the TO.

The government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers and other data for which the government shall treat as deliverable.

9. APPLICABLE STANDARDS AND REFERENCES

For applicable certifications, specifications, standards, policies and procedures that are required for compliance on individual TOs, refer to Application Services Standards on the Application Services Documents Page on our website. Tailor the list as needed for individual TO, may impose additional standards to those required at the contract level. The list is not all-inclusive and the most current version of the document at the time of TO issuance will take precedence. Web links are provided wherever possible.]

10. PRODUCTS STANDARDS AND COMPLIANCE REQUIREMENTS

[If your effort will be requiring the vendor to provide IT Products to meet your requirements then ensure you have selected the applicable IT Product standards and compliance areas from section 10.1-10.18 below. If your effort will not require IT Products then delete section 10.]

10.1 Information Assurance (IA) Technical Considerations

The contractor shall provide COTS IA and IA-enabled products IAW AFI 33-200, Air Force Cybersecurity Program Management. These products must be Committee on National Systems Security Policy Number 11 (CNSSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or NIST FIPS Cryptographic Module Validation Program (CMVP). The following are some examples of IA and IA enabled devices: data/network encryptors, intrusion detection devices such as Firewalls, Intrusion Detection System, Authentication Servers, Security Gateways, High Assurance IP encryptor and Virtual Private Networks.

10.2 DoD IPV6 Requirement

All Products must meet the criteria in DoD IPv6 Standard Profiles for IPv6 Capable Products version 5.0 July 2010 (http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf). Some example IPV6 mandated products from the DoD IPV6 Standards Profile are listed below:

- Host/Workstations - a desktop or other end-user computer or workstations running a general purpose operating system such as UNIX, Linux, Windows or a proprietary operations system that is capable of supporting multiple applications.

- Network Appliance or Simple Server - Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A Simple Server supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)11 servers, a “web camera” appliance that serves pictures via an embedded web server and a network time server appliance that solely functions to serve NTP requests. Advanced Server - End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network.

- Intermediate Nodes – routers, switches, IA or IA enabled devices.

- IPV6 Capable Software - a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform.

10.3 Energy Star

All applicable Products must be EnergyStar® compliant per DoDI 4170.11 and FAR Part 52.223-153.

ENERGY EFFICIENCY IN ENERGY-CONSUMING PRODUCTS (DEC 2007)

(a) Definition: As used in this clause, "Energy-efficient product"…

(1) Means a product that—

(i) Meets Department of Energy and Environmental Protection Agency criteria for use of the Energy Star® trademark label; or

(ii) Is in the upper 25 percent of efficiency for all similar products as designated by the Department of Energy's Federal Energy Management Program.

(2) The term "product" does not include any energy-consuming product or system designed or procured for combat or combat-related missions (42 U.S.C. 8259b).

(b) The Contractor shall ensure that energy-consuming products are energy efficient products i.e., ENERGY STAR products or FEMP-designated products) at the time of contract award, for products that are—

(1) Delivered;

(2) Acquired by the Contractor for use in performing services at a Federally-controlled facility;

(3) Furnished by the Contractor for use by the Government; or

(4) Specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance.

(c) The requirements of paragraph (b) apply to the Contractor (including any subcontractor) unless—

(1) The energy-consuming product is not listed in the ENERGY STAR Program or FEMP; or

(2) Otherwise approved in writing by the Contracting Officer.

(d) Information about these products is available for—

(1) ENERGY STAR at http://www.energystar.gov/products; and

(2) FEMP at www.femp.energy.gov/technologies/eep_purchasingspecs.html.

NOTE: Remove if not applicable. The following are some example products that are required to be energy star compliant: computers, displays and monitors, enterprise servers, copiers, digital duplicators, fax/printer machines, printers, scanners, televisions, cordless phones, battery chargers, set-top and cable boxes and audio and video equipment. For further guidance please see the below URL: http://www1.eere.energy.gov/femp/technologies/eep purchasingspecs.html.

10.4 Encryption Mandates

All Products that will perform any type of data encryption, it is required that the encryption method being used meets FIPS standards for both information assurance and interoperability testing. For more information on FIPS, go to: http://www.itl.nist.gov/fipspubs/by-num.htm. Some examples of FIPS standards would be FIPS 201 which specifies the architecture and technical requirements for a common identifications standard for Federal employees and contractors (i.e., CAC). Another one is FIPS 140-2 which specifies the security requirements that will be satisfied by a cryptographic module (i.e., the underlying algorithms to process information).

10.5 BIOS Mandate

All Products shall be BIOS protection compliant with Section 3.1 “Security Guidelines for System BIOS Implementations of SP 800-147,” per DoD CIO, in order to prevent the unauthorized modification of BIOS firmware on computer systems.

10.6 Biometric Mandate

All Biometric products shall be built to the DoD Electronic Biometric Transmission Specification (EBTS) version 3.0 standard.   For more information please visit the Biometric Identity Management Agency website at: http://www.biometrics.dod.mil/.

