2016

Network Operations and Infrastructure Solutions

NETCENTS-2

Version 2.3

24 July 2018

Table of Contents

Summary of Changes

Version	Date	Author	Notes
1.0	05 Nov 2013	T. Porterfield	Initial Draft
1.1	06 Aug 2014	T. Porterfield	Initial Draft
1.2	28 Apr 2015	J. Frye	Redesigned Document
1.3	1 May 2015	J. Frye	Minor Updates, Returned N7
1.4	12 May 2015	J. Frye	Updates from Randi Williams and Kelly Bryant, corrected Standards table
1.5	14 May 15	J. Frye, R. Williams	Updates from Group Session on 13 May 15
2.0	12 August 15	SJA, J. Frye, K. Mitchell	Incorporating Legal/Policy Comments, Questions and Suggestions.
2.0.1	17 August 2015	G. Smothers, J. Frye	Removed Products Standards from NetOps PWS Template, incorporated minor edits from NC-2 PM
2.2	13 October 2016	J. Williams	Removed Standards Table from User's Guide, updated language in both Section 8 (Quality Processes) and Section 5 (Quality Processes) of the PWS Template inside of User's Guide. Also removed Change Page from document.
2.3	24 July 2018	J. Williams	Updated NAICS Code for Netops. Changed from 517110 to 517311

Network Operations (NetOps) and Infrastructure Solutions for Full and Open and Small Business

1. Scope

The Network Operations (NetOps) and Infrastructure contracts will provide a wide range of Information Technology (IT) Network-centric and Telephony products, services and solutions covering the full spectrum of NetCentric operations and missions, including existing legacy infrastructure, networks, systems and operations as well as emerging requirements based on the Air Force (AF) Chief Information Officer's (CIO) Service Oriented Architecture (SOA) construct. The contracts will provide Network-Centric Information Technology, Networking, and Security, Voice, Video and Data Communications, system solutions and services to satisfy worldwide requirements for Combat Support (CS), Command and Control (C2), and Intelligence Reconnaissance and Surveillance (ISR). These contracts provide capabilities to find, access, collaborate, fuse, display, manage, and store information on the DoD Global Information Grid (GIG). Requirements may include commercial-off-the-shelf (COTS) hardware and software, National Security Systems (NSS), intelligence data handling equipment, C2 equipment, Local Area Networks (LAN), Wide Area Networks (WAN), secure and non-secure video, voice and data systems, and mission equipment. The equipment processes information of varying security classifications and may include sites with Sensitive Compartmented Information Facilities (SCIFs).

For work that clearly falls within the scope of this contract, ordering Contracting Officers (CO) 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 falls within the scope of this Indefinite Delivery/Indefinite Quantity (ID/IQ) contract, the CO should do a scope determination and place it under the appropriate tab in the task order contract file. For scope analysis assistance from the NETCENTS-2 team, please send the draft PWS to the NETCENTS-2 Team at netcents@us.af.mil. Put "Scope Analysis Request" in the Subject line.

NOTE: Please read the ID/IQ contract Network Operations and Infrastructure Solutions Performance Work Statement (PWS) for an overview of the contract scope.

2. Authorized Users

The NetOps and Infrastructure Full & Open and Small Business contracts are open to Air Force Enterprise, DoD and all Federal Agencies.

NOTE: 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

Authorized users with in scope requirements should first complete Appendix N1 – The NetOps and Infrastructure Solutions Task Order Requirement Package Checklist. This checklist facilitates development of a complete requirements package.

Submit the required documents referenced in Appendix N1, to your local CO for final approval. The Table of Contents above includes links to these documents.

3.1 Full & Open vs. Small Business Companion

The NetOps and Infrastructure Solutions includes both full and open and small business ID/IQ contracts. "Companion Contracts" for small business concerns share the same scope of coverage as the full and open contracts. **Please refer to Clause H137(5) for applicable procedures when determining which set of contracts to compete task order RFPs. The CO is responsible for preparing a DD Form 2579 for each task order to screen requirements for those suitable for solicitation among the companion contract holders. Ordering CO should coordinate completion of the DD 2579 with their local Small Business Specialists.**

This guide provides relevant information for both sets of contracts. The guide distinguishes between the two vehicles where information applies only to the full and open or the companion contracts.

3.2 Decentralized Ordering

The NETCENTS-2 NetOps and Infrastructure Solutions ID/IQ contracts employ a decentralized ordering structure. Each local contracting office supporting the awarded requirements shall administer and close each task order. See Clause G019 (h) of the basic ID/IQ contract

All decentralized orders placed by the DoD and other Federal Agencies must be assigned a NETCENTS-2 PMO control Number. The NETCENTS-2 PMO control number is a Request for Proposals/Request for Quotes (RFP/RFQ) number generated in AFWay when the Customer or CO has successfully submitted a RFP/RFQ to the NetOps & Infrastructure Solutions vendors. This number is used for tracking purposes during the entire task order procurement process. For in depth instruction on how to submit a RFP/RFQ in AFWay, refer to the following paragraph or consult Appendix N4, Customer Ordering Guide Using AFWay.

3.3 Solicitation Provisions and Contract Clauses

Task Order RFPs must include provisions and clauses specific to that TO. Examples include option evaluation or exercise clauses, base-specific Wide Area Workflow (WAWF) instructions, handling and recording of government furnished property, and appropriate tax clauses for OCONUS performance.

3.4 Fair Opportunity Exception (FOE)

The acquisition process for obtaining Task Orders through NETCENTS-2 contracts enables different solution providers to participate over the course of the program lifecycle to facilitate competition. The CO will provide contractors a "fair opportunity" to be considered for each order in excess of the Micro-Purchase Threshold unless an exception applies. **See FAR 16.505(b)(2) and Clause H137(6)(c) of the ID/IQ contract for applicable exceptions to the fair opportunity process.**

3.5 AFWay – NETCENTS-2 e-Ordering Tool

Once the requirements package is complete, submit to the NetOps vendors through AFWay, the e-Ordering tool for all NETCENTS-2 ID/IQ contracts. The CO shall initiate and process a RFP (referred to as an "RFQ" in AFWay), and receive vendor responses to the RFP through AFWay. After evaluating vendors' solutions and selecting the awardee the CO should then complete the process by awarding the order in AFWay. See Appendix N4, Customer Ordering Guide Using AFWay.

3.6 Requests for Information (RFI)

Submit any RFI (also referred to as an "RFQ" in AFWay) through AFWay. An RFI should provide vendors sufficient insight into the requirements to permit them to adequately describe relevant capabilities beyond those identified in the overarching contract PWS. This allows the vendors to better address the customer's requirements and reduces the incidence of higher proposed pricing to cover the assumption of risk for insufficiently defined work. To maximize vendor participation follow the same process for RFIs as for RFPs, i.e. submit through AFWay to vendors. Refer to Appendix N4 for the process of submitting an RFP/RFI in AFWay. 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 for documentation. Directions for the use of SAFE can be found in Appendix N5.**

3.7 Classified Task Order Procurement

Customers with CLASSIFIED requirements may 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 Contracting Officer 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 task order.

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

3.8 Task Orders Requiring Hardware/Software Products

Task Orders that require hardware or software products shall be purchased by the NetOps vendors from the Products vendors. Customers should carefully review the PWS template in Appendix N2, and ensure applicable products standards accompany the solicitation to ensure compatibility and compliance with AF network standards. Vendors are required to include a minimum of two quotes with each proposal.

4. Task Orders Period of Performance (PoP)

Task Orders may be issued at any time during the ordering period. The performance period for each task order shall be cited in each individual order and may extend beyond the expiration date of this ID/IQ contract. **See Clause F002 of the basic ID/IQ contract.**

The total duration of any task orders issued under this basic contract shall not exceed five (5) years, including all option periods. The period of performance for any task order shall not extend more than three (3) years beyond the last day of the basic contract ordering period (e.g. a task order issued on the last day of the ordering period of the basic contract could have a one (1) year base period and two (2) one (1) year option periods).

4.1 Full & Open

SB Base Period: May 15, 2015 – May 14, 2018
*Option Period One: May 15, 2018 – May 14, 2019
*Option Period Two: May 15, 2019 – May 14, 2020
*Option Period Three: May 15, 2020 – May 14, 2021
*Option Period Four: May 15, 2021 – May 14, 2022

4.2 Small Business Companion

SB Base Period: April 2, 2015 – April 1, 2018
*Option Period One: April 2, 2018 – April 1, 2019
*Option Period Two: April 2, 2019 – April 1, 2020
*Option Period Three: April 2, 2020 – April 1, 2021
*Option Period Four: April 2, 2021 – April 1, 2022

5. Prime Contractors

5.1 Full & Open

Contractor Name	Contract #
URS Federal Services, Inc.	FA8732-15-D-0030
AT&T Government Solutions, Inc.	FA8732-15-D-0031
BAE Systems Information Solutions, Inc.	FA8732-15-D-0033
Booz Allen Hamilton Inc.	FA8732-15-D-0034
Nextiraone Federal, LLC	FA8732-15-D-0035
Computer Sciences Corporation	FA8732-15-D-0036
Federal Network Systems LLC	FA8732-15-D-0037
General Dynamics Information Technology, Inc.	FA8732-15-D-0038
Harris IT Services Corporation	FA8732-15-D-0039
HP Enterprise Services, LLC	FA8732-15-D-0040
International Business Machines Corporation	FA8732-15-D-0041
LGS Innovations LLC	FA8732-15-D-0042
Lockheed Martin Corporation	FA8732-15-D-0043
L-3 National Security Solutions, Inc.	FA8732-15-D-0044
NCI Information Systems, Inc.	FA8732-15-D-0045
Northrop Grumman Systems Corporation	FA8732-15-D-0046
Raytheon Company	FA8732-15-D-0047
Science Applications International Corporation	FA8732-15-D-0048
SRA International, Inc.	FA8732-15-D-0049
Telos Corporation	FA8732-15-D-0050

5.2 Small Business

Contractor Name	Contract #
The Centech Group Inc.	FA8732-14-D-0010
Epsilon Systems Solutions Inc.	FA8732-14-D-0011
Smartronix Inc.	FA8732-14-D-0012
SMS Data Products Group Inc.	FA8732-14-D-0013
Indus Corp.	FA8732-14-D-0014
Technica Corp.	FA8732-14-D-0015
Telos Corp.	FA8732-14-D-0016
Sumaria Systems Inc.	FA8732-14-D-0017
BTAS Inc.	FA8732-14-D-0018
American Systems Corp.	FA8732-14-D-0019
STG, Inc.	FA8732-14-D-0020
MicroTechnologies LLC	FA8732-14-D-0021
Abacus Technology Corporation	FA8732-15-D-0022
Atlantic CommTech Corporation	FA8732-15-D-0023
CDO Technologies, Inc.	FA8732-15-D-0024
EPS Corporation	FA8732-15-D-0025
Intelligent Decisions, Inc.	FA8732-15-D-0026

6. Contract Line Item Numbering (CLIN) Structure

CLINs 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 NetOps and Infrastructure Solutions SB CLIN structure. For example, all requirements using CLIN 0010 shall contain a "0" in the first digit and a "1" in the third digit and maintain the contract type, Fixed Price, and all requirements using CLIN 0020 shall contain a "0" 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: 0030, 0040, 0050, 0060, and 0070.

6.1 CLIN / Pricing 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 Services	Firm Fixed Price (FFP)
0200	1200	2200	3200	4200	Network Centric Services	Cost

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
0300	1300	2300	3300	4300	Network Centric Services	Labor Hour (LH)
0400	1400	2400	3400	4400	Data	Firm Fixed Price (FFP)
0500	1500	2500	3500	4500	Warranty	Firm Fixed Price (FFP)
0600	1600	2600	3600	4600	Other Direct Costs (ODC)	Cost
0700	1700	2700	3700	4700	Travel	Cost

6.2 CLIN / Pricing Structure Small Business

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 Services	Firm Fixed Price (FFP)
0020	1020	2020	3020	4020	Network Centric Services	Cost
0030	1030	2030	3030	4030	Network Centric Services	Labor Hour (LH)
0040	1040	2040	3040	4040	Data	Firm Fixed Price (FFP)
0050	1050	2050	3050	4050	Warranty	Firm Fixed Price (FFP)
0060	1060	2060	3060	4060	Other Direct Costs (ODC)	Cost
0070	1070	2070	3070	4070	Travel	Cost
0080		2080 **2085	3080 **3085		Post Award Conference & SB 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 NetOps and Infrastructure Solutions. This 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 the ID/IQ contract.

Any task order issued during the ID/IQ Base Period must use the Base Period CLIN Structure. Once an Option Period has been *exercised*, any task order 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 IDIQ contract.

Each number identified in the CLIN represents a specific element of the IDIQ contract. For example, the base year period CLIN 0010 is broken down into four (4) distinct components:

- The first digit represents the Ordering Period of the IDIQ

- 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 0010 - NETCENTRIC Total Solution - Base Year
CLIN 0011 - NETCENTRIC Total Solution - Option Year One
CLIN 0012 - NETCENTRIC Total Solution - Option Year Two
CLIN 0013 - NETCENTRIC Total Solution - Option Year Three
CLIN 0014 - NETCENTRIC Total Solution - Option Year Four

OR,

CLIN 0010 - NETCENTRIC Total Solution
Sub-CLIN 0010AA - NETCENTRIC Total Solution - Base Year
Sub-CLIN 0010AB - NETCENTRIC Total Solution - Option Year One
Sub-CLIN 0010AC - NETCENTRIC Total Solution - Option Year Two
Sub-CLIN 0010AD - NETCENTRIC Total Solution - Option Year Three
Sub-CLIN 0010AE - NETCENTRIC Total Solution - Option Year Four

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

CLIN 0015 - NETCENTRIC Total Solution - Base Year
CLIN 0016 - NETCENTRIC Total Solution - Option Year One
CLIN 0017 - NETCENTRIC Total Solution - Option Year Two
CLIN 0018 - NETCENTRIC Total Solution - Option Year Three
CLIN 0019 - NETCENTRIC Total Solution - Option Year Four

OR,

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

7. North American Industry Classifications System (NAICS) Code

The North American Industry Classification System (NAICS) Code for this requirement is 517311, Wired Telecommunications Carriers, and **cannot be changed at the Task Order level**.

8. Quality Processes (Full and Open/Small Business)

As a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 (or higher) or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method 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 prime offeror's organizational level performing the contract. If not ISO certified or 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 The Government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

9. Contract Data Requirements List (CDRL) (ID/IQ Level)

Section J, Exhibit A, A005 Contractor Manpower Reporting
Contractors are required to report all contractor labor hours (including subcontractor labor hours) required for performance of all services provided under the Network Operations & Infrastructure ID/IQ contracts. The reporting will be done for each task order awarded in the Contractor Manpower Reporting Application at http://www.ecmra.mil.

Each Task Order should provide the contractor with your organization requiring Activity Code (UIC).

10. Points of Contact

Customer Service (CS) – Email the NETCENTS-2 Team at netcents@us.af.mil if you have specific questions. **Please ensure "*NetOps and Infrastructure*" is noted in the subject line for review and appropriate distribution.**

If you require immediate assistance, the team can be reached at COMM 334-416-5070 / DSN 312-596-5070 Option 1.

11. NETCENTS-2 Document Updates

For the latest revisions to this and other NETCENTS-2 documents, please follow the instructions in Appendix N6 – NETCENTS-2 RSS Feed Instructions.

Appendix N1: NetOps and Infrastructure Solutions Requirements Package Checklist

Instructions: Use this checklist as a guide while completing your requirements package. Submit the completed checklist and the other applicable documents to the local contracting office to continue the Task Order process.

NOTE: This checklist references Air Force-specific guidance and best practices. Defer to your Agency's authorities.

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
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:	NetOps and Infrastructure Solutions, Section 5	☐
2.	**SCOPE ANALYSIS & SCOPE DETERMINATION**		
a.	Compare your requirements to the NetOps and Infrastructure Solutions ID/IQ requirements contained in the NetOps and Infrastructure Solutions PWS Template. This action ensures proposed requirements fall within scope of the NetOps and Infrastructure Solutions ID/IQ.	N2: NetOps and Infrastructure Solutions PWS Template☐	☐

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
b.	You may request that the NC-2 Technical 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 may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil		☐
4.	**MARKET RESEARCH**		
	Perform and document market research in a manner adequate to support acquisition decisions. If needed, a Market Research Report template may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil		☐
5.	**ACQUISITION PLANNING**		
a.	Some large or complex acquisitions may require an Acquisition Plan.	FAR 7.103 - 7.107 AFFARS 5307.1 – Acquisition Plans	☐
b.	Provide Acquisition Strategy Panel (ASP) Briefing Charts and ASP Minutes, if applicable.	AFFARS 5307.104-92 Acquisition Strategy Panels (ASP)	☐
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)	☐

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
6.	**NAICS CODE**		
	The **NAICS** code for the NetOps & Infrastructure Solutions ID/IQ has already been determined to be: **517311, Wired Telecommunications Carriers** This cannot be changed at the Task Order level.		☐
7.	**SERVICES DESIGNATED OFFICIAL (SDO)**		
	Appoint an SDO to coordinate with AFPEO/CM for all requirements with an estimated value of $100M or greater, and for coordination with OSD of IT requirements over $500M and other requirements over $1B.	AFI 63-138, 21 May 2013	☐
8.	**QUALITY ASSURANCE**		
a.	Appoint a Contracting Officer Representative (COR) if not already identified as part of the Multi-Functional Team.		☐
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). If needed, a QASP Template may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil		☐
9.	**REQUIREMENTS**		
a..	Is this a Sole Source Task Order? Contractor:	FAR 16.505(b)(2)	☐

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
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. If needed, a Justification and Coordination & Approval template may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil	FAR 6.303 FAR 16.505(b)(2)	☐
c.	Use the NetOps and Infrastructure Solutions PWS Template with attention to the following sections: - Services Delivery Summary - Data Item Deliverables - Standards & References	N2: Network Operations and Infrastructure Solutions PWS Template☐	☐
d.	If classified information necessitates contractual security specifications, complete and include a DD 254.	AFI 31-601, Chapter 4	☐
e.	Identify any supplementary attachments that need to be provided (i.e., network topology, building lists, government property).		☐Yes ☐No ☐N/A
f.	Are there any requirements which are Mission Essential Requirements? If yes, they must be identified as such.	DFARS 237.76	☐Yes ☐No ☐N/A
g.	Since services are being required, determination must be made by the Program Office certifying that no Inherently Governmental Functions (IGF) are being accomplished by the Contractor. If needed, an IGF Memo template may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil	FAR 7.503(e), DFARS 207.503	☐Yes ☐No ☐N/A

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
h.	Will there be Government Furnished Property (GFP) and Space? If yes, the Customer must provide a statement that the GFP or space is available. If needed, a template may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil NOTE: Not applicable for items incidental to the place of performance. See FAR 45.000(b)(5)	☐	☐
i.	Are there any consolidated contract requirements, that are, two or more requirements previously acquired separately now consolidated into a single requirement? If yes, provide justification. Applicable to actions greater than $6M.	DFARS 207.170-2 AFFARS 5307.170-3	☐ Yes ☐ No ☐ N/A
j.	Is this a new start program/project? If yes, provide supporting file documentation, including appropriate congressional notification/approvals.	AFFARS5332.702-90 "New Start Validation," and SAF/AQ memorandum, Congressional New Start Notification for Investment Appropriations, dated February 1, 2000	☐ Yes ☐ No ☐ N/A
10.	**INDEPENDENT GOVERNMENT COST ESTIMATE (IGCE)**		
	Provide a copy of an Independent Government Cost Estimate (IGCE) to include costs for option years. If needed, an example IGCE may be requested from the NETCENTS-2 Team by e-mail: netcents@us.af.mil		☐
11.	**TASK ORDER AWARD EVALUATION**		
a.	Use the Evaluation Guidelines to outline selection criteria for Task Order award, subject to ordering CO approval. If needed, example Evaluation Guidelines are provided.	Appendix N7: Example FAR 16 RFP with Evaluation Criteria	☐
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	☐

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
b.	Are the services being requested **severable or non-severable?**	DoD 7000.14R, Vol. III, Chapter 8	☐
c.	Confirm the Wide Area Workflow Inspector Code within 5 days of contract award.	DFARS 252.232-7003	☐
13.	**CLIN STRUCTURE AND PRICING**		
	Provide a CLIN / Pricing Structure	NC-2 NetOps and Infrastructure Solutions 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)**		
	A NETCENTS-2 RAD was accomplished. Local Contracting and MAJCOM 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. The NETCENTS-2 RAD is available on the NETCENTS-2 website.	http://www.netcents.af.mil/ Portals/30/documents/NE TCENTS- 2/AppSrvsDocuments/NE TCENTS- 2%20Requirements%20A pproval%20Document%20 (RAD)%20_5279.pdf?ver= 2016-08-03-155132-037	☐
16.	**TASK ORDER POST AWARD TASKS**		
a.	**The Contractor Performance Assessment Report (CPAR)** is required for NETCENTS-2 Task Orders. Provide a CPAR point of contact, which is normally the Contracting Officer Representative (COR). CPARS Focal Point Name: E-mail: Phone:		☐

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
b.	If the Task Order is projected to be less than $1M annually, a Customer Survey is required instead of a (CPAR). Contact the NETCENTS-2 Team by e-mail at netcents@us.af.mil or visit the NETCENTS-2 website for the NetOps Customer Survey		
c.	**Does the PWS contain information deemed classified under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy?**	5 U.S.C. § 552(b)(1) (2012)	☐

Appendix N2: NetOps and Infrastructure Solutions Task Order PWS Template

INSTRUCTIONS:

1. **You may use this format for your NETCENTS-2 NetOps and Infrastructure Solutions PWS. Using a standard template helps offerors know where to look for requirements and can decrease the time required to solicit proposals for the TO.**

2. **Save a copy of this template and modify it according to your requirements. Each time a PWS is accomplished, refer 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 and should be removed once section is complete.**

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 Appendix 1, *NetOps and Infrastructure Solutions Compliance & Standards List* and the NETCENTS-2 Network Operations and Infrastructure Solutions Users Guide, Appendix N3, *NetOps and Infrastructure Solutions Compliance & Standards List*.**

6. **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.**

7. **Recommended deliverables and standards are included as an Attachment in the PWS template and modified language relevant to your specific requirement should accompany the TO solicitation.**

NETCENTS-2 SOLUTIONS
NetOps and Infrastructure Solutions – Full & Open (F&O)/Small Business (SB)
Companion

[Add Your Own Task Order Title]

Task Order Performance Work Statement

Name:	
Organization:	
Address:	*(physical mailing address)*

Executive Summary

[*Provide a short description of the work to be performed]*

NETCENTS-2 NetOps and Infrastructure F&O
TO PWS
[Requesting Agency TO Title]

1. Purpose
[This paragraph should define the overall purpose and objectives of the contract.]

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 domains). Do not go into too much detail, as this will be detailed under the "requirements" paragraphs that follow.]

3. Requirement/Description of Services
[The Description of Services, describes at a high level (big picture), the services required under the contract, not each specific task. It should be consistent with the outcomes in the Services Summary and linked to Air Force (AF)/organizational requirements. The objective is to state, using established industry/government standards, what we need (objective), not how we need each task accomplished (methodology). The following is a list of the services/requirements on the NetOps Indefinite Delivery/Indefinite Quantity (ID/IQ) contract. They can be modified as needed to meet TO requirements. Sections 3.1-3.5 are example requirements that will help you facilitate the development of your PWS.

IMPORTANT--Describe the end product or outcome you want but avoid telling the contractor how you want it done. Ensure that you include all appropriate Contract Data Requirements List (CDRLs) for required deliverables and refer to DFARS Part 227 for inclusion of appropriate Intellectual Property provisions and clauses.] <mark>[Delete those that do not apply.]</mark>

3.1 Singularly Managed Infrastructure with Enterprise Level Security (SMI-ELS) Infrastructure Implementation and Operation

3.1.1 Singularly Managed Infrastructure (SMI)
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

The contractor shall provide services and solutions to realize a SMI that brings together at the middleware layer disparate networks and communications capabilities into a consistent AF enterprise-wide Information Technology (IT) capability.   The SMI shall support all AF mission requirements, and share data through federation with other infrastructure environments across the DoD, Federal agencies and Joint and Coalition environments. The contractor shall provide the capabilities for Core Enterprise Services (CES), transport layers, metadata environments, enclaves, Communities of Interest (COIs) and federation that make an SMI possible.

3.1.1.1 Core Enterprise Services

The contractor shall provide services and solutions that provide infrastructure capabilities to execute and manage content delivery services that deliver information to the warfighter and operational end user. CES will include but not be limited to storage management, messaging, transaction management, workflow management, search and discovery, directory services and service execution through an application server capability for control and management of multiple services. CES will provide monitoring for Quality of Service (QoS) and governance of configuration and contract management to ensure a stable environment. The contractor shall ensure these solutions exploit the DoD CES when and wherever possible and deliver AF-specific CES as required to augment the DoD CES to fulfill the AF mission.

Notes: Cyber Security (CS) related services, while part of Core Enterprise Services, are listed separately in the Enterprise Level Security section. Transport layer capabilities are covered in the Network Operations section and deliver the physical infrastructure upon which middleware and services operate, including physical plants and network operations capabilities.

3.1.1.2 Enclaves

The contractor shall provide services and solutions to identify a logical partitioning of the network and its information assets into capabilities-based enclaves. In the SMI-ELS Concept Document, enclaves are defined as virtual collections of hardware, software (including services), network and users that share common features, such as: authentication, authorization, trust, account directories and policies. The contractor shall provide services and solutions to enable the establishment of trust relationships and inter-enclave credentialing through which enclaves can interoperate and control the direction and nature of information exchanges, allowing the execution of multi-enclave service threads. The contractor shall provide services and solutions to facilitate migration of legacy enclave environments to enclaves compliant with the SMI-ELS Concept Document.

3.1.1.3 Federation

The contractor shall provide services and solutions that facilitate federation—a set of minimal agreements between enclave layer components which enable interaction between enclaves to take place transparently. The contractor shall provide federation capabilities within single domains and across multiple domains. Where applicable, the contractor shall provide federation capabilities across other domains within the DoD and Intelligence Community (IC) to share mission-critical information. The contractor shall establish federated naming and authentication between enclaves to enable discovery across them in accordance with applicable guidance, policy and direction. Contractor services and solutions shall adhere to core specifications, standards and technologies, such as PKI, SAML, JMS and WS-*, etc.

3.1.1.4 Metadata Environments (MDEs)

MDEs include the generation, consumption and management of metadata to enable the operational user to discover authoritative and aggregated data and support automated mediation where appropriate. The contractor shall provide services and solutions that help generate and manage metadata and MDEs. The contractor shall maximize the use of commercial-off-the-shelf (COTS) products when and where appropriate.   Metadata are characteristics or attributes of information assets, describing the type of information asset, its structure or syntax and its content or semantics, plus a wide range of other attributes that assist users in finding, managing and consuming information contained in assets. The contractor shall develop and sustain a MDE to be used in the discovery of information by end users and other services, the management of information assets for storage, retention and records management; and security authorization and access control. All metadata shall be created in accordance with the DoD Discovery Metadata Specification (DDMS) as appropriate. The contractor shall develop MDEs in accordance with the DoD Enterprise Architecture (EA) Data Reference Model or IC Architecture Reference Model as appropriate. The contractor shall develop a federated query capability to enable end users to discover and exploit mission services to gain mission essential information. Federated queries shall access MDEs within Enclaves to determine where information resides and how to access it. The MDE is characterized by the components and services it provides.

3.1.1.4.1 Metadata Components
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The MDE comprises the following components: Metadata Registry (MDR), Metadata Catalog and Service Registry.

3.1.1.4.1.1 Metadata Registry
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall develop and support a MDR to hold metadata definitions for the various types of metadata in a persistent store that is accessible during runtime operations. The contractor shall develop the capability for the MDE to use metadata from the MDR to tag instances of information assets with metadata values to support discovery, lifecycle management, storage management and categorization of the individual information assets. The contractor shall develop and support the capability for the MDR to track releasable information about individual artifacts and components of those artifacts where applicable. The metadata registry shall store COI vocabularies and other metadata artifacts, describing the concepts and terminology required for information exchange within a COI. The vocabularies will be used by ADS's to format exposed information assets and by the semantic discovery capability to allow users to find information assets and the services that deliver those assets. The contractor shall make it possible for vocabularies and other metadata artifacts registered in the AF MDE to become available through the DoD MDR or IC MDR using federation. The contractor shall manage metadata that enables users to discover and consume information provided by mission capabilities implemented as services.

3.1.1.4.1.2 Metadata Catalog
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall develop and support Metadata Catalogs that include metadata to describe individual information assets and that link those assets to the content delivery service that provides the asset to the end user. The metadata shall include the format of the information asset as delivered by the service, expressed as an XML schema, PDF or other government approved format and adhering to the vocabulary prescribed by the COI that governs that information asset. Metadata shall also include the tags necessary to support the DDMS.

3.1.1.4.1.3 Service Registry

The contractor shall leverage existing service registry and provide support for a Service Registry where all services are registered and stores information about implemented services, service interfaces and the ports and bindings involved. The Service Registry shall also track the identities and credentials of services within the enterprise Cyber Security infrastructure. The Service Registry shall support the invocation of services to deliver information assets once selected by an end user or another requesting service. Metadata Catalog entries shall point to services registered in the Service Registry, where the Service Oriented Architecture (SOA) infrastructure will be able to invoke the service to deliver the information asset to the requestor. The Service Registry shall enable the information stored in it to be federated with other DoD or IC service registries.

3.1.1.4.2 Metadata Environment Services

MDE services include the following: MDE Infrastructure Services, MDE Lifecycle Management, Discovery Services and MDE Federation.

3.1.1.4.2.1 MDE Infrastructure Services

The contractor shall provide infrastructure services to support MDEs. These services and solutions include, but are not limited to, Cyber Security, messaging, application hosting, storage management and other core enterprise services. The contractor shall provide standard repository management services and solutions to support authorized administrative personnel in the creation, update, retrieval and deletion of items within the MDE.

3.1.1.4.2.2 Metadata Lifecycle Management

Metadata Lifecycle Management includes the following services: Metacards and Asset Registration, Automated Metadata Population Services (AMPS), Versioning and Indexing.

3.1.1.4.2.2.1 Metacards and Asset Registration

The contractor shall provide services and solutions that support the manual or automatic population of metacards for registered assets in a structure that is compliant with DDMS or IC standards most current version and is in correlation with one or more COI vocabularies. The contractor shall provide services and solutions that support registering infrastructure services as assets, including but not limited to, the following:

1. Services developed to support COI business processes (e.g., content exposure, aggregation and presentation).

2. Service interfaces based on one or more XML schemata or other government approved format.

3. Vocabulary artifacts that describe COI domain knowledge. This includes Web Ontology Language (OWL) representations of knowledge and XML Schema Definition (XSD) representations of message types.

4. Information assets that are instances of authoritative content. This includes unstructured text documents, images, blob fields in databases and any other assets that qualify as requiring accountability of their content.

3.1.1.4.2.2.2 Automated Metadata Population Service
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall develop and support an Automated Metadata Population Service (AMPS) to automatically create the metadata for an information asset or service. AMPS shall automatically create metacards for registration in the Metadata Catalog. Users shall be able to invoke AMPS during registration of their assets to create metacards. AMPS shall be available as a service that can be invoked automatically during creation of an asset or in large scale metadata creation. AMPS shall be capable of tagging information assets defined by XML schemas as payloads coming from content delivery services so that services can be registered in the MDE and invoked upon discovery by an end user.

3.1.1.4.2.2.3 Versioning
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services that will deliver version control of all metadata artifacts. These services will include but not be limited to capabilities that maintain different versions of the metadata artifacts such as metacards, ontologies and indexes; manage and control deprecation of artifacts such as COI vocabularies; provide publication to consumers of versioning activities; ensure the application of the correct versions of the artifacts to other metadata services such as discovery, indexing and automated metadata generation and maintain histories and activity logs of metadata artifact versioning activities.

3.1.1.4.2.2.4 Indexing
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services that will deliver indexing capabilities to support discovery and management of information assets. These services will include but not be limited to the indexing of metacards using keywords, concepts and other indexing schemes; the application of the ontologies generated from COI vocabularies to the indexing of artifacts; the generation of the indexes either from metadata artifacts such as XSDs and WSDLs or directly from information assets in other formats such as documents, emails or presentations. The

services will also include capabilities that will maintain the indexes as metadata artifacts subject to the same constraints for versioning that are applied to the metadata artifacts to which the index references.

3.1.1.4.2.3 Semantic Discovery Services
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that support a semantic discovery capability that is based on vocabularies constructed by COIs. Semantic discovery users will be able to discover information based on their own preferred vocabulary and automatically navigate across other users' vocabularies to find information relevant to each query. The semantic discovery capability will support both users seeking mission critical information as well as developers responsible for implementing new information capabilities for those users. The semantic discovery capability will pass DDMS metacard contents, rather than asset content, directly to consumers with delivery service invocation instructions which will be activated by consumers as required. The semantic discovery capability will federate with other DoD and IC Components and their information assets through the Joint DoD/DNI Federated Search Specification.

3.1.1.4.2.4 Federation of MDEs
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that support the federation of MDEs. Federation of MDEs will direct discovery queries to the right enclaves and, using the IA infrastructure, access information and services across enclaves. The federation of MDEs will include the capability for MDEs to broadcast information requests and queries across all enclaves, if direct requests are not possible. The federation of MDEs will support the mutual exchange of metadata to share reference data and support roll-up of summary metadata for the purposes of discovery and metadata management.

3.1.2 Enterprise Level Security (ELS)

3.1.2.1 Cyber Security Architecture
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to realize a Cyber Security architecture that permeates all components and operations. The contractor shall deliver information architecture services that conform to the Air Force Enterprise Architecture along with adherence to DoD and federal standards for Cyber Security, using role-based, policy-based or attribute-based controls, and managing trusted relationships between network enclaves. The contractor shall support the conformance with the 2-way authentication and end to end security stipulated by SMI-ELS and the AF Cyber Security Enterprise Architecture.

The contractor shall provide services and solutions in support of a Cyber Security architecture that delivers but is not limited to the following five categories of security services: confidentiality, integrity, availability, authenticity and non-repudiation. The contractor shall provide services and solutions to exploit the Cyber Security architecture to protect information consumed and

generated by mission services. The contractor shall provide the capability of delivering these services at a level commensurate with the information assets being protected.

The contractor shall provide infrastructure capabilities that enable SOA solutions to implement IA in accordance with WS assurance standards. WS standards will be defined at the task order level, but the expected ones are:

WS-Security
WS-SecureConversation
WS-SecurityPolicy
WS-Trust
XML Signature
XML Encryption
XML Key Management (XKMS)

The contractor shall provide Cyber Security architecture, services, and solutions as stipulated by IC standards or other US, Allied, and Parner standards as specified in TO.

3.1.2.1.1 Confidentiality
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide confidentiality security services that prevent unauthorized disclosure of data, both while stored and during transit.

3.1.2.1.2 Integrity
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide integrity security services that prevent unauthorized modification of data, both while stored and in transit, and detection and notification of unauthorized modification of data.

3.1.2.1.3 Availability
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide availability services that ensure timely, reliable access to data and information services for authorized users.

3.1.2.1.4 Authenticity
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide authenticity services that ensure the identity of a subject or resource is the one claimed. The contractor shall ensure that authenticity applies to entities such as users, processes, systems and information.

3.1.2.1.5 Non-Repudiation
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide non-repudiation services that ensure actions within the AF, DoD or IC SOA service invocations, information queries, etc., are attributable to the entity that invokes them.

3.1.2.2 3.1.2.2 Cyber Security Services
[Modify Cyber Security requirements as they relate to your TO.]

The contractor shall provide services and solutions to implement and conduct IA operations such as, but not limited to, identity management, identity authentication, threat analyses and certification and accreditation.

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 applications 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 sig-na¬tures, 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 Task Order, 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.

3.1.2.2.1 Identity Management
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to accomplish identity management to enable users and applications to discover one another and utilize services provided by entities using methods such as the negotiated collaborative approach. The contractor shall also provide

capabilities to selectively monitor interactions and manage all active identities to include user, services, machines and services identity based on PKI.

The contractor shall provide services and solutions to accomplish lifecycle entity identity management from user creation to user revocation, as depicted in Figure 2. Entities are defined as both human and non-human users possessing accounts within the enterprise. The contractor shall support user creation (identity confirmation, credentialing, enrollment), user management (provisioning across single or multiple systems and services, automated provisioning workflow and self-service), user access (identification, authentication and authorization) and user revocation (de-provisioning and disablement). The contractor shall enable the de-provisioning process through automated account disablements and token revocation. The contractor shall provide access controls with rights, roles and privileges. The contractor shall provide the capability for all accounts to comply with FIPS 196, or other specified standard in TO, by using approved methods of authentication such as, but not limited to, the following:

1. PKI based authentication.
2. One-Time Password Tokens.
3. Biometrics with PIN or password.

3.1.2.2.2 Threat Analysis
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall conduct comprehensive threat analyses for Network Defense of the SOA Cyber Security architecture in support of DoDIN Network Defense.

3.1.2.2.3 Certification and Accreditation
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to help address the risks associated with AF network convergence into an interoperable enterprise and accomplish the certification and accreditation (C&A) of the AF SOA infrastructure. The contractor shall follow the RMF or ICD 503 to accomplish the infrastructure C&A as applicable. In order to satisfy DoD system security documentation requirements, the contractor shall register the SOA infrastructure in the Enterprise Information Technology Data Repository (EITDR), and complete the Security, Interoperability, Supportability, Sustainability and Usability (SISSU) checklist, as described in the IT LEAN Reengineering and SISSU Guidebook, v5.0, 4 April 2007. The contractor shall accredit the SOA infrastructure so that it can be leveraged by individual mission services. TOs for classified network support will identify when alternative registries and C&A guidance is applicable.

3.1.2.3 Enabling Security Capabilities
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide the following enabling capabilities to facilitate Warfighter access to critical mission capabilities:

1. Ensure all interactions between people, machines and services are verified using security policy.

2. Conduct confirmed two-way authentication using DoD-PKI and Federal Bridge credentials or applicable IC PKI and bridge.
3. Authorize access to data based on groups and roles.
4. Monitor and log all activities to provide for both real time assessment and historical analysis.
5. Use automated tools to analyze and detect anomalous behavior using real time/logged information to preclude and prevent internal attacks on AF information and computing resources.
6. Delegate roles and groups based on policy.
7. Mediate graduated access to data for various types of users.
8. Enable efficient cross-domain information sharing across networks operating at different classification levels (e.g., SIPRNET, NIPRNET and JWICS).
9. Operate, maintain and configure point to point, VPN and bulk encryption for network and longhaul circuits.
10. Provide encryption to the base campus SIPRNet connectivity.
11. Provide SCI network security capabilities as specified in TOs.

3.1.3 Enterprise Service Management
==[Sample language below. Modify to fit your requirement. Delete if not applicable.]==

The contractor shall provide services and solutions to accomplish Singularly Managed SMI-ELS service level management. The contractor shall provide operation and maintenance of the SMI-ELS infrastructure including, but not limited to, network monitoring, load balancing, information archival and backup, disaster recovery, Continuity of Operations (COOP) and Enterprise Support Desk (ESD). The ESD shall support users encountering issues in accessing mission capabilities.

The contractor shall provide lifecycle management of services for both requestors of services and service providers. The contractor shall establish processes to inform users of the availability of new version of services.

The contractor shall provide enterprise service management to SCI networks as specified in TOs.

3.1.4 SMI-ELS Architecture Documentation
==[Sample language below. Modify to fit your requirement. Delete if not applicable.]==

The contractor shall document the SMI-ELS within the AF Enterprise Architecture (EA). The contractor shall document the Metadata Environment in the DoD EA Data Reference Model (DRM). The contractor shall document the standards and protocols that the AF will enforce in the DoD EA Technical Reference Model (TRM). The contractor shall develop DoD Architecture Framework (DoDAF) products or products adhering to other architecture guidelines as specified in TOs. The contractor shall support process improvement events, such as AFSO21, to address SMI-ELS processes and issues. The contractor shall document AFSO21 products and engineered processes in the Process Reference Model (PRM) and DoD EA System Reference Model (SRM).

The contractor shall develop, document, and register SCI architectures and artifacts per TO directions. The contractor shall document engineering processes and process improvement activities and artifacts per TO directions for SCI systems and networks.

3.2 Network Services and Solutions

The contractor shall provide services and solutions that enable Network Operations and Network Infrastructure capabilities. Networks as defined in this section are for data, voice and video.

3.2.1 Network Operations

The contractor shall provide services and solutions that enable Network Operations (NetOps) to operate and defend the DoD Information Network (DoDIN) to ensure information superiority. DoDIN network operations refer to land, air, and space networks across multiple levels of security. The contractor shall provide capabilities that support the essential tasks, Situational Awareness (SA), and Command and Control (C2) that comprise the operational framework that comprise NetOps. The contractor shall support the following essential NetOps tasks: DoDIN Enterprise Management (EM), DoDIN Network Defense (DoDNetD), and DoDIN Web Content Management.

The contractor shall provide services and solutions that help the Government attain the following desired effects in its management of the DoD Information Network (DoDIN):

1. Assured System and Network Availability that ensures uninterrupted availability and protection of system and network resources. This includes providing for graceful degradation, self-healing, fail-over, diversity and elimination of critical failure points.

2. Assured Information Protection of information in storage, at rest, while it is passing over networks, including from the time it is stored and catalogued until it is distributed to users, operators and decision makers.

3. Assured Information Delivery of information to users, operators and decision makers in a timely manner.

3.2.1.1 DoDIN Enterprise Management (EM)
The contractor shall provide services and solutions that enable Enterprise Management. This shall include traditional systems and network management (Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management), as well as information and infrastructure protection. It shall also encompass the DoDIN's information technology (IT) services management and consist of the many elements and processes needed to communicate across the full spectrum of the DoDIN, including the following:

1. Enterprise Services Management
2. Systems Management
3. Network Management
4. Satellite Communications Management

5. Electromagnetic Spectrum Management

3.2.1.1.1 Enterprise Messaging and Directory Services

The contractor shall provide services and solutions that enable directory services, e-mail and organizational messaging in accordance with Enterprise Architecture.

3.2.1.1.2 Enterprise Application Services and Service Management

The contractor shall provide services and solutions that enable service management and the management of enterprise application services, including, but not limited to, the following:

1. Monitoring and measuring application and service health and performance.
2. Reporting and visualizing key application and service QoS metrics.
3. Monitoring and enforcing Service Level Agreement (SLA) compliance.
4. Managing application and service lifecycles.
5. Provisioning applications and services.
6. Logging and auditing application and service activities.
7. Anticipating application and service problems and sending alert notifications.
8. Pinpointing the root cause of application or service problems and allocating resources to correct the problems.
9. Automating failover and load balancing.
10. Mediation services transforming service messages and performing content based routing.
11. Correlating enterprise service messages for business transaction tracking.

3.2.1.1.3 Enterprise Information Management

The contractor shall provide services and solutions that enable information management services, including, but not limited to, the following:

1. Collaboration Services
2. Continuity of Operations
3. Disaster Recovery
4. Data Storage
5. Storage Area Network
6. Network Attached Storage
7. Back-Up/Archive
8. Records Management

3.2.1.2 DoDIN Network Defense (ND)

The contractor shall provide services and solutions that enable DoDIN Network Defense, including, but not limited to, the following:

Cyber Security (CS) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This shall include, but not be limited to, providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA services shall include, but not be limited to:

1. Assured Information Sharing and Management
2. Access Control
3. Cross-Domain Security
4. Information Environment Protection
5. Certification and Accreditation
6. Risk Analysis
7. IA Awareness
8. Auditing
9. Emanations Security (EMSEC) /TEMPEST for TS or SCI environments
10. Communication Security (COMSEC)
11. Operation Security (OPSEC)
12. Information Protection
13. Authentication
14. Resource Protection
15. Federated Identity Management
16. Virtual Private Networking
17. Network Protection
18. Filtering
19. Intrusion Detection and Prevention
20. Cryptographic Services
21. Key and Certificate Services
22. Insider Threat Protection
23. Anomalous Behavior Detection
24. Time Compliance Network Order (TCNO)
25. Computer Incident Response Team (CIRT)
26. Air Force Computer Emergency Response Team (AFCERT)
27. Telecommunications Monitoring and Assessment Program (TMAP)

   1. Computer Network Defense (CND) – Defensive measures to protect, monitor, analyze, detect and respond to unauthorized activity with DoD information systems and computer networks and defend information, computer and networks from disruption, denial, degradation or destruction. This shall include, but not be limited to, the employment of IA capabilities in response to CND alert or threat information and the capability to predict, analyze and defend against new attack vectors.

   2. Computer Network Defense Response Actions (CND RA) – Deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. The contractor shall also rapidly and accurately implement JTF-GNO and NetOps directed Information Operations Condition (INFOCON) changes and provide command and control on the progress and completion.

3. Defense Critical Infrastructure Protection (CIP) – Actions taken to prevent, remediate or mitigate the risks resulting from critical infrastructure vulnerabilities. Actions shall include, but not be limited to, changes in tactics, techniques or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; etc.

3.2.1.3 DoDIN Web Content Management
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to develop and administer web sites that enable Web Content Management and help ensure information is available to users on the DoDIN to accomplish their mission. Capabilities shall include, but not be limited to, those that enable the following core services areas:

1. Web Content Discovery – The ability to quickly search for information throughout the DoDIN. The contractor shall provide the capability for operational staffs to search across multiple sources from one place using a web crawler and web browser, vice making several attempts. Once products are located, the Content Delivery service shall permit users to pull in needed products.

2. Web Content Delivery – Delivery of requested information to DoDIN users. The contractor shall provide the capability for timely delivery of items across multiple, heterogeneous communication systems with delivery and read receipt notifications, providing assured delivery of information products.

3. Content Storage – The contractor shall provide and support physical and virtual places to host data on the network throughout the DoDIN with varying degrees of persistence.

The contractor shall provide services and solutions that provide Network Operations Centers with capabilities such as, but not limited to, the following:

1. The ability to optimize the flow and location of information over the DoDIN by positioning and repositioning data and services to optimum locations on the DoDIN in relation to the information producers, information consumers, and the mission requirements.

2. The ability to ensure that the DoDIN is optimally delivering the information required by DoDIN users in accordance with information delivery priorities.

3. The visibility of information flowing across the DoDIN and of those systems used to store, catalog, discover, and transport information.

4. Tools to view information flows and access, determine impact to network capacity, and ensure user profiles are being satisfied with a reasonable quality of service.

5. The capability to prioritize information requirements, determine the sources responsible for providing that information, and stage information content throughout the DoDIN in support of a given operation.

6. The ability to track and maintain knowledge of various requests and user profiles for information.

7. The ability to coordinate changes in operating parameters of DoDIN assets.

8. The ability to review and validate the user-profile database.

3.2.1.4 Network Operations Enabling Capabilities
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that accomplish or provide the following enabling capabilities:

1. Distributed Network Connectivity – Robust, redundant data paths and nodes with both physical and logical diversity to maximize effectiveness and eliminate single points of failure.

2. COOP – Plans and capabilities to enable uninterrupted NetOps operations with seamless transfer of operations, especially network C2 following outages at any key NetOps sites. These shall include, but not be limited to, fully redundant backup capabilities with automatic failover that is transparent to users.

3. Information Management and Exchange – Automated tools and processes to facilitate the exchange of information and to aid operators in visualizing network operations and events, to facilitate rapid event characterization and information exchange and to keep pace with rapidly changing networks. Operate the Base Information Transfer System and Official Mail Center. Provide Privacy ACT, Freedom of Information Act (FOIA) and record management training.

4. Standardization – Standardization of configurations, processes and applications across the enterprise from the gateways to the desktops to facilitate centralized management, enhance security through configuration control and save manpower in certification and accreditation, patch implementation, hardware/software upgrades and asset tracking.

5. Risk Management – A multi-faceted and global approach for risk management on applications currently residing on the network and new applications waiting to be fielded. This approach shall assess the benefits of adding the application to the network and any security risks it may introduce, the ability to execute corrective actions or configuration control measures and the potential effect any change would have on network configuration, services, or other applications. This process shall apply across MAJCOMs and include arbitration processes in the event of a conflict between the intended user and others. Solutions shall follow government approved standards such as the Information Technology Infrastructure Library (ITIL) framework.

6. Change Management – Tools, tactics, techniques and procedures for accomplishing change management across the AF enterprise to help implement network operational concepts.

7. Training – Resources needed to provide training such as training materials, instructors and facility.

8. System Administrator - Set up, configure, develop, maintain, troubleshoot and support internal and external networks.

9. Database Management - Perform loads, upgrade, patches, data recovery, backups and maintain active directory.

10. Account Management – Create, modify and delete; voice, data and video accounts and provides means to unlock Common Access Card (CAC).

3.2.1.5 Network Command and Control
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

The contractor shall provide services and solutions that enable network command and control, including, but not limited to, the following:

1. The consolidation of network SA services and solutions that integrate C2 capabilities, eliminate the need for scheduled manual reporting and provide the warfighter with on-demand, real-time operational status of networks, core services and applications directly serving or influencing his or her Area of Responsibility.

2. Rapid characterization and response to anomalous activity, including, but not limited to, "low and slow" network probe and exploitation efforts and implement appropriate defensive actions or countermeasures.

3. Trend analysis and correlation of network incidents (e.g., probes, intrusions and virus outbreaks), outages and degradation events.

4. Rapid implementation of security countermeasures by facilitating the coordination of network restoration priorities and actions after an intrusion or adverse network event.

5. Coordination and reallocation of limited resources (e.g., bandwidth, frequencies) in response to multiple and/or conflicting warfighter requirements.

3.2.1.6 Network Management and Enterprise Services
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

The contractor shall provide services and solutions that accomplish Network Management for AF Network Operation Center (AFNOC)/ Integrated Network Operations and Security Center (I-NOSC) activities such as, but not limited to, the following:

1. Automation and enforcement of network policy.

2. Operation of network sensors.

3. Monitoring and analysis of network behavior.

4. Network performance analysis and tuning.

5. Network counter measures.

6. Network boundary management and control.

7. Network security access.

8. Network service orchestration.

9. Execution of INFOCON.

10. Asset management to include equipment management.

The contractor shall provide services and solutions that accomplish Network Management and Support for the Enterprise Support Unit (ESU) and the Enterprise Service Desk (ESD) anticipated activities such as, but not limited to, the following:

1. Network configuration management.

2. Load balancing.

3. Vulnerability analysis and response.

4. Application and content management.

5. COOP management.

6. Resource virtualization.

7. Information lifecycle management.

8. Service Orchestration.

9. Virtualized IT service support.

10. Help Desk/Call Center.

11. Security Management Service.

The contractor shall provide services and solutions that accomplish Enterprise Services to support Network Operations such as, but not limited to, the following:

1. IT service virtualization.

2. IT Support.

3. Service/security management and provisioning.

4. Domain security.

5. Cross-domain security.

6. Collaboration (video teleconference).

7. Content and service staging.

8. Federated content discovery.

9. Application, system, services and data hosting.

10. Development of applications for database or web pages.

11. Producer to consumer availability of service.

12. Configuration and change management.

TOs from other agencies, departments or AF functional communities for the same purpose may be issued. These TOs may specify and substitute other standards and guidance in order to provide solutions tailored to meet their network management and enterprise services strategies.

3.2.2 Network Infrastructure
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions in support of transport layer capabilities to deliver the physical infrastructure upon which the SOA middleware and services operate, including, but not limited to, messaging capabilities and site preparation and installation services. Support of the transport layer includes the AF's Information Transport System (ITS) which is the engineering, installation and sustainment of the high-performance, survivable fiber optic backbone to include "wired" and "wireless" networks.

3.2.2.1 Messaging
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide messaging capabilities allowing separate, uncoupled applications to reliably communicate asynchronously. The messaging system architecture generally replaces the client/server model with a peer-to-peer relationship between individual components, where each peer can send and receive messages to and from other peers. The contractor shall provide delivery pathways, such as Web services, HyperText Transfer Protocol (HTTP) or HyperText Transfer Protocol Secure (HTTPS) connections, or other links, as needed to support content delivery and presentation service requests. The contractor shall tag and register delivery pathways as necessary. The contractor shall support other data transport pathways, such as File Transfer Protocol (FTP) and Open DataBase Connectivity (ODBC), for legacy systems and databases.

The contractor shall provide messaging services including, but not limited to, the design and/or implementation of: messaging architecture; point-to-point distribution of messages; publish-subscribe distribution of messages; message producer; message consumer; one-way interaction between a message producer and a message provider; request-reply interaction between a message producer and a message consumer and connectivity between an application and a messaging provider.

The contractor shall provide messaging services that encompass, but are not limited to, provision of federated, distributed and fault-tolerant enterprise messaging capabilities; message publishing and subscribing, peer-to-peer messaging and queuing; support for the configuration of QoS parameters for a published message, including the priority, precedence and time-to-live (TTL); provision of guaranteed delivery to disconnected users or applications; development of Online Asynchronous Processing (OLAP) and real or near real-time enterprise data reporting capabilities.

3.2.2.2 Site Preparation and Installation Services

The contractor shall perform site preparation and installation activities to support implementation of required services and solutions under this contract at any AF, DoD or other Federal Agency location.

3.2.2.2.1 Requirements Analysis and Conceptual Design

The contractor shall perform requirements analyses and conceptual designs at required locations. During this process, the contractor shall collect all the information to complete a requirements analysis and conceptual design. The contractor shall survey, evaluate and provide technical advice concerning all existing infrastructures, communications, power, Heating, Ventilation and Air Conditioning (HVAC) and environmental aspects of the site. The contractor shall provide an implementation plan, in accordance with the TO, reflecting the strategy, schedule and recommendations (e.g., site architecture, topology and configuration) for the implementation with considerations of on-site failover and continuity of operations. The government will provide applicable information, as available, such as existing/projected user network resources and locations, GFE, base support requirements and other written information related to specific implementation for each TO to establish the unique characteristics of each site. Access to government facilities will be provided and interviews shall be coordinated with government points of contact specified in the TO.

Types of support and services provided by the contractor shall include, but not be limited to: Email, Server and Storage Area Network Administration, Security Boundary Administration, Print Management, Configuration/Release Management (i.e. Security/Patch Administration, etc.), Mobile/Remote User Services Support and Administration, Network Infrastructure Management and Administration, Certification and Accreditation (i.e. Security Scanning, etc.), Directory Services and Event Management.

The contractor shall possess reach back capabilities to obtain expertise that may not be immediately available onsite and the ability to surge in times of crisis.

The contractor is required to deliver all services and solutions provided under this contract described below. The contractor shall design, develop, install, document and test custom solutions and their infrastructures. The contractor shall enable system solutions to integrate with: Air Traffic Control, Land Mobile Radio, Command Post Switches, Defense Red Switch (DSR), Defense Red Switch Network (DRSN), Giant Voice, Enhanced 911, Cell Systems, Base Altering Systems and Crash Nets and any other systems specifically identified in the TO.

3.2.2.2.2 Site Survey

The contractor shall perform site surveys at required locations. The findings of the site survey and any actions required in preparation for system installation shall be documented.

3.2.2.2.2.1 Systems Engineering

[NOTE: If applicable, insert additional MAJCOM or organization Systems Engineering policies, requirements or guidelines. Include any special instructions for Top Secret/TS SCI systems or applications.]

The contractor shall provide systems engineering solutions for the analysis, design, integration, installation, testing and life-cycle support of new and upgraded systems associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture. The contractor shall employ disciplined systems engineering processes in accomplishing contract tasking, using commercial best practices in accordance with AFI 63-1201, LifeCycle Systems Engineering, for systems engineering processes in planning, architecting, requirements development and management, design, technical management and control, technical reviews, technical measurements, integrated risk management, configuration management, data management, interface management, decision analysis, systems management, inspections and maintenance, sources of supply maintenance and repair, and test and evaluation, verification and validation. These systems engineering solutions shall follow industry standard engineering processes and may include but not be limited to: technical assessments of all user requirements, integration of all GFE and Contractor Furnished Equipment (CFE) as proposed, hardware and software information, network applications, system design, training (COTS or customized)(initial and recurring), maintenance and support, system interface studies and control documents, network integration and test plans, cost analysis/trade-off studies, engineering change proposals, Voice Switching System (VSS) facility and systems/applications studies, VSS call detail recording and traffic measurement data analysis, engineering support (digital transmission/switching equipment) to government engineers. The contractor shall provide reengineering capabilities to examine structures, systems and roles for the purpose of executing a ground-up redesign for achieving long-term, full-scale integration required for the DoDIN.

TOs will further refine the systems engineering processes according to MAJCOM or functional policies and practices. The contractor shall employ the principles of open technology development described in the DoD Open Systems Architecture Contract Guidebook for Program Managers and in NetCentric Enterprise Solutions for Interoperability (NESI) body of knowledge, and systems engineering activities used in developing contractor solutions shall adhere to open architecture designs for hardware and software and employ a modular open systems architecture approach.   The contractor's systems engineering planning and design activities shall also adhere to the DoD's Information Sharing and NetCentric Strategies published by the DoD CIO and the engineering body of knowledge and lesson's learned accumulated in NESI. TOs may require adherence to other governmental standards.

3.2.2.2.2.2 System Upgrade/Update Support

The contractor shall provide system upgrade support and future planning associated with delivery of infrastructure capabilities as defined by the AF EA. The contractor shall maintain currency with the design and development of systems similar to those implemented in the VSS and discuss recommended changes or strategies with the government. The contractor shall identify current or anticipated problem areas relating to telephony hardware and software systems and present technical issues of interest or value to the government regarding VSS.

The contractor shall provide information regarding technology advancement to the government and support new telecommunications products and solutions as they are approved by the DoD JITC and introduced into the VSS network. These newly emerging solutions must adhere to AF or IC security requirements as they pertain to voice telecommunications assets prior to installation.

3.2.2.2.2.3 Post-Cutover Support
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

Each solution shall include a warranty as specified in Section I, Clause 52.246-17. In addition to FAR Clause 52.246-17, the following additional requirements apply: Users shall have highly reliable and maintainable telephony products and system solutions to interoperate with the described environment. Components shall be maintainable and expandable by the user without voiding the warranty coverage.

In addition to any OEM warranty coverage, three types of post cutover operation and maintenance support shall be provided: System Support, Workmanship Support and Construction Support. The contractor shall provide for restoration of the system and repair of equipment in a timeframe specified as required by this contract, unless stated otherwise in the TO. The means to transport equipment and repair personnel both to and from the government site is the responsibility of the contractor. The contractor shall provide technical support, software support and hardware replacement for failed components, engineering support and maintenance services necessary to ensure active management, reliable operations and rapid restoration. These technical support services shall include Tier II to Original Equipment Manufacturer (OEM) level support as required based on the need to achieve problem resolution. All technical support shall be provided by certified technical personnel fluent in the English language. If the Offeror is alerted to a degradation or failure, the Offeror shall provide immediate support to the operational user to identify, troubleshoot and remedy the problem. The Offeror shall execute all hardware repair actions necessary to return the affected system to full operational capability. If the failed equipment is no longer under any alternative warranty support, the Offeror shall provide replacement equipment. Technical support shall be provided on a continuous, as-needed basis twenty-four (24) hours per day, 365 days per year for systems, peripherals, applications and devices deployed. The contractor shall provide toll free, email, DSN and PSTN access capabilities to contact requesting support for support issues.

3.2.2.2.3 Design/Integration Reviews
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

The contractor shall conduct design and integration reviews if required in the TO and in compliance with disciplined system engineer processes. This may be a formal or informal preliminary and final design reviews.

The contractor shall provide a single source of integration management for worldwide support, planning and sustainment of dissimilar manufacturer's switching systems, applications and peripheral equipment related to the VSS. The contractor shall identify cross functional applications and technical issues from selected symbiotic functional areas and document the opportunities for resolving the issues. The contractor shall report impacts on the issues such as costs, return on investment, schedule dependencies and recommend functional and technical

solutions. The contractor shall identify integration issues and problems such as requirements definition, architecture and policy/standards compliance and engineering guidelines compliance. The contractor shall enable convergence with data systems and/or collaborative tools as specified and required in the TO.

3.2.2.2.3.1 Prototypes
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall develop schedules and implementation plans with definable deliverables, including parallel operations where required, identification of technical approaches and a description of anticipated prototype results associated with delivery of infrastructure capabilities as defined by the AF DoD or applicable IC enterprise architecture. The contractor shall operate and maintain prototype applications, infrastructures, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process.

3.2.2.2.3.2 Preliminary Design/Integration Review (PDR)
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

During the PDR, the contractor shall present initial draft system design associated with delivery of infrastructure capabilities as defined by the enterprise architecture for government review.

The draft documents to be reviewed shall include those specified in the TO. Examples may include the system requirements, the final Site Survey Report, System Design, Installation Specification (IS), Engineering Drawings and Installation Plan. This review shall include a list of recommended long-lead time items that the government must order and have available at the time of system installation. This review shall be in sufficient detail to ensure technical understanding of the following: mission and requirements analysis, identification of all equipment and software to be integrated and to be used in the development of the design and the scope and schedule of the work to be performed.

3.2.2.2.3.3 Final Design/Integration Review (FDR)
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

During the FDR, the contractor shall present final system design documentation associated with delivery of infrastructure capabilities as defined by the enterprise architecture for government review. The documents shall consist of those identified in the TO. Upon government approval of the FDR documentation, the contractor will be authorized to proceed with the installation. If discrepancies are identified, the contractor shall correct all discrepancies and another FDR may be required at the discretion of the government.

3.2.2.2.4 Site Preparation
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

As part of an overall system design and installation, the contractor may be required to perform site preparation support as required by the IS and approved by the Government Contracting Officer. The Government may, at its option, perform any portion or all of the requirements

documented in the site survey report. Base civil engineering functions (or equivalent) will be used whenever possible. The contractor shall work with the base Quality Assurance Personnel (QAP) to accept civil engineering functions (or equivalent) as being in accordance with the approved implementation plan prior to beginning work. The final IS shall specify what site preparation the Government will perform and what site preparations the contractor will perform.

3.2.2.2.4.1 Pre-Installation Briefing
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

As required by the TO, the contractor shall present pre-installation briefings at the user sites. These briefings shall include the implementation strategy, installation schedule, verification that all allied support is completed and the site is ready for installation and discussions of any potential problem areas. Additional pre-installation briefings may be held, as required by the government.

3.2.2.2.4.2 Government Support
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The government will furnish facilities and utilities to the contractor, including light, heat, ventilation, electric current and outlets for use by installation personnel as required and stated in TOs. These facilities and utilities will be provided as specified in the Site Survey Report. These facilities will be readied prior to arrival of contractor personnel and be provided at no cost to the contractor. The contractor shall provide required temporary utilities, which are not readily available in the work area. The contractor shall coordinate, through the on-site COR, any requirement before temporary disconnection of a utility. The contractor shall submit a request in writing to the on-site COR fourteen (14) days in advance of the necessity of utility disconnection.

3.2.2.2.4.3 Installation
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall engineer, install, configure, modify, relocate or remove Communication and Information (C&I) systems for operational use. The systems and equipment installations or modifications must comply with established architectures. The contractor shall perform validation and verification testing on the system, assist users in configuring the system to meet their system requirements and provide all applicable operating manuals/system management guides. Further, the contractor shall provide pre-cutover and post-cutover on-site training IAW with TOs. The government will identify personnel who will receive this training. The training shall provide for in-depth hands-on maintenance, operations and database administration.

3.2.2.2.4.4 Inside Plant
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall, (as required by each TO), install and configure all the components for inside the plant (e.g., power, groundings, HVAC, racks, fiber optic distribution panels, equipment, internal cabling, comm. closet, etc.). The contractor shall install and test all cable and components IAW accepted industry standards, unless superseded by a Government approved IS indicated within the TO. Electrical and communications cable, conduits, and

circuits shall be installed IAW the National Electric Code (NEC). The contractor shall clearly label each end of every individual cable in accordance with the floor plans or engineering drawings. The contractor shall provide attached labels that are durable and legible. For any deviations to the specific installation specification, the contractor shall submit a proposal to the CO for approval.

3.2.2.2.4.5 Outside Plant
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall, as required by each TO, install and configure of all the components for outside the plant (e.g., fiber, manholes, duct, building entries, trenching, digging, constructions, external cabling, etc). The contractor shall install and test all cable and components IAW accepted industry standards, unless superseded by a government approved IS indicated within the TO. Electrical and communications cable, conduits and circuits shall be installed IAW the NE. The contractor shall clearly label each end of every individual cable in accordance with the floor plans or engineering drawings. The contractor shall provide attached labels that are durable and legible. For any deviations to the specific installation specification, the contractor shall submit a proposal to the CO for approval. The contractor's design should not include aerial cable unless the government has approved specific site exceptions. When use of aerial cable is approved, installation and test shall be IAW accepted industry standards, unless superseded by a government approved IS indicated within the TO.

3.2.2.2.4.6 Tools and Testing Support
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide all tools, installation materials and test equipment required to perform any required product installation and maintenance as called for by the TO. All tools and test equipment shall remain the property of the contractor. Any damage caused by the contractor to existing site facilities or equipment which might occur during site preparation, installation, testing or cutover of the system will be repaired at the expense of the contractor unless otherwise directed by the government. The site shall be restored to the original condition which existed prior to the event unless otherwise directed. The TO will specify testing and inspection requirements. The contractor shall demonstrate that the system design meets the reliability/availability/maintainability requirements of the TO. Mean Time Between Failure data will be used to calculate the reliability/availability/maintainability of the system. The calculations shall be based on all of the equipment installed in the network. The contractor shall be capable of performing reliability, availability and maintainability analyses of components, isolated sub-networks and the entire system.

3.3 Dynamic Test Environment
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services to support the design, implementation and operation of a dynamic test environment. The dynamic test environment will enable applications developers to deploy their applications and services into the infrastructure and test the operation of those applications and the effect of those applications on other fielded capabilities.

3.3.1 Design

The contractor shall provide tools and services to support the design of the dynamic test environment. This will include but not be limited to: defining concepts for dynamic testing; articulating processes and procedures for conducting dynamic testing; architecting the test environment; evaluating and selecting products and technologies for the test environment.

3.3.2 Implementation

The contractor shall provide tools and services to implement the dynamic test environment. This will include but not limited to, configuring the products and technologies required by the design of the test environment; installing those products and technologies in location designated by the design; developing capabilities necessary to fully integrate the products and technologies with each other and with existing infrastructure capabilities; integrating the products, technologies and developed capabilities with existing infrastructure capabilities to configure the test environment and developing and executing test procedures to ensure the proper functioning of the test environment.

3.3.3 Operation

The contractor shall provide tools and services to operate the dynamic test environment. This shall include, but not be limited to; developing operating procedures, user guides, training materials and other documentation to ensure the correct use of the test environment by users; developing administrative and management processes and documentation to ensure proper operation of the test environment in support of end users; monitoring the operation of the test environment to ensure users are achieving their test objectives; conducting performance evaluations of the test environment; and scheduling and executing technology refreshes and other activities to ensure the ongoing operation of the test environment.

3.4 Communication Operations and Maintenance (O&M)

The contractor shall provide services and solutions that accomplish O&M that include, but not limited to the following:

1. Operations and Telephony Infrastructure to include telephone customer support.

2. Meteorological and Navigational Aids (METNAV).

3. Land Mobile Radios (LMR).

4. Personal Wireless Communication Systems (PWCS).

5. Video Teleconferencing (VTC).

6. Satellite Communications (SATCOM).

7. Air Traffic Control and Landing Systems (ATCALS).

8. Radar.

9. Computer Systems Control (Tech Control) including but not limited to Circuit Management, Circuit Management Office and Telecommunications Manager.

10. Electronic Communication Management.

11. Visual Imagery and Intrusion Detection

12. Deployment Manager.

13. Antennas.

3.5 General Requirements

[The General Requirements 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 quality control plans or systems, location of the work, hours of work, physical security, emergency or special events, environmental or hazardous requirements, security requirements or specific training requirements. Modify each section IAW your requirements.] Sections 3.6-3.6.32 are example requirements that will help you facilitate the development of your PWS. [Delete those that do not apply, except where specified.]

3.5.1 Contractors Use of NETCENTS-2 Products Contract
[Do Not Remove]

The contractor shall obtain all products and associated peripheral equipment required by each individual TO from the NETCENTS-2 Products contract.

3.5.2 Enterprise Software Initiative
[Do Not Remove]

See DFARS 208.7402 regarding use of the DoD's Enterprise Software Initiative (ESI)

Blanket Purchase Agreements (BPAs) for software license purchases.

3.5.3 Software License Management
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide maintenance and support to control the entire asset lifecycle, from procurement to retirement, which includes applications, license agreements as well as 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.

3.5.4 Hardware
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

All hardware provided in support of solutions under this contract shall include all software and associated hardware required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the OEM.

3.5.5 Software Support
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

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 support all software revisions deployed or resident on the system and sub-systems. The data rights ownership/licensing guidance is specified in DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017.

3.5.6 Government Furnished Equipment (GFE)
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

Under some TOs, the government will provide products acquired under this contract, other contracts and GFE identified in site specific TOs. The contractor's design shall incorporate existing systems/subsystems to the maximum extent possible, based on cost/technical tradeoff analysis conducted during the engineering process to ensure security and resource sharing of both GFE and Contractor Furnished Equipment (CFE).

3.5.7 Host Nation Installations
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

As specified by the TO, the contractor shall use commercial telephone industry installation standards as documented in TL9000 compliant procedures for accomplishment of all installation work unless otherwise prohibited by host nation regulations and/or standards. The contractor shall determine if any host nation restrictions are applicable to any installation. The contractor shall be responsible for compliance with all host nation labor, safety and environmental laws, regulations and standards applicable at each installation location. If any additional permits or regulations apply, the contractor shall inform the government and provide a proposal to initiate the appropriate documentation upon approval from the government.

3.5.8 Tools and Test Equipment
<mark>[Sample language below. Modify to fit your requirement. Delete if not applicable.]</mark>

Unless specified otherwise in the TO, the contractor shall provide all tools and test equipment required to perform any required product installation and maintenance as called for by the TO. All tools and test equipment shall remain the property of the contractor.

3.5.9 Warranty
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Each product shall include a warranty as specified in Section I, Clause 52.246-17. In addition to FAR Clause 52.246-17, the following additional requirements apply: Users shall have highly reliable and maintainable network-centric products and system solutions to interoperate with the described environment. Components shall be maintainable by the user without voiding the warranty coverage. Components, which are expandable, shall be expandable by the user without voiding the warranty coverage provided the government adheres to standard commercial practices in accomplishing the additions. Four types of warranty shall be provided:

1. System Warranty
2. Workmanship Warranty
3. Construction Warranty
4. Equipment Warranty

The warranty program shall provide for restoration of the system and repair of equipment in a timeframe specified in this contract, unless stated otherwise in the TO. The contractor shall provide means to transport equipment and bear transportation charges and responsibility for equipment and repair personnel under warranty while in transit both to and from the government site.

3.5.9.1 System Warranty
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall provide a minimum 1-year system warranty (some customers may require 2 or more years of warranty) to include coverage of all equipment supplied, installed and integrated by the contractor associated with delivery of infrastructure capabilities as defined by the AF EA. The system warranty shall ensure the full operational use of the system (CFE and GFE). The contractor shall provide to the government a 24-hour a day, 7-day a week point of contact for the system warranty. The system warranty shall begin at the time the final system DD Form 250 is signed by an authorized government representative. The system warranty shall provide fault diagnosis, hardware and software repair, replacement or redesign. The contractor shall be responsible for diagnosing any problems, identifying malfunctioning equipment and removing the equipment for repair. Prior approval shall be obtained from the authorized government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the government, unless stated otherwise in the TO. The system warranty shall include transportation for both contractor personnel and equipment to and from the specific site. The system warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS, after notification by the authorized government site representative unless stated otherwise by the TO. Costs for system warranty will be included within each TO proposal provided by the contractor as required by the TO.

In lieu of a system proposal that includes a traditional warranty, the customer and contractor may agree to a basic system proposal plus a block of hours for contractor Maintenance Support Services. For many contractors and customers, this strategy has proven advantageous since traditional system warranties can be voided by today's dynamically changing networks forcing the customer to maintain the network in a static environment during the warranty period. In addition, support is limited to a much narrower scope with a traditional system warranty whereas a contractor Support Services contract is much more flexible in solving problems as they arise within the entire Network-Centric environment.

3.5.9.2 Workmanship Warranty
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall provide a minimum 1-year workmanship warranty (some customers may require 2 or more years of warranty) on all work provided or integrated under this contract. The warranty shall ensure the full operational use of the system (CFE and GFE). The contractor shall provide to the government a 24-hour a day, 7-day a week point of contact for the workmanship warranty. The workmanship warranty shall begin at the time the final system DD Form 250 is signed by an authorized government representative. The workmanship warranty shall provide fault diagnosis, hardware and software repair, replacement or redesign. The contractor shall be responsible for diagnosing and fault isolation of any problems, identifying the poor workmanship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the government. The workmanship system warranty shall include transportation for both contractor personnel and bits, pieces and parts to and from the specific site and the actual repair. The workmanship warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS, after notification by the authorized Government site representative unless stated otherwise by the TO.

3.5.9.3 Construction Warranty
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall provide a minimum 1-year construction warranty (some customers may require 2 or more years of warranty) on all work provided or integrated under this contract. The warranty shall ensure the full operational use of all work. The contractor shall provide to the government a 24-hour a day, 7-day a week point of contact for the construction warranty. The construction warranty shall begin at the time the final system DD Form 250 is signed by an authorized government representative. The construction warranty shall provide fault diagnosis, repair, replacement or redesign. The contractor shall be responsible for diagnosing and fault isolation of any degradation problems, identifying the poor construction-ship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized government site representative or government COR before affecting any repair. The construction warranty shall include transportation for contractor personnel, bits, pieces and parts to and from the specific site and the actual repair. The construction warranty shall provide for a return to service any degrading component or area within 48-clock hours CONUS, 96-clock hours OCONUS, after notification by the authorized government site representative unless stated otherwise by the TO.

3.5.9.4 Equipment Warranty

Unless specified otherwise in the TO, the contractor shall provide standard, OEM pass through, extended or otherwise warranties for the periods specified in the TO for all hardware and software products, for both CONUS and OCONUS government sites located worldwide. Repairs shall be accomplished within 48-clock hours CONUS, 96-clock hours OCONUS, of receipt of the equipment warranty trouble call, unless stated otherwise by the TO, when the contractor is performing the warranty repair. The warranty shall also provide for repair or replacement of equipment and repair and distribution of updated software to all users who purchased the software from this contract. ,Warranty coverage commences on the date of acceptance in block 21B of the DD Form 250, Commercial Invoice dated and signed or SF 1449 dated and signed.

The contractor shall provide a worldwide warranty repair solution capability for systems with qualified maintenance repair personnel and leverage existing OEM support infrastructures to the greatest extent possible. Repairs shall be performed at a time required by the Task/Delivery Order/Delivery Order or as coordinated by the government COR. The contractor shall provide a 24-hour, 7-day a week warranty repair point of contact to receive calls from the government. The contractor shall provide the capability for toll-free telephone access for obtaining technical warranty repair support assistance from worldwide locations. The contractor shall provide the tools, equipment and consumables required for personnel to complete their duties. The contractor shall not invalidate the warranty provided on components purchased under this contract when the government elects to perform user self-maintenance and/or self-installation during the warranty period. Note: The government will perform routine user-maintenance for all equipment both during and after the warranty period using separately orderable spare parts and/or repaired parts from this contract. The government will only be liable for any damage to the equipment that results from government Maintenance or additions to equipment that did not adhere to stand commercial practice.   At no additional charge to the government, the contractor shall furnish, for hardware purchased under this contract, all repairs (labor and parts) for the duration of the warranty period. At a minimum, repair during the warranty period shall be equivalent to standard per-call maintenance during the Principal Period of Maintenance (PPM) as specified in this PWS. The government, at its option, may order additional repair coverage during the warranty period. The governments purchase of additional repair coverage will be specified in details by the TO.

All parts replaced during the warranty period, in an unclassified environment, shall become the property of the contractor. However, in classified environments the government will maintain title of certain items. These items typically will be broken storage devices/mediums.   All other parts may be returned to the contractor and the government will have up to 30 days to relinquish possession of the part.

The warranty shall not apply to maintenance required due to the fault or negligence of the government.   If government negligence results in a repair call (either for equipment under warranty or per call maintenance), the maximum repair time shall not apply and the government will pay the price per hour specified in the contract for the hours rendered to complete the repair.

Only new or reconditioned parts shall be provided for repairs. If reconditioned parts are provided, the reconditioned parts shall carry the same warranty provisions as originally provided by the contractor for new parts.

The contractor guarantees to repair at no charge any malfunction which reoccurs within 90 calendar days of the initial repair. Warranty of Repair is a separate warranty from those described elsewhere in the contract.

If the contractor elects to replace the malfunctioning hardware, the contractor shall either provide the government with a permanent replacement which shall contain a unique serial number or shall provide the government with a temporary replacement with a unique serial number.   If the contractor elects to repair the malfunctioning hardware, the contractor shall repair and return the repaired hardware to the government at which time the temporary replacement shall be surrendered to the contractor at the contractor's expense.

3.6 Maintenance
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall provide a worldwide maintenance solution capability (on-site and on-site per-call) for systems provided under this contract with qualified maintenance personnel, leveraging existing OEM support infrastructures to the greatest extent possible. Maintenance shall be performed at a time required by the TO or as coordinated by the government COR. The contractor shall provide a maintenance POC 24-hours-a-day, 7-days-a-week to receive calls from the government. The specific maintenance requirements will be included in the TO and may include maintenance on systems/equipment not purchased under this contract. The contractor shall provide the capability for toll-free telephone and e-mail access for obtaining technical maintenance support assistance from worldwide locations. The contractor shall provide remote engineering and technical support via telephone or other remote system capabilities to assist maintenance personnel, analyze software, hardware, system problems and provide problem resolutions. This support may consist of routine maintenance, testing, diagnostic fault isolation, problem resolution, activation of features and/or equipment, software configurations and general information on features or capabilities of equipment. All requests for remote maintenance services shall be acted upon immediately upon receipt of the request and logged for inclusion in a service ticket status log of some type. The requesting unit shall be notified of the current status of corrective actions for hardware and software related problems that cannot be immediately corrected. The contractor shall provide the tools, equipment and consumables required for personnel to complete their duties.

3.6.1 Per-Call Maintenance/Standard Per-Call Maintenance (SPCM)
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall provide the government with on-site per-call maintenance at the government location for all cable plant and non-cable plant items. One instance of a per-call maintenance visit shall include the repair of all units identified at the time the government notification call to the vendor was placed. The minimum charge per-call shall not exceed one (1) labor hour. The maximum charge per-call shall not exceed any limitations (labor and parts) indicated by the government at the time of the maintenance call without prior approval from the designated government official and as funded in the applicable TO. Hourly rate charges shall commence when the contractor representative reports to the government site representative indicated in the call. Outside the Principal Period of Maintenance (OPPM) is defined as all time other than the PPM. If a call is placed during the OPPM or, if the government wants the weekend/holiday time to count toward time to repair,

then the OPPM rate may be applicable. The OPPM rate shall be applicable only if specifically requested by the government at the time of the maintenance call and approved by the CO.

3.6.2 Contractor Provided Non-Cable Plant, Non-Switching System SPCM
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 8 hours to respond and 48 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 16 hours to respond and 96 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the TO.

3.6.3 Government Owned Equipment Non-Cable Plant, Non-Switching System SPCM
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall maintain the non-cable plant and non-switching systems (i.e., microwave radios, UPS equipment, multiplexers, antennas, LAN/CAN/MAN/WAN equipment, VTC equipment, phones, land mobile radios (LMR) Air Traffic Control and Landing Systems (ATCALS) and Meteorological and Navigational Aid (METNAV)) and those provided by the contractor under this contract. The contractor shall have, from the time of notification of equipment failure(s), a maximum of 8 hours to respond and 48 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 16 hours to respond and 96 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the TO.

3.6.4 Switching System SPCM
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 4 hours to respond and 24 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 8 hours to respond and 72 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the TO (i.e., non-ISDN/ISDN capable, DSS, etc.).

3.6.5 Cable Plant Maintenance
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 2 hours to respond and 8 hours to complete the repair(s) or temporarily replace or patch the malfunctioning components for CONUS or 4 hours to respond and 12 hours to complete the repair(s) or temporarily replace or patch the malfunctioning components for OCONUS, unless otherwise stated in the TO. This maintenance shall include inside and outside cable plant maintenance. If the government cannot provide drawings identifying placement of both inside and outside cable components to be maintained, then the government will order a cable-plant survey via TO using the applicable labor categories; the contractor shall not be held accountable for any repair timeframes until the government provides such drawings. The contractor shall also provide, on a pre-scheduled basis, preventative and routine maintenance required for optimized usage and life of the existing cable plant on a per-

call basis. Within 24 hours of a repair or patch that restores service using a temporary repair, the contractor shall provide the government with a draft list for components that were temporarily repaired until permanent replacements could be obtained. In this event, the contractor shall provide a firm-fixed-price proposal to the user for installation of the components identified in the draft list.

3.6.6 Rapid Response Per-Call Maintenance (RRPCM)

For RRPCM, the contractor shall have a maximum time of 2 hours from the time of notification of failure(s) to respond, unless stated otherwise in the TO. Repair time shall be within 12 hours.

3.6.7 System Maintenance

Unless specified otherwise in the TO, the contractor shall provide all supplies, parts, tools and test equipment required for maintenance of the system and be responsible for total system maintenance.

3.6.8 Maintenance Charges

The per-call maintenance charge may include the CLIN labor rate, travel and ODCs and transportation of any equipment, as applicable. Replaced faulty parts shall remain the property of the government.

3.6.9 Maintenance Alternative

The government may select maintenance alternative (standard or rapid per call response) with the issuance of a TO. The government shall have the option to change the type of maintenance by giving the contractor 30-days' notice and a contract modification. Any change in type of maintenance will not be considered a partial termination of the TO for the convenience of the government.

3.6.10 Relocation and Removal

The contractor shall relocate and remove systems as specified in the TO. The contractor shall be responsible for storage, staging and deployment of any equipment and materials provided as part of awarded TOs unless otherwise mutually agreed upon by the contractor and the government.   If removal of equipment and/or material is necessary, the contractor shall be responsible for disposal and shall comply with all applicable industry rules and regulations. Any equipment removal and/or disposal shall be coordinated with a designated official at the host base communications squadron.

3.7 Surge Requirements

Surge requirements include greater than expected requirements/workload for existing services within the scope of TO awarded. Normally, surge requirements are of short duration, from 1 to 6 months. An example of a surge requirement is additional help desk or system maintenance support personnel required to handle temporarily increased workloads because of war or contingency. Surge requirements shall be accomplished as required under the TO.

3.8 Unified Capabilities Requirements (UCR)
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the TO, the contractor shall report to the government through quarterly PMRs, how each solution awarded meets the UCR.   Detail shall include, but not be limited to the applicable MILDEP Service Level Architecture requirements. For example, vendor shall report how each awarded solution that is implemented at a United States AF Installation meets the United States AF i-TRM Architecture requirements. Similar report requirements including the ConstellationNet Architecture may also be requested at the TO level.

3.9 Special Asset Tagging
[Sample language below. Modify to fit your requirement. Delete if not applicable.]

See DFARS 252.245-7001 regarding Special Asset Tagging requirements.

3.10 [Next Requirement]

4. Contractual Requirements
[The following contract requirements are applicable to all TO.   Each requirement should be tailored to fit your TO.]

4.1 Performance Reporting
[Modify to fit your TO. Sample language below.]

The contractor's performance will be monitored by the government and reported in Contractor Performance Assessment Reporting (CPARs). Performance standards shall include the contractor's ability to:

1. Provide quality products, incidentals and customer support.

2. Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times.

3. Provide satisfactory product repairs or advance replacement, as appropriate.

4. Provide timely and accurate reports.

5. Respond to the customer's requests for proposals and configuration assistance as identified in each delivery order.

6. Meet subcontracting goals.

4.2 Program Management
[Modify to fit your TO. Sample language below.]

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

4.2.1 Services Delivery Summary
[Modify to fit TO level service/performance parameters. Make sure the services required have measurable outcomes.]

The Services Delivery Summary (SDS) will be in accordance with AFI 63-101, Acquisition and Sustainment Life Cycle Management and FAR Subpart 37.6, Performance-Based Acquisition. SLAs will be defined in each TO.

[Modify to fit your TO. Example Table below.]

Desired Outcome		Performance Objective	Performance Threshold	
Overall Outcome	Specific Outcomes		Target	Tolerance
Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure compliance with NetOps and Infrastructure Solutions deliverables requirements	Deliver the NetOps and Infrastructure Solutions w/ predetermined outcomes and on time	Documentation submitted IAW CDRL A001 verifies the TO was completed on time	98% of the time

4.2.2 TO Management
[Modify to fit your TO. Sample language below.]

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/TO 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 services, 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 should 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.

4.2.3 Configuration and Data Management
[Modify to fit your TO. Sample language below.]

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. The contractor shall have an approved property control system IAW FAR 45, DFARS 245 and approved procedures to document and track all GFM and GFE. The contractor shall provide as-built documentation including, but not limited to, drawings and diagrams of the solution provided under each TO identifying specific cards in a chassis/shelf. The as-built documentation shall also include layout drawings, power drawings/specifications, floor plans and engineering specifications generated in support of the installation of the system. Documentation shall also include equipment listing with serial/model numbers and manufacturer specifications.

4.2.4 Records, Files and Documents
[Modify to fit your TO. Sample language below.]

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 NetOps and Infrastructure Solutions contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

4.3 Security Management

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

the TO. All Classified Contracts must have at a minimum, the Clause 52.204-2 Security Requirement, incorporated into the contract.

Each base will follow its own classified process IAW with the proscribed Federal guidance of the NISPOM and FAR "Subpart 4.4 along with DD Form 254. When transmitting classified information ensure all classified information is properly sanitized and/or degaussed of all sensitive/classified information IAW AFSSI 5020.

For assistance and guidance on submitting Classified TO, the NETCENTS-2 Customer Service can be reached at COMM 334-416-5070 / DSN 312-596-5070 Option 1.

4.3.2 Personnel Security
<mark>[Modify to fit your TO. Sample language below.]</mark>

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).

Certain TOs may require personnel security clearances up to and including Top Secret and certain TOs 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 contract/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 contract/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 Antiterrorism (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.

4.3.3 Protection of System Data
<mark>[Modify to fit your TO. Sample language below.]</mark>

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 Regulations 5400.7-R and DoDM 5200.01 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.

4.3.4 On-Site Task Approval Process
[Modify to fit your TO. Sample language below.]

The contractor shall, for CONUS tasks (7-day notice) and for OCONUS tasks (14-day notice), notify the on-site COR in writing before a requirements analysis/conceptual design visit, site survey and other on-site tasks are to be performed. The following information must be provided: Names of Employees, SSAN, Security Clearance, Location, Project Number, On/About Date Planned for On-Site Work, Anticipated Duration of Visit, Support Required.

4.3.5 Travel Requirements
[Modify to fit your TO. Sample language below.]

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 the tourist class, 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.

4.3.6 Other Direct Cost (ODC)
[Modify to fit your TO. Sample language below.]

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

4.4 [Next Requirement]

5. Quality Processes (Full and Open/Small Business)

As a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 (or higher) or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method 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 prime offeror's organizational level performing the contract. If not ISO certified or 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   The Government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

Attachment 1 – Deliverables and Standards

Deliverables

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoDI 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 will 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.

Appendix N4: Customer Ordering Guide Using AFWay

Customer and Contracting Officer Instructions for NetOps and Infrastructure Solutions

(AFWay can be found at: https://www.afway.af.mil/)

Important Considerations.

- Before initiating a Request for Proposal (RFP) or Request for Information (RFI) (both are referred to as an "RFQ") in AFWay, complete all of the required documentation referenced in Appendix N1 and verify with your Contracting Officer no further documentation is required.

- Although the term RFQ is indicative of products requirements for a delivery order and the term RFP is indicative of services requirements for a task order, these two terms will be synonymous in this document. **All references to the term RFQ will designate any customer solicitation from vendors for solutions to requirements, whether it involve products or services.**

- Customers who wish to solicit a Request for Information (RFI) from services vendors will use the same process to gather this information as they would for a RFQ.

- If the NetOps and Infrastructure Solutions RFQ requires IT software/hardware procurement, vendors are responsible to include these estimates as part of their response to the RFQ. A minimum of two of these estimates must be provided with the response to the customer RFQ.

- If only using AFWay for NETCENTS-2 Services task orders, you may expedite your acquisition by using "**NC2S**" as your ECAN. Keep in mind, if an ECAN is changed and there are open RFQs or Orders already in a workflow, they will now be attached to the new ECAN's workflow which may cause issues in your approval process.

- Vendors will be registered with accounts in AFWay by the time ordering is available for the respective NETCENTS-2 NetOps and Infrastructure Solutions ID/IQ contracts.

- No Government Purchase Card (GPC) acquisitions are allowed on the NetOps and Infrastructure Solutions ID/IQ contract.

- AFWay is an unclassified system. There will be no classified information processed via AFWay. Classified task orders will follow a unique process entirely outside of AFWay at the advisement of the NETCENTS-2 PMO and decentralized customer organization.

- For optimal use of the AFWay website, vendors are encouraged to use Internet Explorer 8.0 or earlier versions. AFWay is not compatible with any other browser.

1. **AFWay Registration for New Users**

   a. To register as a new customer to AFWay, navigate to https://www.afway.af.mil/ using your web browser, and select the "Registration" button on the AFWay Home Page.

   Figure 1 – AFWay Home Page

   b. Fill in all of the required fields, identified with an asterisk. NOTE, the "Agency" field determines the approval process for RFQs. Depending on the menu selection, the user will be required to complete one of the following two steps to successfully complete registration.

      1. If the "Agency" field is "DEPT OF DEFENSE – AIR FORCE," four additional required fields will appear: MAJCOM, BASE, DRA, and ECAN. The DRA and ECAN fields are critically important to the success of a Customer's RFQ reaching the Contracting Officer (CO) for approval and distribution to the NETCENTS-2 NetOps and Infrastructure Solutions vendors.

         - **MAJCOM** – Enter your MAJCOM
         - **BASE** – Enter your Base
         - **ECAN** – Use your original ECAN at your base or "NC2S" if only using AFWay for NETCENTS-2 Network Operations ID/IQ
         - **DRA** – This field determines the person who will fulfill the Base Equipment Custodian Officer (BECO) role in the approval chain. The BECO will then assign the respective CO. For help finding the correct Direct Reporting Activity (DRA), select the "Help finding your DRA" link to the right of the DRA field. A page showing "DRA's By Base" will appear. DRA's are listed according to the base in alphabetical order. If the base has more than one DRA, check for the respective MAJCOM and Organization, or verify with your Base Equipment Custodian Officer (BECO) for the correct DRA.

2. If the "Agency" field is populated with any other menu selection, no additional fields will appear. After registration is complete, the Customer will need to contact the AFWay phone at (334) 416-5771, Opt 1, 5, 5, and send an e-mail to team5@gunter.af.mil to finish account configuration and have the ability to generate RFQs to vendors. This is available to active duty and federal employees only.

c. Once all of the applicable fields have been completed, click on the "Register on AFWay" button to complete the registration process. If there are any errors, a new page will be displayed indicating any registration errors. Click on the "Return to Registration" button, correct any errors, and then click on the "Register on AFWay" button.

d. After successful registration, you will be directed to a Welcome screen and a one-time temporary password will be sent to the E-mail Address used during registration.

2. Logging into AFWay

a. To login to AFWay, navigate to https://www.afway.af.mil/ using your web browser.

b. Click on the "Log In" link under the Home Page heading on the left.

Figure 2 – User Login Page

c. Enter your E-mail Address established during your AFWay registration and corresponding Password, and click the Login button. Note, use your one-time temporary password issued via email upon initial authentication. You will be prompted to change this password after successfully logging in.

NOTE: If an incorrect Password is entered 3 times, the account will be locked. Contact the Field Assistance Service (FAS), DSN 596-5771, opt 5 and a new one-time temporary password will be automatically generated and sent via e-mail. After a successful login to the system, you will be required to change the password.

d. Forgotten Password

- If you've forgotten your password, select the "Forgot Password?" link to get to the following screen.

60
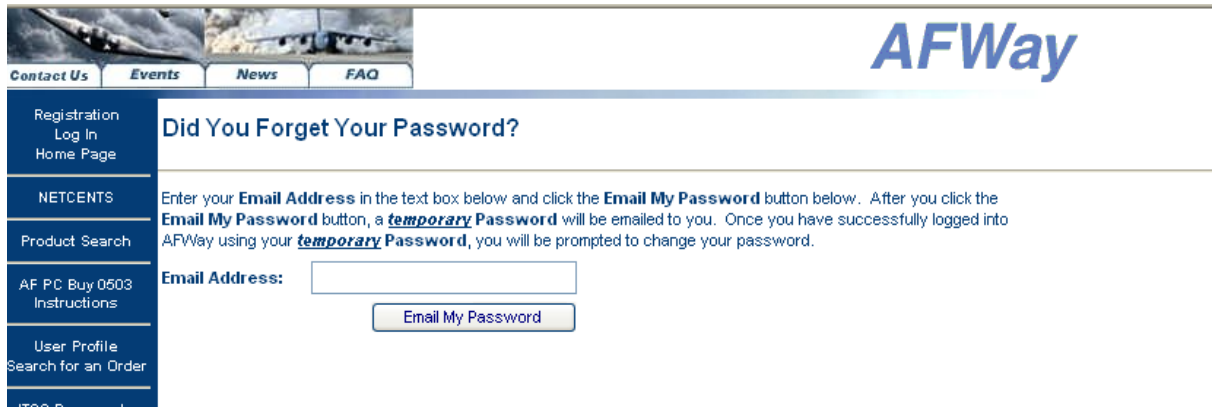
Figure 3 – Forgotten Password Page

- Enter your E-mail Address used during AFWay registration and click the "Email My Password" button. A one-time temporary password will be e-mailed. After successfully logging in, you will be required to change the password.

- If your E-Mail Address is unknown, incorrect or invalid, please contact the FAS, DSN 596-5771, opt 5 for AFWay assistance.

3. Account Setup

a. Upon successfully logging into AFWay, your User Profile page will be displayed as seen in Figure 4.

b. On the User Profile page, click on the "View/Edit Your Account Information" link.

c. Verify that you are registered as a Customer in the Authorization section, and verify that the Agency that is selected is correct.

d. If you are not a DoD Air Force customer, verify that the agency listed is correct.

Figure 4 – User Profile Page

e. If any changes are made, click on the "Update User Information" button at the bottom of the page. Return to the User Profile page by selecting the "User Profile" link in the left blue menu pane.
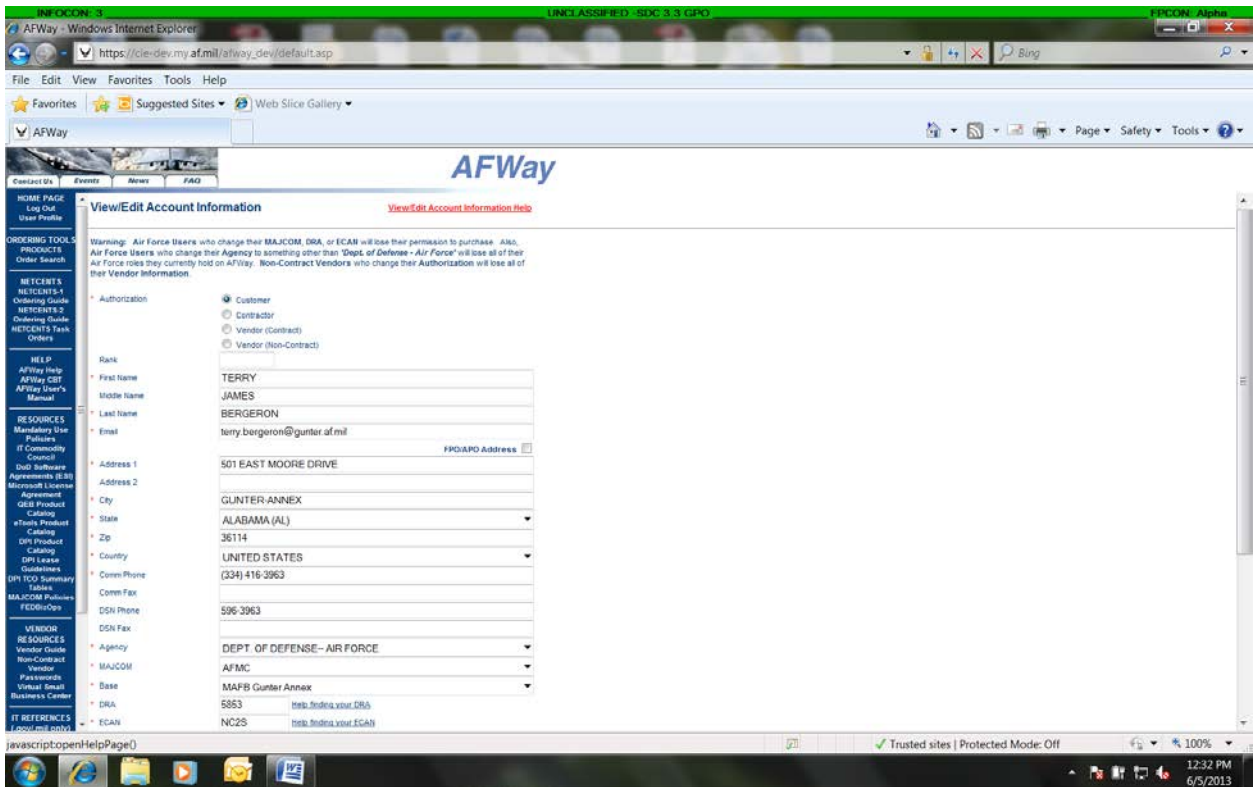
Figure 5 – View/Edit Account Information Page

4. **Submitting a Request for Quote (RFQ) Using AFWay**

    a. After you've successfully logged into AFWay, navigate to the User Profile page by clicking on the "User Profile" link from the menu selections on the left.

    b. Initiate the RFQ process by clicking on the "Submit a Request For Quote" link.

    NOTE: If an error occurs stating that you do not have permission to purchase, contact the FAS, DSN 596-5771, opt 5 for AFWay assistance.
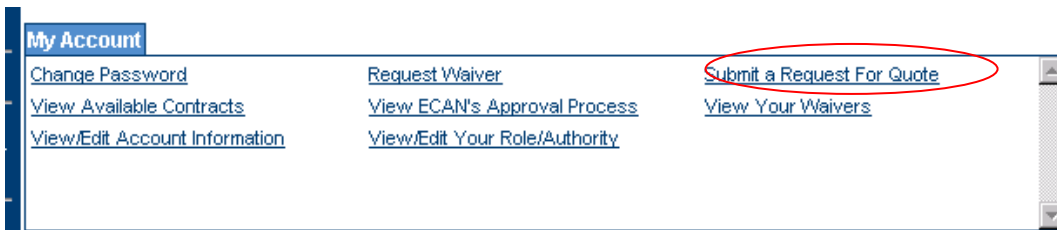
Figure 6 – Submit a Request For Quote Link

    c. Upon clicking the link, the RFQ page is displayed to the User. The RFQ page allows the User to specify and include all information required for a RFQ. Follow the instructions below for completing each section of the RFQ page:
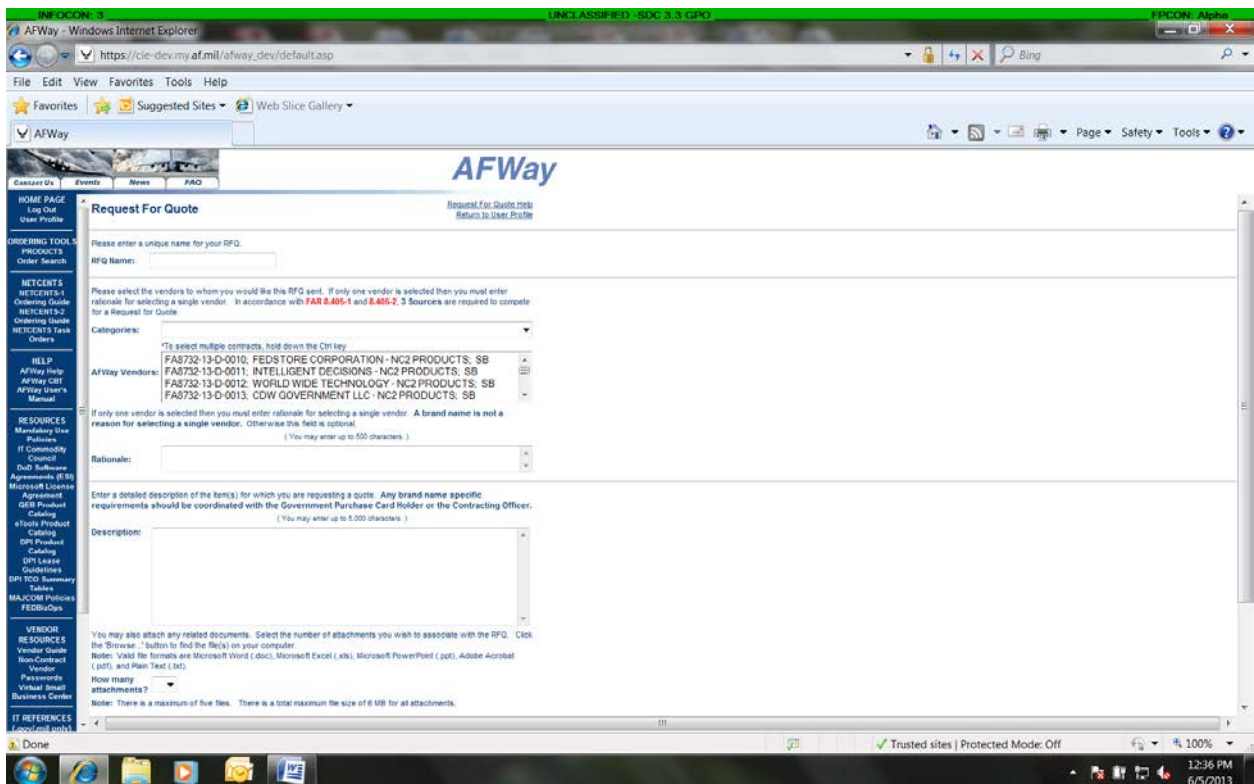
Figure 7 – Request for Quote (RFQ) Page

- **RFQ Name**: Create a unique NetOps and Infrastructure Solutions RFQ name, but ensure the name begins with 'NC-2 NetOps and Infrastructure Solutions ...' (i.e. NC-2 NetOps – System Acronym)

- **Categories**: Select either 'NC-2 NetOps and Infrastructure Solutions Small Business' or 'NC-2 NetOps and Infrastructure Solutions Full & Open'

- **AFWay Vendors:** By selecting either 'NC-2 NetOps and Infrastructure Solutions Small Business' or 'NC-2 NetOps and Infrastructure Solutions Full & Open,' the applicable set of vendors will be highlighted. NOTE: **Do not deselect any NC-2 vendors from this list.** All NC-2 vendors must have an opportunity for fair competition based on Federal Acquisition Regulation (FAR) unless a Fair Opportunity Exception (FOE) has been approved by the CO.

- **Rationale: This field requires no input** unless there is an exception to fair opportunity. This field is reserved for Sole Source justification/rationale when only one vendor is selected in the AFWay Vendors field.

- **Description:** Use one of the following to provide a general description of the overall RFQ requirement(s)

    - Network Services and Solutions

    - Communication Operations and Maintenance (O&M)

    - Dynamic Test Environment

- **How Many Attachments?:** First, enter the quantity of attachments. Then attach any required documentation needed as part of the RFQ so the Vendors can adequately respond (PWS, Instructions to Offerors, Proposal Evaluations, etc). Select Browse to attach document(s). The RFQ has a limitation of 5 attachments, which must be less than 6MB in size. Recommendation: Use the AMRDEC SAFE ACCESS FILE EXCHANGE (SAFE) website to post large amounts of documentation. Directions for the use of SAFE can be found in Appendix N5.

- **Desired Delivery Date**: **The desired delivery date entered should be the estimated first day of performance.**

- **Quantity Requested**: This field is not applicable for a Services RFQ; however, place a "1" in this field for 1 Service requested.

- **Anticipated Price:** Use your Independent Government Cost Estimate (IGCE) **

** IMPORTANT: Keep in mind your IGCE will not be visible to the vendors. Only the CO and the customer are able to see the IGCE posted on AFWAY.

d. Once all of the fields have been completed and reviewed, click on the "Submit RFQ" button to complete the process and generate an RFQ. A window will display notifying the User that the RFQ was successfully added and it will be assigned a unique RFQ ID.

Request For Quote   RFQ Help

Request For Quote (RFQ ID 74) Successfully Added.

Close Window Return to User Profile

Figure 8 - RFQ Successfully Added Page

5. RFQ Approval Process & Tracking

Please note that the current email notification system in AFWay is working sporadically. We advise that you check your AFWay RFQ status on a regular basis to ensure that the RFQ is moving along at a timely rate until this email issue is resolved. Although we are publishing the email process in this guide, your email notifications may not be working

a. An RFQ submitted by a DoD Air Force customer will go through an approval process (workflow process), NC2S, determined by the DRA and ECAN number entered during registration or account setup. After each approval step, an e-mail notification is sent to the approver and the customer who initiated the RFQ.

b. Non-AF. An RFQ initiated and submitted by customers who are not 'Agency - DoD Air Force,' and thus, no DRA and ECAN, will go directly to vendors for responses once the RFQ is submitted.

c. Once the AF customer has submitted an RFQ, the RFQ approval (workflow) process for DoD Air Force customers is as follows:

- **Equipment Custodian (EC)** – Determined by ECAN

- **Base Reviewer (optional)** – Determined by BECO

- **Base Equipment Control Officer (BECO)** – Determined by DRA

- **Approval Official (AO)** – Determined by EC

- **Resource Advisor (RA)** – Determined by EC

- **Contracting Officer (CO)** – Determined by BECO

d. **Contracting Officer (CO)** is the final approval step in the workflow process. The CO either approves or disapproves, and enters a Vendor Response Due Date. The Vendor Response Due Date entered should be the **deadline date the vendors have to submit a response to a RFQ**. The CO can change the desired delivery date, if necessary, and should reflect the estimated first day of performance. See Figure below.
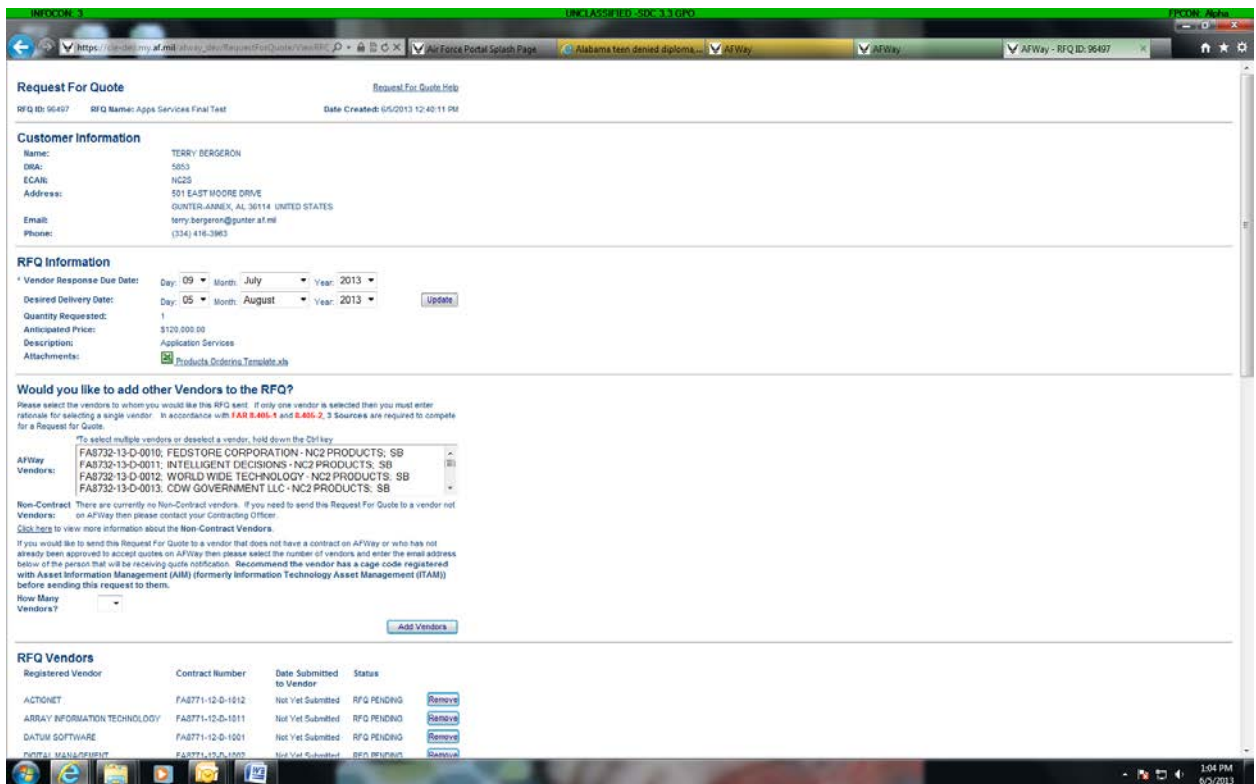
Figure 9

e. At this point, the CO can approve and submit the order.
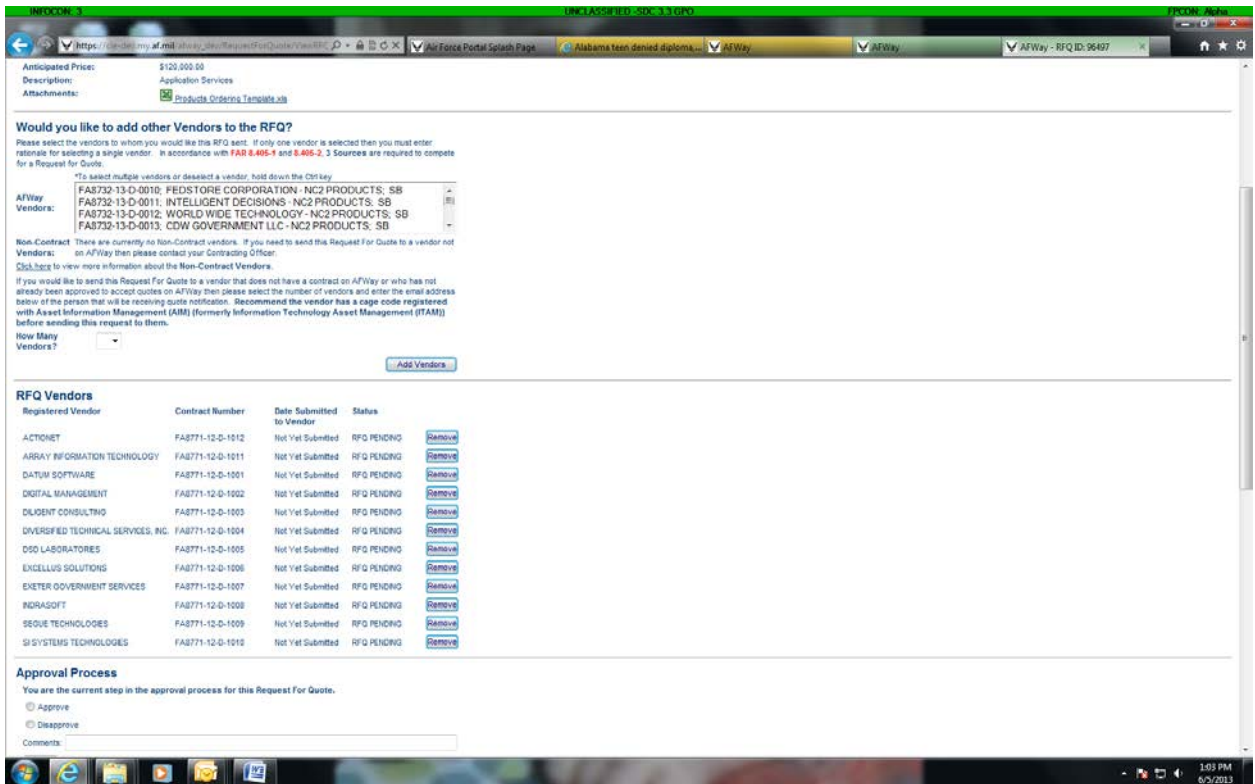
Figure 10

f. Once approved by the CO, the vendors will receive an e-mail notification alerting them of a new RFQ for action. When a vendor submits a response for solution or chooses to decline, the customer originating the RFQ will receive an e-mail notification.

Note: Once the vendor submits a solution it cannot be re-submitted. To accomplish an amendment to an RFQ already posted, the customer must submit a new RFQ in AFWAY and reference the old RFQ number.

The customer can view a vendor response to an RFQ by navigating to the User Profile page, clicking on the "Request for Quotes" tab, and clicking on the RFQ ID number of the respective RFQ. The RFQ page will display all RFQ information. Scroll down to view the status for each vendor, clicking on the plus sign (+) next to the vendor to expand and view their response.
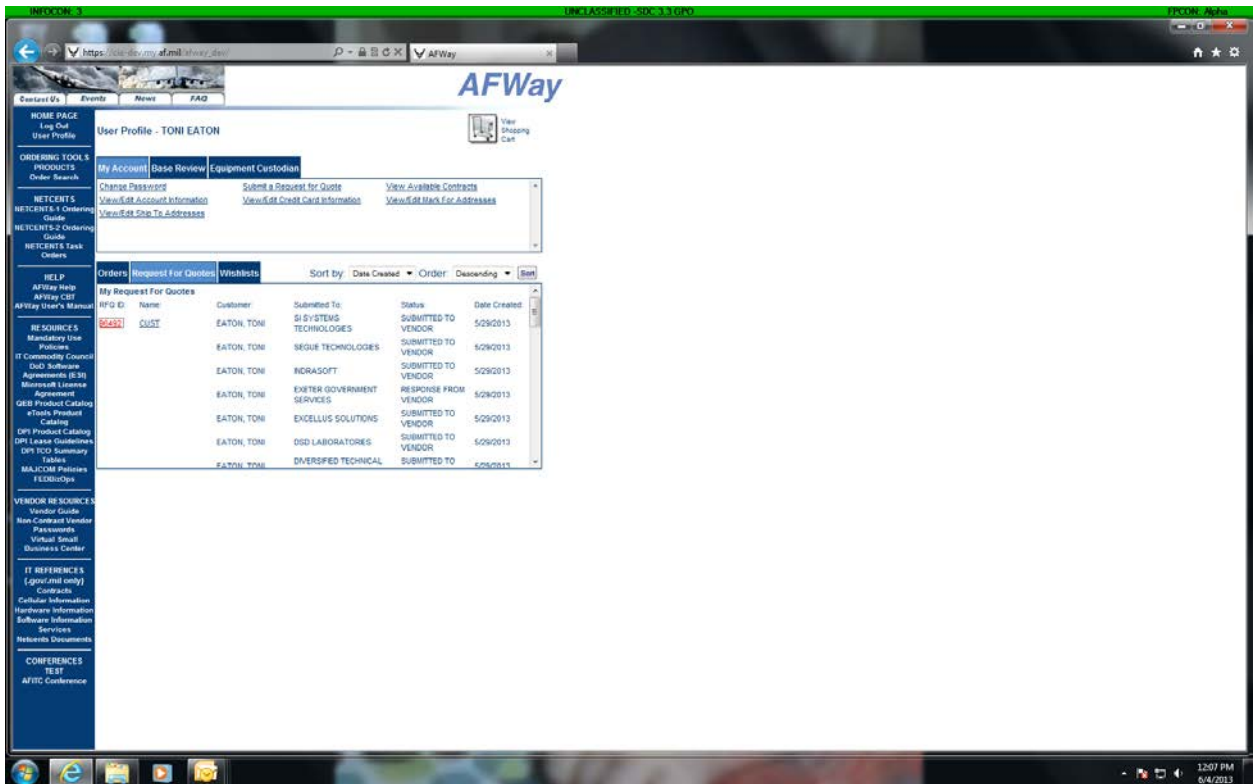
Figure 11 – RFQ Page for Submitting Information To Vendor

6. **Creating an Order Using AFWAY**

   IMPORTANT: This is step is critical for contract management and oversight. Be sure to complete this step after evaluating all proposals and selecting the one proposal that will be awarded a task order.

   a. When all of the vendors have replied to the RFQ, or once the vendor's deadline to submit a response to the RFQ has passed, the customer and respective CO should follow their local procedures to evaluate responses from vendors for the respective RFQ and determine which, if any, should be awarded as a task order.

   b. Once decided, an Order must be created in AFWay. To create an Order from an RFQ, the customer who initiated the RFQ must navigate to the User Profile page and click on the "Request for Quote" tab.

   c. Click on the RFQ ID number to open the RFQ.

   d. Click on the plus sign next to the vendor who was evaluated to have the best proposal to open their solution.
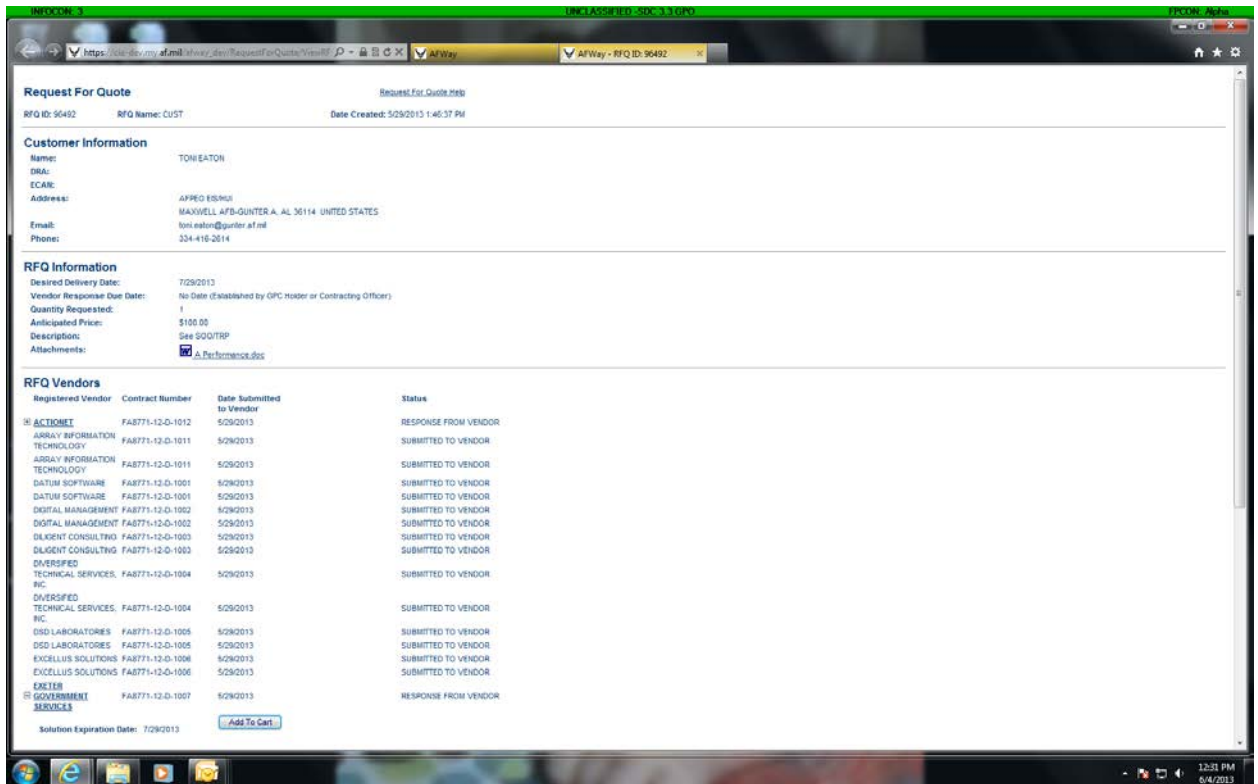
Figure 12

e. Select the Add to Cart button on the right side of the solution.

f.   The Shopping Cart will appear, populated with the solution. Click the "Checkout" button when you are ready to create the order.
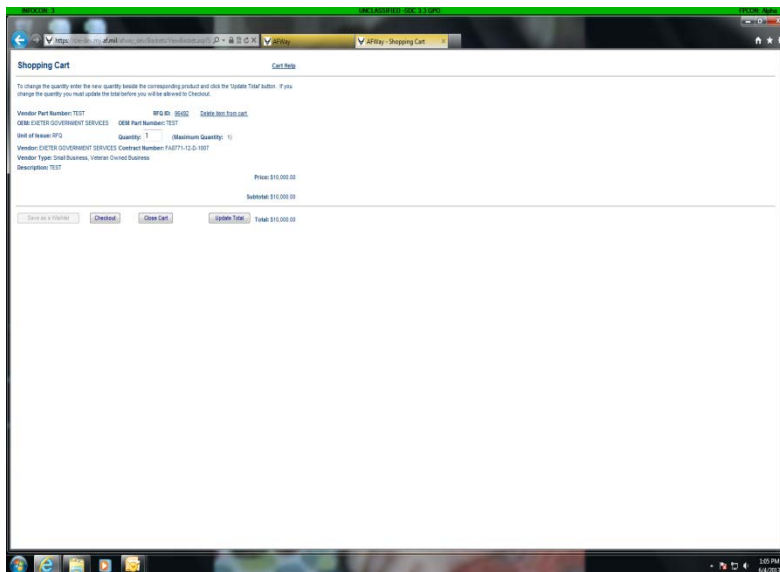
Figure 13

g. The Shopping Cart will close and you will be required to confirm the "Ship To Address" and "Mark For Address" as shown in Figure 14 below.

h. Enter any additional comments the vendor needs to be aware of. Once all information is reviewed and confirmed, click on the "Next" button.

Figure 14 – Confirm Addresses Page

i. The Process Order page will appear as shown in Figure below. Attach any documents applicable to the order and/or select the "Next" button.
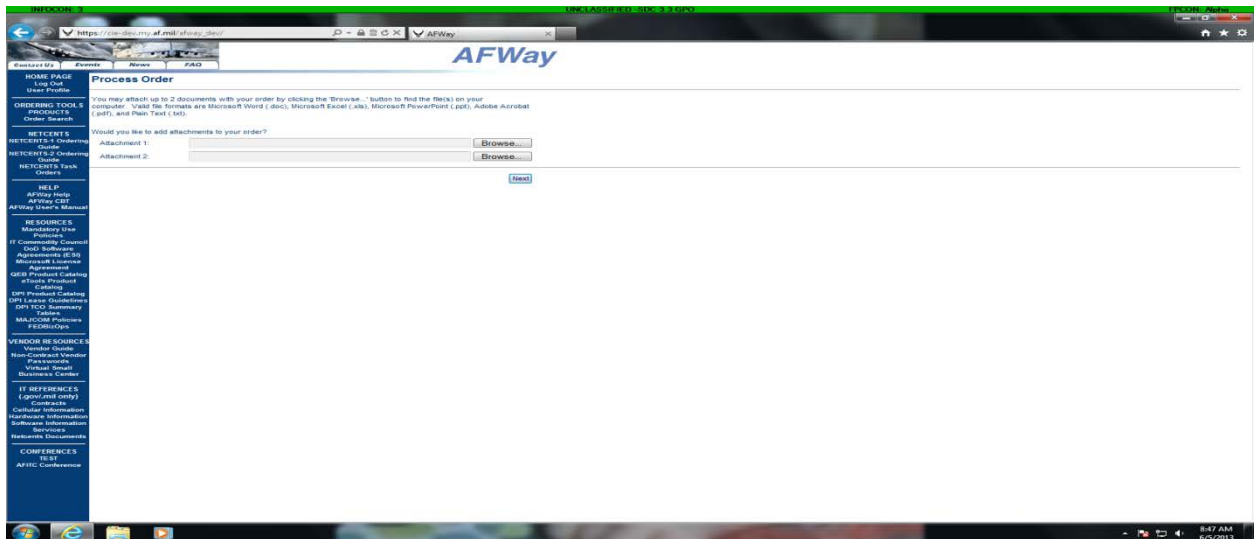
Figure 15

j. AFWay will assign an Order/Tracking number to the order. The order and status can be found on the User Profile page under the "Order" tab.

- DOD-AF Customers: the order will be routed directly to their respective CO for approval.

69

- Non-DoD AF Customers: All customers other than DoD Air Force customers will enter their own funding information, approve, and submit the order directly to the vendor.

7. *CO Instructions to Approve an Order*

The CO will receive an e-mail notification alerting them they need to approve an order in AFWay. The CO will login to AFWay and be directed to the default User Profile page.

a. Under the Orders tab, the CO should click on the corresponding Tracking Number to open the order and review the order for accuracy. See Figure below.
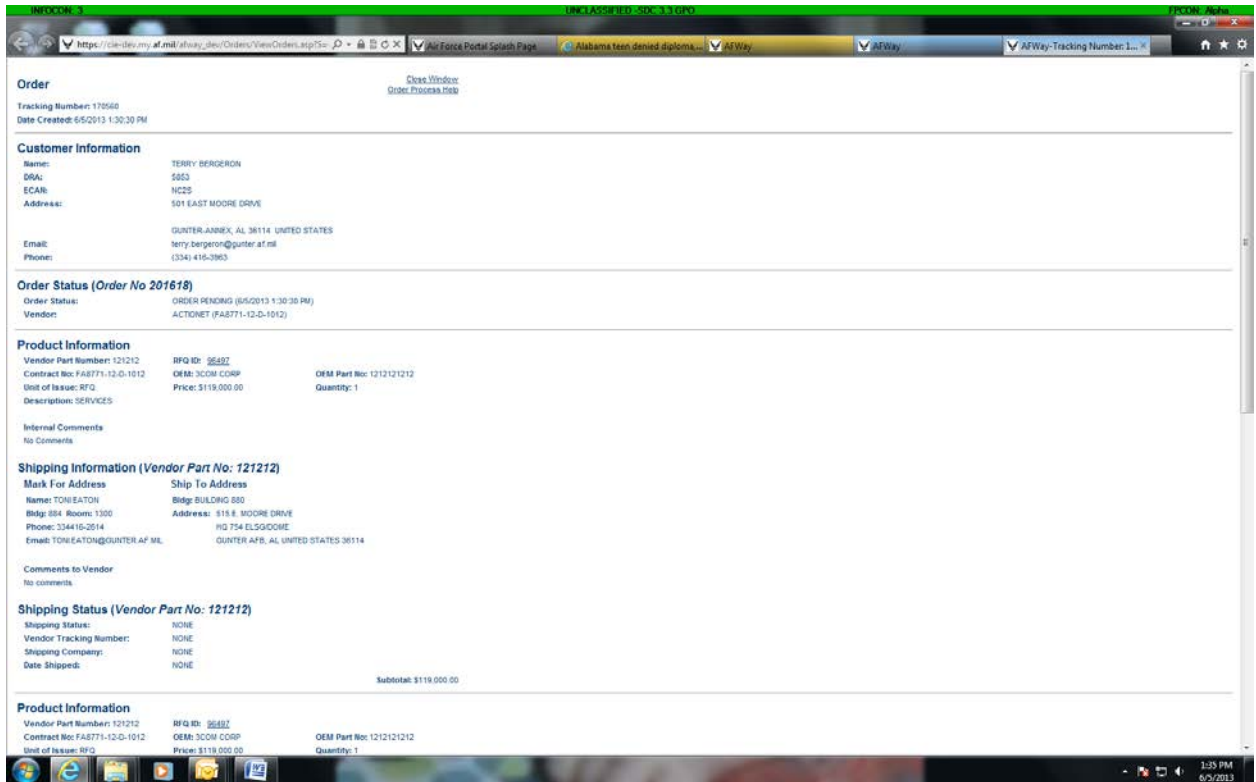
Figure 16

b. The CO can choose to approve or disapprove the order and add comments, internally and to the Vendor if necessary, and Submit.
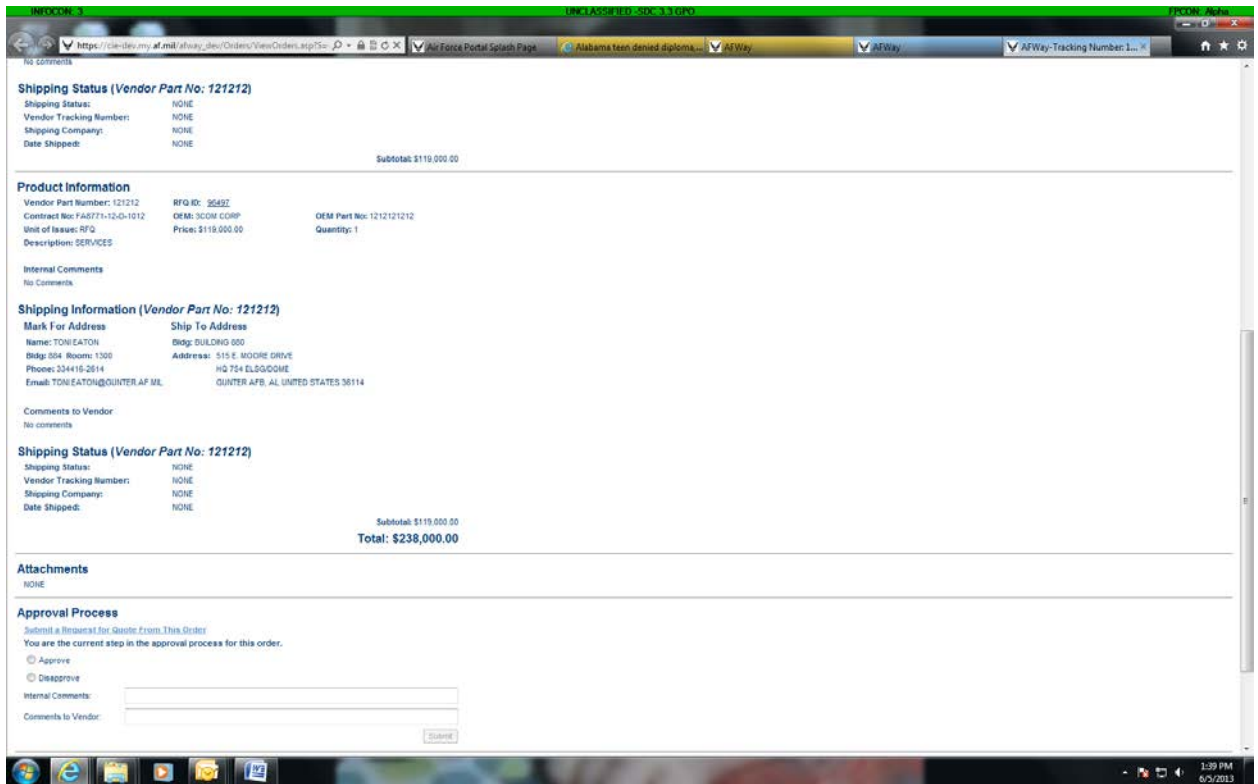
Figure 17

Next, the Enter the funding information and attach a signed copy of the contract award document that was created in your contract writing system (i.e. CONWRITE).

Click on Submit This Order.

Appendix N5: AMRDEC Safe Access File Exchange (SAFE)

SAFE can be used for free by both contractors and vendors to exchange files that exceed the AFWay 6MB size and 5 attachment documentation limits. SAFE is a simple file sharing alternative because user accounts are not required; therefore, anyone can use SAFE. Please note that SAFE is not a permanent repository and files will remain for a 14-day maximum.

- SAFE is an alternative for the contracting community to send large files to vendors and for vendors to send large files to contracting officers.

- SAFE is a file sharing system hosted by the Army at Redstone Arsenal.

- Users can upload 25 documents with a total 2GB limit.

- SAFE has an ATO from the Army and has 128-bit encryption security.

   --Approved by Army IO to share FOUO and Privacy Act files.

-How to use SAFE

- Enter email address

   - If using an email other than .mil or .gov, the sender will receive an email and must complete a verification step. All .mil or .gov email addresses are seamless

   - Upload documents (files are virus scanned)

   - Enter recipient's email (multiples allowed)

   - Optional to add FOUO or Privacy Act Statement

   - Recipient receives email notification with URL and password

   - The email is not unsafe, if the user would email the documents anyway, no harm

   - Recipient can view and download files

   - Senders can receive email notification of recipient's download

- SAFE is not a permanent repository, there is a 14 day maximum files are available; afterwards, they are purged and no longer visible.

- SAFE was tested with notification times of less than 15 minutes.

- SAFE URL https://safe.amrdec.army.mil/safe2/Welcome.aspx

- See the attached User's Guide for more information.

SAFE User's Guide

For senders:

1. Go to URL https://safe.amrdec.army.mil/safe2/Welcome.aspx

2. Click OK on the "consent banner"

3. For COs, click the CAC user link (see figure 1)

   For vendors, click the guest user link (see figure 1)

4. Select the CAC credential for "email" and enter your PIN

5. Enter your name (see figure 2 for next steps)

6. Enter your email address twice (one for verification)

7. Enter a description of the file

8. Click the Browse button to locate and upload your file. Repeat as needed for multiple files.

9. Optional – The deletion date defaults to the maximum date of 14 days. You can lower this date.

10. Enter the email address of the intended recipient and click Add. Repeat as needed for additional recipients.

11. Optional – Select any caveats such as FOUO or Privacy Act statements

12. Optional – Select notification settings and additional security settings

13. Click Upload and I Agree on the SAFE Usage banner and you're finished

For recipients:

1. You will receive an email from AMRDEC (see figure 3)

2. Copy the included password (see figure 3)

3. Click on the provided URL (see figure 3)

4. Paste the password in the box (see figure 4)

5. Click on the file(s) to open or save the file(s) (see figure 5)
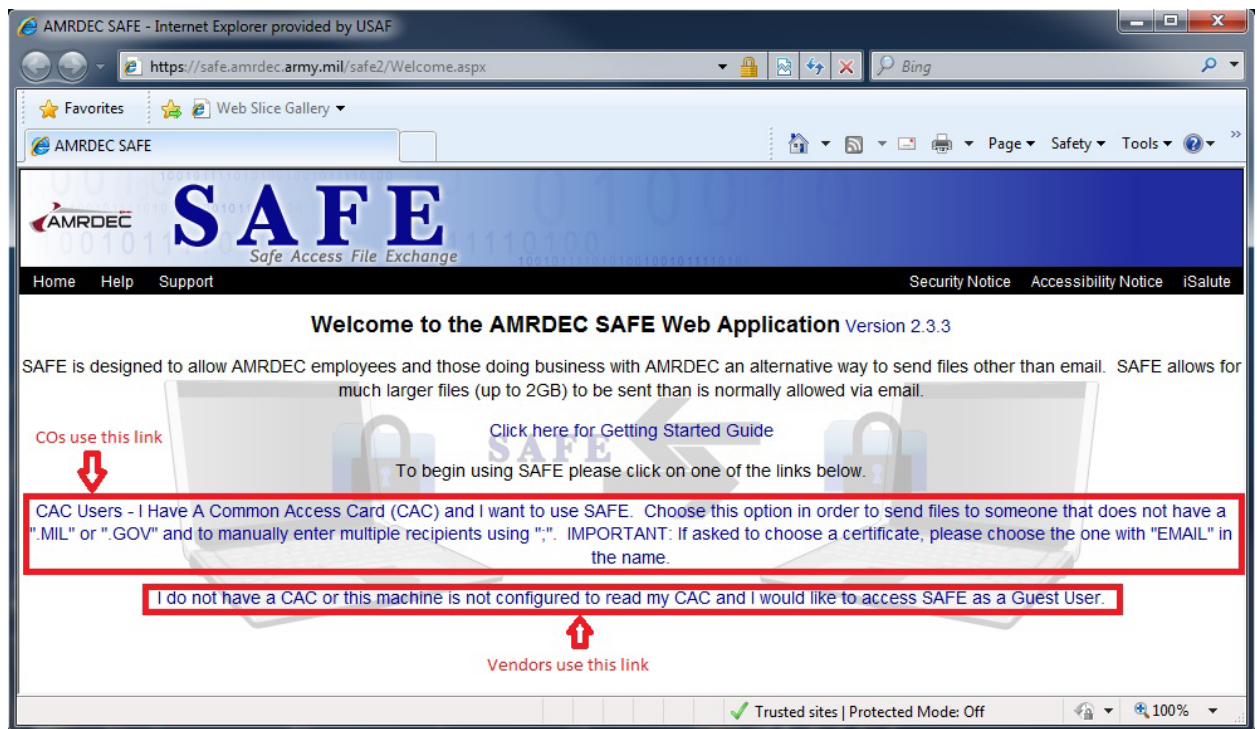
Figure 1
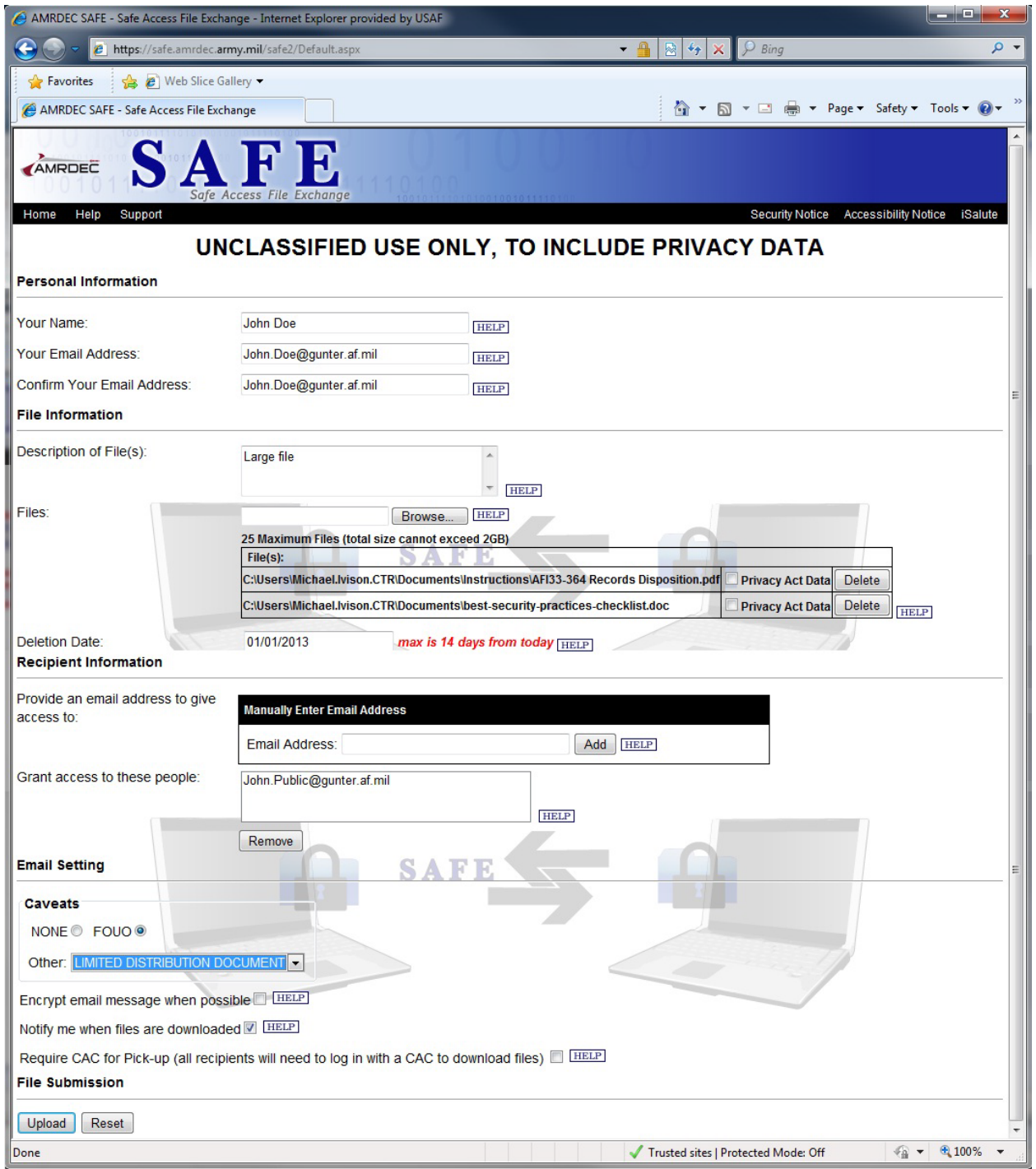
Figure 2
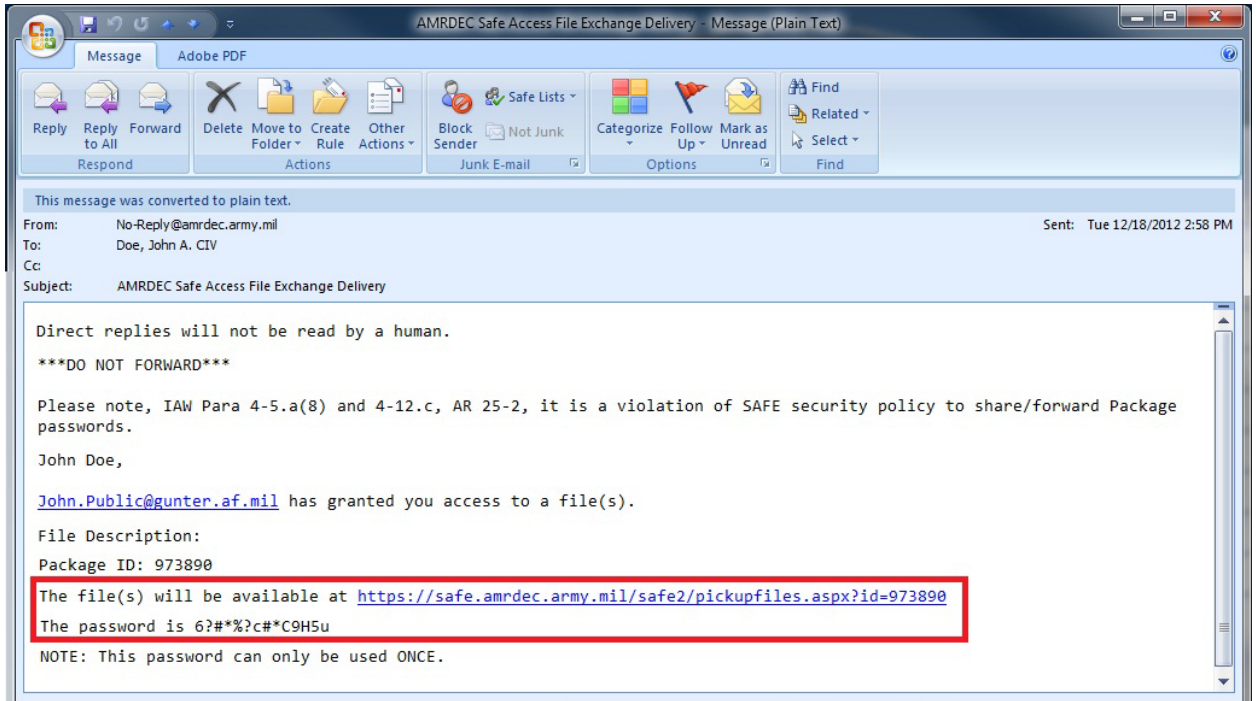
Figure 3
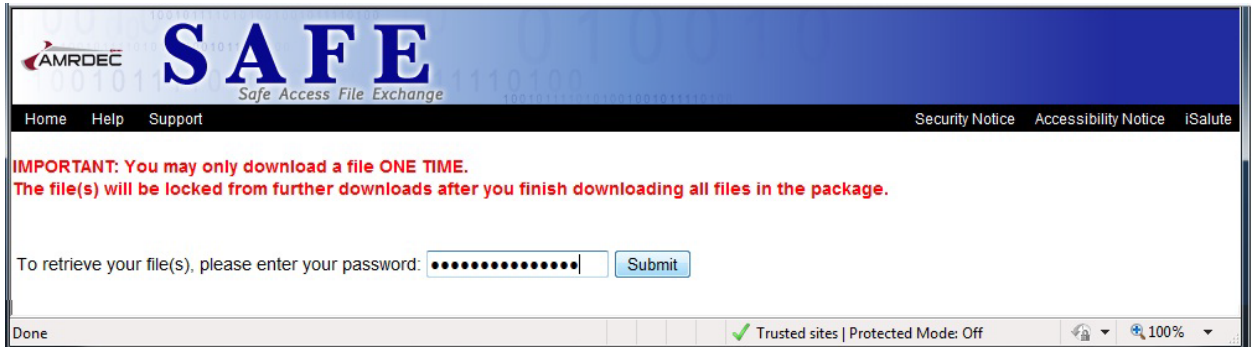
Figure 4
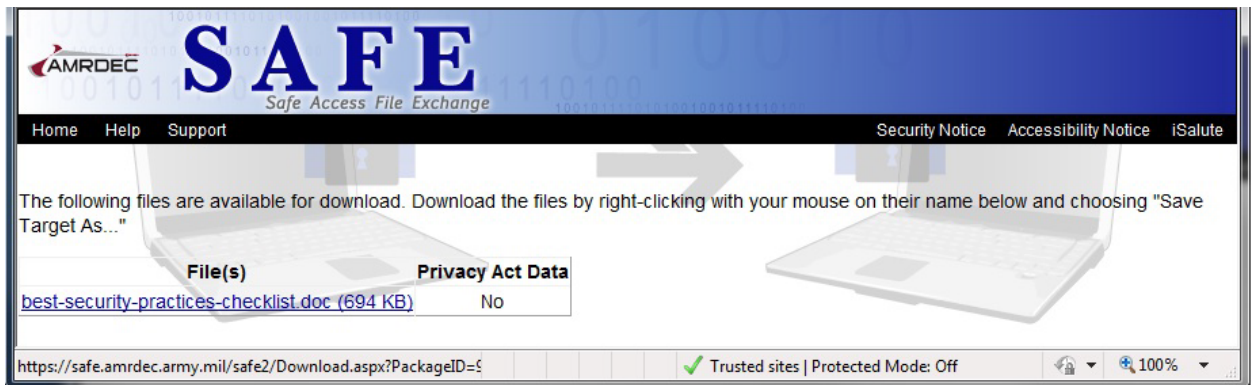
Figure 5

Appendix N6: NETCENTS-2 RSS Feed Instructions

1. **Go to** http://www.netcents.af.mil/contracts/netcents-2/index.asp

2. Select "View All RSS" at the top right of the page.

3. Select "NETCENTS" in the "News Feed" category.
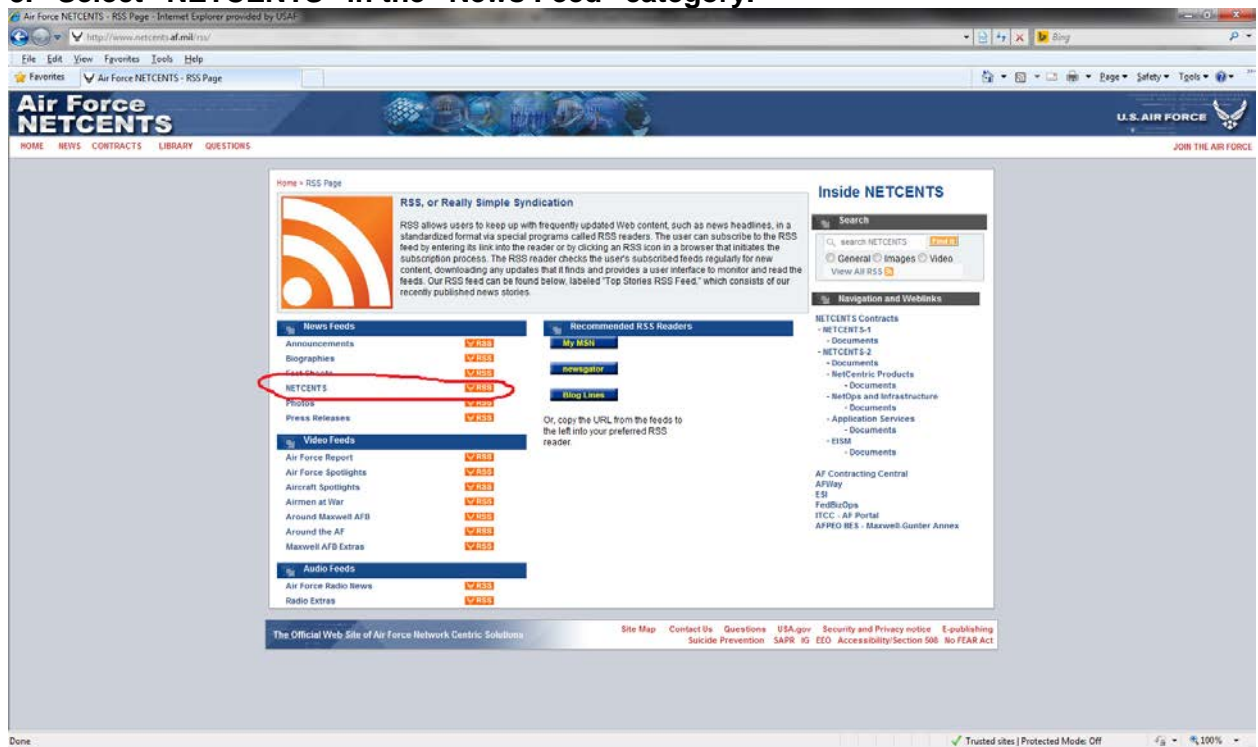
4. Highlight your Browser URL and select "Copy", by right-clicking your mouse or hitting "Ctrl-C" on your keyboard.

5. **In Microsoft Outlook, right-click on "RSS Feeds" in your left navigation pane (between "quarantine" and "Search Folders") and select "Add a new RSS Feed."**
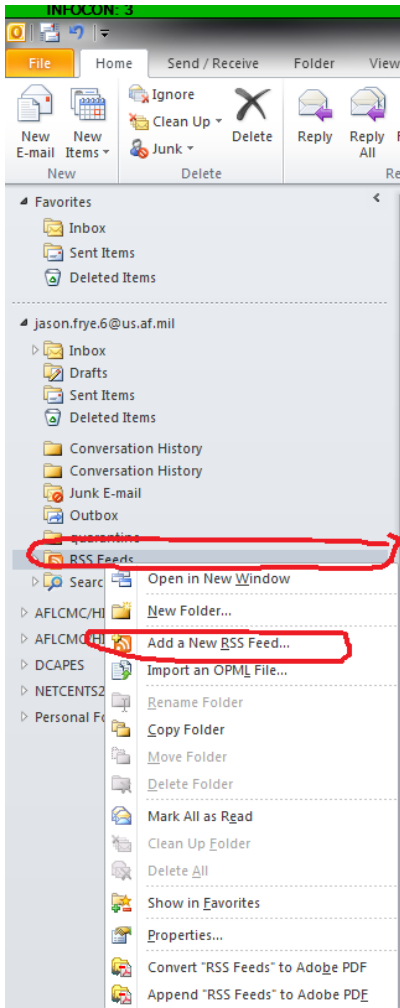
6. **Paste the URL into the Outlook dialog box using "Ctrl-V" on your keyboard. Right-clicking does not appear to work a/o 20 Nov 14 in Outlook 2010.**

7. **Select "Yes" for any "subscribe to only a RSS feed that you trust" message that is displayed.**

8. You will now receive updates when we post new documents for any of the NETCENTS-2 ID/IQs to our website.
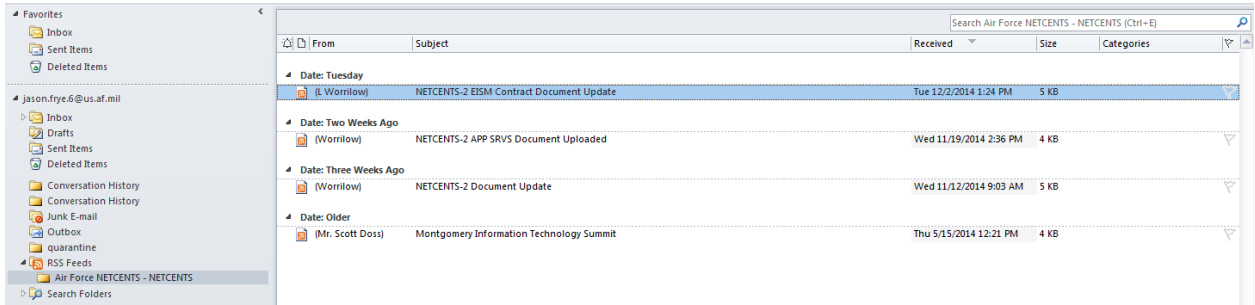
Appendix N7: Example FAR 16 RFP with Evaluation Criteria

MEMORANDUM FOR: [NETWORK OPERATIONS & INFRASTRUCTURE SOLUTION SB] CONTRACT HOLDERS

FROM: ORGANIZATION

SUBJECT: Request for Proposal (RFP) ### for XXX REQUIREMENT

1. This is a Request for Proposal (RFP) for XXX Requirement. This requirement is being solicited in accordance with the NETCENTS-2 Network Operations & Infrastructure Solution Small Business Companion IDIQ contracts awarded DD MMM YYYY.

2. The following documents are provided for preparation of a proposal. [THESE ARE ONLY EXAMPLES, INCLUDE AS APPROPRIATE TO YOUR REQUIREMENT]

   a. Performance Work Statement

   b. Instructions to Offerors and Evaluation Criteria

   c. Contract Data Requirements Lists (CDRLs)

   a. Spreadsheet format for labor categories, hours, and price.

3. Offerors must include the following representations and certifications specific to this task order with their proposals. If an identified representation or certification is addressed in the System for Award Management (SAM), the offeror shall so state. [THESE ARE ONLY EXAMPLES, INCLUDE AS APPROPRIATE TO YOUR REQUIREMENT]

   a. DFARS 252.225-7020 – Trade Agreements Certificate (Jan 2005)

   b. DFARS 252.225-7035 – Buy American – Free Trade Agreements – Balance of Payments Program Certificate (Jun 2012)

4. Clauses in the ID/IQ contract that apply to the FFP CLINs [or CR CLINs] and to all contract types are incorporated into the task order. The following clauses in the IDIQ requiring fill-ins are completed as follows:

   b. FAR 52.203-14 Para (b)(3) Any required posters may be obtained from XXXXX

   c. FAR 52.215-21 Alt I Para (b)(1) data shall be included as described in 15.408

5. Proposals may be submitted electronically or hand-carried to the Contracting Officer. Proposals are due no later than XXX and must conform to the requirements of this RFP and its attachments.

6. This is a Firm Fixed-Price requirement and will utilize CLINs 0010, 0060, and 0070 as indicated in the attached documents.

7. The anticipated acquisition schedule is as follows:

   a. Proposals Due XXX

   b. Contract Award XXX

c. Contract Performance Begins ==XXX==

8. This RFP is not authorization to begin performance, and in no way obligates the Government for any costs incurred by the contractor for this requirement. The Government reserves the right not to award a task order in response to this RFP. Prior to commencement of any activities associated with performance of this requirement, the Government will issue a written directive or contractual document signed by the Contracting Officer with appropriate consideration established.

9. Questions regarding this RFP are due no later than ==XXX== and shall be submitted to the Contracting Officer at ==email address== with a courtesy copy to the Contract Specialist ==XXX== at ==email address==.

==XXX==
Contracting Officer

Attachments: [==LIST AS APPROPRIATE TO YOUR REQUIREMENT==]

1 - Performance Work Statement

2 – Instructions to Offerors and Evaluation Criteria

3 - Contract Data Requirements Lists (CDRLs)

4 - Spreadsheet format for labor categories, hours, and price

ATTACHMENT 2

PROPOSAL SUBMISSION INSTRUCTIONS

The contractor shall submit a written price and technical proposal for consideration before the <mark>due date and time</mark> for this RFP. Your proposal shall include the following:

A Cover Letter that provides the following information:

- Contract number
- Small Business Status/Categories as appropriate
- Company point of contact with email, phone and facsimile number
- CAGE Code
- DUNS number
- A statement that your company understands the requirements specified in the Performance Work Statement (PWS) and will meet the performance standards and requirements therein.
- A statement that your company does or does not take exception to any of the requirements of the PWS or terms/conditions of this task order.
- A spreadsheet to provide the effort (labor categories and hours) and pricing required for this task order. A format for this spreadsheet is included with this RFP package.

Contractors are to propose to the following CLIN structure for this task order:

CLIN 0010 FFP

    CLIN 0010 AA – FFP – Period of Performance ….

    CLIN 0010 AB – FFP – Period of Performance ….

    CLIN 0010 AC – FFP – Period of Performance ….

    CLIN 0010 AD – FFP – Period of Performance ….

    CLIN 0010 AE – FFP – Period of Performance ….

CLIN 0060 ODCs

    CLIN 0060 AA – ODCs – CR – Period of Performance ….

    CLIN 0060 AB – ODCs – CR – Period of Performance ….

    CLIN 0060 AC – ODCs – CR – Period of Performance ….

    CLIN 0060 AD – ODCs – CR – Period of Performance ….

    CLIN 0060 AE – ODCs – CR – Period of Performance ….

CLIN 0070 Travel

    CLIN 0070 AA – Travel – CR – Period of Performance ….

    CLIN 0070 AB – Travel – CR – Period of Performance ….

    CLIN 0070 AC – Travel – CR – Period of Performance ….

    CLIN 0070 AD – Travel – CR – Period of Performance ….

    CLIN 0070 AE – Travel – CR – Period of Performance ….

EVALUATION CRITERIA

The Government anticipates awarding a task order to the offeror whose proposal provides the best value to the Government, price and other factors considered, and award may be made to other than the most highly rated or lowest priced proposal. Proposals will be evaluated based on the factors described below.

The Government will evaluate proposals based on the following factors:

- Technical

    - Labor (Mix, Skill Sets, and Hours/FTEs)

    - Discriminators

    - Experience

• Price

• Assumptions, Conditions, and Exceptions

NOTE: Any exception to the solicitation may render a proposal unacceptable.

TECHNICAL:

LABOR:

Describe your plan to both staff and manage the services required in the PWS.
Include information detailing labor category descriptions, skills matrix, and effort required (hours/FTEs) in support of task requirements.

At a minimum, proposed personnel will be evaluated based on the skills deemed by the Government to be necessary to successfully complete the requirements in the PWS.

Define Necessary Skillsets Here and/or Reference Appropriate PWS Paragraphs.

DISCRIMINATORS:
Offerors shall provide the technical methodology/approach to be used in performing the requirements of the PWS for the following technical discriminators.
[THESE ARE ONLY EXAMPLES – Use Discriminators appropriate to your requirement]

a) Creating and storing metadata IAW DDMS v1.0.

b) Replacing point to point interfaces by exposing data via web services.

c) Ensuring applications for mobile devices are platform independent (can run on standard mobile devices – Apple/Android/Microsoft)

Offerors must specifically identify the approach/technology proposed, along with the standards utilized and the tools and methodologies of how the solution/approach is developed. The Government will evaluate the approach/solution to ensure it is viable. The characteristics of viable solutions (in conjunction with the other evaluation factors) will be used to determine the proposal which provides the best value to the Government.

The Service Delivery Summary identifies the performance standards (key and essential tasks) by which the successful contractor will be measured. The labor/effort and technical discriminators proposed must reflect an understanding of these requirements.

EXPERIENCE

Describe three projects your company has completed, within the last three years, which reflect your company's ability to perform the discriminator items in this RFP. Each customer reference shall include a contracting and technical point of contact along with email address, phone number, and title.

The Government may supplement the experience information provided with information concerning your performance from any other reliable source including its own experience with your company.

PRICE

In the spreadsheet provided, list all labor categories and hours necessary to fulfill the requirements of the PWS. [For a FFP Task Order – For a CR Task Order, include hourly rates, indirect rates/costs, and fee]. If applicable, include costs for travel (include pricing for per diem, air fare, rental car, etc.) and ODCs in accordance with the NC-2 CLIN structure. Provide pricing for each CLIN identified for the initial period of performance and each of the option periods.

Identify your G&A rate for Prime and Sub in order to allow for evaluation of total cost for travel and ODC prices. ODC's in direct support of this task order shall be approved by the Contracting Officer prior to purchase and shall be purchased in accordance with the terms of the basic IDIQ contract.

For award purposes, the Total Evaluated Price (TEP) is the price proposed for base year requirements (basic award) and all options periods identified in the RFP.

Prices will be evaluated for reasonableness [and realism for CR TO]. Prices which are excessively high [or low] may be considered [unrealistic and] unreasonable and may receive no further consideration.

ASSUMPTIONS, CONDITIONS & EXCEPTIONS

NOTE: Any exception to the solicitation may render a proposal unacceptable.

If your company takes exception to any of the requirement of the PWS or terms/conditions of this task order, they must be clearly identified in your proposal.

These will be reviewed for potential impact on your ability to successfully meet the Government's requirements. Any assumptions, conditions or exceptions which may negatively impact performance of this requirement could render the proposal ineligible for award.