10.7 Special Asset Tagging

The contractor shall provide special asset tags IAW DODI 8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property, to Include Unique Identification (UID) tagging requested by non-DoD customers. NOTE: Remove if not applicable. If the following criteria apply then leave the above statement in your PWS. All items for which the government's unit acquisition cost is $5,000 or more:

- Items for which the government's unit acquisition cost is less than $5,000, when identified by the requiring activity as DoD serially managed, mission essential or controlled inventory;

- When the government's unit acquisition cost is less than $5,000 and the requiring activity determines that permanent identification is required;

- Regardless of value, (a) any DoD serially managed subassembly, component or part embedded within an item and, (b) the parent item that contains the embedded subassembly, component or part.

If you require further guidance on Special Asset Tagging please see DoDI 8320.04 at: http://www.dtic.mil/whs/directives/corres/pdf/832004p.pdf.

10.8 Software Tagging

COTS software items shall support International Standard for Software Tagging and Identification, ISO/IEC 19770-2, Software Tags when designated as mandatory by the standard. NOTE: Check ISO/IEC 19770-2 to see if Software Tagging applies to this acquisition. Some examples of when you might require software tagging would be if you needed to record unique information about an installed software application or to support software inventory and asset management. For more information please go to: http://tagvault.org/.

10.9 Radio Frequency Identification (RFID)

The contractor shall provide RFID tagging IAW DoD Radio Frequency Identification (RFID) Policy, 30 July 2004 or most current version. NOTE: Check RFID Policy, 30 July 2004 at: https://acc.dau.mil/adl/en- S/142796/file/27748/ RFIDPolicy07-30-2004.pdf to see if Special Asset Tagging applies to this acquisition. Some example uses of RFID are when tags are placed into freights containers, ammunition shipments or attached to unit level IT equipment to facilitate accountability.

10.10 Hardware and Associated Software and Peripherals

All hardware delivered under this delivery order (DO) shall include associated software, documentation and associated peripherals required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the Original Equipment Manufacturer (OEM). This is true only if the applicable OEM provides such items with the product itself.

10.11 Authorized Resellers

The contractor may be an authorized reseller of new and refurbished/remanufactured equipment for OEMs proposed under this DO. The contractor may also procure directly from the OEM or utilize other legitimate distribution channels to provide the required products. Any contractor's channel relationships with their OEM partners (gold, silver, etc.) will be represented in the best pricing offered. DOs may restrict the use of authorized resellers, specific OEMs or identify required OEMs. Any product offering that is remanufactured or refurbished shall be clearly identified as such by the contractor. Remanufactured products shall have the OEM or factory certification if available for that product.

10.12 Technical Refresh

In order to ensure new design enhancements and technological updates or advances, the contractor shall offer, under this DO, hardware and software components available to the contractor's commercial customers. Furthermore, the contractor shall make available any commercially available updates to the hardware and software provided under this DO. If such updates are available to other customers without charge, then they shall also be made available to the government without additional charge. The contractor will ship these updates to existing customers who have acquired the hardware/software being updated under this DO. Vendor commercial product offerings shall include "state of the art" technology, i.e., the most current proven level of development available in each product category.

10.13 Trade Agreement Act (TAA)

All proposed products offered in response to any RFQ issued under this contract must be compliant with the Trade Agreements Act of 1979 (TAA) and related clauses in Section I of this contract. In accordance with DFARS 252.225-7021, the Trade Agreements Certificate at DFARS 252.225-7020 shall be provided for each end item defined and specified in a solicitation subject to the waivers and exceptions provided in FAR 25.4 and DFARS 225.4. Please note that Federal Acquisition Regulation (FAR) paragraph 25.103(e) includes an exemption from the Buy American Act (BAA) for acquisition of information technology that are commercial items.

10.14 Items on Backorder

In their response to a RFQ, the contractor shall provide notification, if applicable, that a particular item is on backorder, the expected lead-time to fulfill the order, etc. It shall be implicit that a response to an RFQ with no items identified on backorder is a declaration that the items are available at the time of quote submission.

10.15 Installation

The only time installation services can be procured are when the services and cost are included in the price of the product as sold commercially. In the rare instances where installation services are required, the contractor shall provide installation support related to the applicable products(s) as defined in the DO. In those instances, the DD Form 254 (DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION) requirements will be addressed in the individual DO and only at the security level necessary.

10.16 Warranty

The contractor shall provide any OEM pass through warranty and standard commercial warranties applicable to the products being purchased at no cost. This shall apply to new, refurbished and remanufactured equipment.

10.17 Customer Support

The prime contractor shall provide 24x7 live telephone support during the warranty period to assist in isolating, identifying and repairing software and hardware failures, or to act as liaison with the manufacturer in the event that the customer requires assistance in contacting or dealing with the manufacturer.

10.18 Product Maintenance

The contractor shall provide associated maintenance and upgrades to include spares/parts and emergency support worldwide, during the warranty period.

Appendix A3 – AMRDEC SAFE ACCESS FILE EXCHANGE (SAFE)

Go to: NETCENTS-2 Application Services Support Documents on this website
http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp

Appendix A4 – NETCENTS-2 RSS Feed Instructions

Go to: NETCENTS-2 Application Services Support Documents on this website
http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp