ORDER FOR SUPPLIES AND SERVICES	IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution	PAGE 1 OF 1 PAGE(S)

1. DATE OF ORDER	2. ORDER NUMBER	3. CONTRACT NUMBER	4. ACT NUMBER
07/13/2018	47QFWA18F0034	FA8771-12-D-1007	A21918595

FOR GOVERNMENT USE ONLY	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 285F	ORG CODE Q07FA000	B/A CODE AA20	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE AF151	C/E CODE H08	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT		AI	LC	DISCOUNT

7. TO: CONTRACTOR *(Name, address and zip code)*
[redacted]
EXETER GOVERNMENT SERVICES, LLC
9841 WASHINGTONIAN BLVD STE 400
GAITHERSBURG, MD 20878-5389
United States
[redacted]

8. TYPE OF ORDER
B. DELIVERY

REFERENCE YOUR

Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.

This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.

C. MODIFICATION NO.
P00000
TYPE OF MODIFICATION:

AUTHORITY FOR ISSUING

9A. EMPLOYER'S IDENTIFICATION NUMBER
[redacted]

9B. CHECK, IF APPROP WITHHOLD 20%

Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.

10A. CLASSIFICATION
Veteran Owned Business

10B. TYPE OF BUSINESS ORGANIZATION
P. Partnership

11. ISSUING OFFICE *(Address, zip code, and telephone no.)*
GSA Region 07
LATASHA GOINES
819 Taylor St
Fort Worth, TX 76102-0000
United States
817-978-3075

12. REMITTANCE ADDRESS *(MANDATORY)*
EXETER GOVERNMENT SERVICES, LLC
9841 WASHINGTONIAN BLVD.
GAITHERSBURG,MD 20878-5389
United States

13. SHIP TO*(Consignee address, zip code and telephone no.)*
Crystal Palacios
1960 1ST STREET WEST
BLDG, 977, STE D101
JBSA RANDOLPH, TX 78150-4453
United States
210-565-2509

14. PLACE OF INSPECTION AND ACCEPTANCE
Crystal Palacios
1960 1ST STREET WEST
BLDG, 977, STE D101
JBSA RANDOLPH, TX 78150-4453
United States

15. REQUISITION OFFICE *(Name, symbol and telephone no.)*
Hunter R Lynch
819 TAYLOR ST
FORT WORTH, TX 76102-6124
United States
(817) 585-2703

16. F.O.B. POINT	17. GOVERNMENT B/L NO.	18. DELIVERY F.O.B. POINT ON OR BEFORE 07/12/2019	19. PAYMENT/DISCOUNT TERMS NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS
Destination			

20. SCHEDULE

ITSS Project Number: ID07180006
ACT#: A21918595

a. This is a hybrid T&M and firm fixed priced task order issued under the Air Force NETCENTS-II Application Services Contract FA8771-12-D-1007. The task order consists of a Base and four Option Years.

This is a severable requirement.

The contractor's revised Technical proposal (dated June 12, 2018) and revised Pricing (dated June 12, 2018) are hereby fully incorporated into the awarded task order.

All applicable terms and conditions from the contactor's basic NETCENTS II Indefinite Delivery Indefinite Quantity (IDIQ) Contract, and the additional terms of this task order, shall become legally binding upon the contractor at the time of award and through the period of performance.

The contractor shall provide all labor and services in accordance with the Performance Work Statement (PWS) and the proposal provided by the contractor on the date stated above. The Government is not obligated to reimburse the contractor for costs incurred in excess of the total amount awarded on this task order, and the contractor is not obligated to continue performance under this task order or otherwise incur costs in excess of the work requirements outlined in the finalized PWS dated 18 May 2018, the contractor's proposal, and this FM300.

The total dollar amount for the Base Year is $7,980,166.56 (detailed below to include travel). Incremental funds will be added to this task as they become available. Incremental funding shall be added bilaterally via the changes clause at FAR 52.212-4(c), Changes. The CLIN ceilings are allocated as followed:

Base Year Labor-FFP: [redacted]
Base Year Labor-T&M: [redacted]
Base Travel: [redacted]
Base Year Total: [redacted]

The contractor is not authorized to incur additional costs above and beyond those costs that have been funded by the Contracting Officer under the terms of this order, which is [redacted]. The contractor shall notify the Contracting Officer once 75% of the current funded amount for the Base Year has been expended.

Changes to this order shall be made in writing only, and shall not be made by anyone other than the Contracting Officer.

b. Period of Performance and Awarded Amounts

Base Year: July 13, 2018 to July 12, 2019
Option Year 1: July 13, 2019 to July 12, 2020
Option Year 2: July 13, 2020 to July 12, 2021
Option Year 3: July 13, 2021 to July 12, 2022
Option Year 4: July 13, 2022 to July 12, 2023

Base Year Labor-FFP: B-4
Base Year Labor-T&M: B-4
Base Travel: B-4
Base Year Total: B-4

Option Year 1 Labor-FFP: B-4
Option Year 1 Labor-T&M: B-4
Option Year 1 Travel: B-4
Option Year 1 Total: B-4

Option Year 2 Labor-FFP: B-4
Option Year 2 Labor-T&M: B-4
Option Year 2 Travel: B-4
Option Year 2 Total: B-4

Option Year 3 Labor-FFP: B-4
Option Year 3 Labor-T&M: B-4
Option Year 3 Travel: B-4
Option Year 3 Total: B-4

Option Year 4 Labor-FFP: B-4
Option Year 4 Labor-T&M: B-4
Option Year 4 Travel: B-4
Option Year 4 Total: B-4

Total Base plus four Option Years: B-4

c. Option periods were evaluated at the time of contract award. The option periods included in this task shall be exercised in accordance with FAR clauses 52.217-8 and 52.217-9. Options shall be exercised at the discretion of the Government, within the terms expressed in the aforementioned clauses. Options shall be exercised at the dollar values accepted in the contractor's revised quote dated June 12, 2018 at the time of award.

POC: Latasha M. Goines, Contracting Officer, 817-978-3075, latasha.goines@gsa.gov

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	Base Year-Labor-T&M	1	lot	B-4	B-4
0002	Base Year -Labor-FFP	1	lot	B-4	B-4
0003	Base Year-Travel	1	lot	B-4	B-4

21. RECEIVING OFFICE *(Name, symbol and telephone no.)* AIR FORCE PERSONNEL OPERATIONS ACTIVITY, 210-565-2509		**TOTAL From 300-A(s)**
22. SHIPPING POINT Specified in QUOTE	23. GROSS SHIP WT.	**GRAND TOTAL** B-4
24. MAIL INVOICE TO: *(Include zip code)* General Services Administration (FUND) The contractor shall follow these Invoice Submission Instructions. The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).	25A. FOR INQUIRIES REGARDING PAYMENT CONTACT: GSA Finance Customer Support	25B. TELEPHONE NO. 816-926-7287
	26A. NAME OF CONTRACTING/ORDERING OFFICER*(Type)* LATASHA GOINES	26B. TELEPHONE NO. 817-978-3075
	26C. SIGNATURE LATASHA GOINES 07/13/2018	
GENERAL SERVICES ADMINISTRATION	**1. PAYING OFFICE**	**GSA** FORM **300** (REV. 2-93)

General Services Administration (GSA)

Greater Southwest Region

Task Order #ID07180006

IT Operations Support Services

for the

Air Force Personnel Operations Activity (AFPOA)

Performance Work Statement (PWS)

Under

NETCENTS-2 Application Services

as of April 16, 2018

This PWS is the finalized version to be used for the purposes of award and incorporates changes as a result of RFQ questions received 10 April 2018.

1. Purpose

AFPOA provides robust information technologies supporting the human resource needs of Total Force commanders and Airmen on behalf of Air Force (AF)/ A1. AFPOA acquires and maintains IT systems that support the AF/A1 mission and the operations at HQ Air Force Personnel Center at Joint Base San Antonio - Randolph, TX. The AF/A1 mission is to deliver a global 24/7 Total Force personnel service capability providing integrated, standardized systems that are easy to access and use.

2. Scope

The Air Force Personnel Operations Activity requires Application Services support through the Air Force NETCENTS contract vehicle for network-centric IT, networking equipment, and support services to specific mission areas identified by the Air Force Personnel Operations Activity (AFPOA). The scope of this requirement is to acquire IT support services in the following task areas:

Task 1: Program Management
Task 2: Requirements Support
Task 3: Field Support
Task 4: Operations & Data Center Support
Task 5: Cybersecurity and Software Management Support
Task 6: Lifecycle Management Support

3. Requirements

The Contractor shall provide the following services:

3.1. <u>Task 1 Program Management (CLIN 0001 / NETCENTS CLIN 1100/1300)</u>: The Contractor shall apply requisite technical and management skills and techniques to assure satisfactory, timely completion of program milestones, and establish project controls reporting systems which will provide routine and realistic assessments of the program progress through the end of life cycle period as measured against the project control documents and detailed work plan.

3.1.1. Kick-Off Meeting: The Contractor shall schedule, coordinate, and host a Kick-Off meeting at a location approved by the Government no later than 14 days from award. The meeting will provide an introduction between the Contractor personnel and Government personnel. The meeting will provide the opportunity to discuss technical, management, security logistics and travel authorizations and reporting procedures. At a minimum, the attendees shall include representatives from the AFPOA Directorates, Contracting Officer, Contracting Officer Representatives, General Services Administration/Direct Client Support Representative and other relevant Government personnel.

3.1.2. Monthly Status Report (MSR): The Contractor shall provide a MSR for all tasks describing all service level metrics required throughout this PWS, status of execution under the contract, any known contract issues or deficiencies, expected information or support required from the Air Force, high level funding status (where appropriate), and a risk matrix with details on medium/high risks. The Contractor shall submit an individual MSR for each task to the Program Manager for each associated PWS task. The Contractor shall distribute the MSR for work efforts assigned by the 5th business day of the month.

3.1.2.1. The MSRs shall include:

3.1.2.1.1. Progress since last report.

3.1.2.1.2. Risks that may delay the work effort's completion and proposed solutions.

3.1.2.1.3. Steps to accomplish each work effort, percentage complete status, and the target date for each work effort's completion.

3.1.2.1.4. Concerns, issues, delays, risks, and proposed resolutions of identified problems or concerns.

3.1.2.1.5. Project activities, Key Personnel, and planned expenditures by task/subtask for the next month.

3.1.2.1.6. Personnel changes that impact ability to execute/perform responsibilities.

3.1.2.1.7. Changes to the program management plan and/or the quality control plan.

3.1.2.1.8. For each employee: labor category, hours worked (denoting on or off site), and cumulative hours worked.

3.1.2.1.9. Problem Notification Reports.

3.1.2.1.10. List of applications/systems/software management status and estimated completion date.

3.1.2.1.11. Issues affecting system accreditation and authorization and software management (include description, impact and recommended solution)

3.1.2.1.12. Any changes to requirements with description of issues that impact ability to execute/perform responsibilities as outlined.

3.1.2.1.13. Identifying Contractors trained, subject matter, and date trained.

3.1.2.1.14. Required deliverables and the timeframe for their delivery are located in Section 6.0, Table 1 of this PWS.

3.1.3. Program Management Plan: The Contractor shall submit a program management plan describing the overall methods used to meet the PWS requirements. This document is an evolutionary document that will be reviewed and updated throughout the lifecycle of this requirement. This will include partnering and subcontracting plans and identifying the tasks that they will be performing. The Plan must be kept current. It shall be re-submitted for approval as described in the Deliverables Schedule in Section 6 whenever any changes result in a schedule impact.

3.1.4. **Schedule**: The Contractor shall submit a schedule for major tasks in the PWS. This shall include all specific instances in the PWS where a specific date or days are award are identified.

3.1.5. **Quality Control Plan**: The Contractor shall submit a quality control plan detailing how the Contractor will ensure quality products and services are provided to the Government. The plan shall be provided 30 days after task order award. This document is an evolutionary document that will be reviewed and updated throughout the lifecycle of this requirement.

3.1.6. **Meetings**: The Contractor shall provide meeting support and shall accomplish the following:

3.1.6.1. Participate in status meetings, not more than once a week, to review current and planned activities for the major task areas.

3.1.6.2. Prepare an "Activity Report Brief" at least one business day prior to the Status Meeting that details the results and planned actions for the Contractor's team supporting the tasks. Typical topics may include status, stoplight charts, and planned acquisitions and changes/updates to the program management plan. The information in this report shall be considered the foundation for the monthly status reports.

3.1.6.3. Conduct and/or attend monthly program reviews to present status of tasks.

3.1.6.4. Conduct and/or attend initial Assessment and Authorization (A&A) and Government requested software management task kick-off meetings and weekly meetings thereafter to present ongoing project status until each project is completed (Applicable to the A&A Task).

3.1.6.5. Required deliverables and the timeframe for their delivery are located in Section 6.0, Table 1 of this PWS.

3.2. **<u>Task 2 Requirements Support (CLIN 0001/ NETCENTS CLIN 1300)</u>:** The Contractor shall support the following Requirements Division (DFR) tasks:

3.2.1. **Commanders Tool Kit (CCTK):** The Air Expeditionary Force (AEF) Online; CCTK provides commanders with an effective way to monitor and manage their unit's deployment readiness and provides Airmen with a single-point access for requisite deployment readiness information within the Personal Deployment Preparedness Tool (PDPT) via AEF Online. The User Management System (UMS) application provides a common login experience and user management tool for all applications. The Deployment Readiness Checklist (DRC) application allows online mobility processing at the unit, along the travel path, and at the deployed location. The Online Mobility Folder (OMF) application provides the ability to electronically store and transfer numerous documents that are needed for mobility processing eliminating the need to carry these documents by hand.

3.2.2. **Application Development**: The Contractor shall provide application developers in support of the CCTK mission. The Contractor shall possess and maintain a Department of Defense (DOD) 8570 Cyber Security certification in support of the CCTK mission. The Contractor shall have upon hire and maintain SECRET security clearance.

The Contractor shall:

3.2.2.1. Provide a Senior Application Developer who provides leadership and management support for Contractor personnel assigned in support of the Application Development task. The Senior Application Developer shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service.

3.2.2.2. Develop code modules in C-Sharp programming language using Microsoft Visual Studio to provide new functionality (requirements), modify, correct, and refactor defect or bug fixes for the CCTK, PDPT, UMS, DRC, and the OMF applications within AEF Online IAW software engineering practices provided by the government and according to direction provided by the government lead.

3.2.2.3. Develop code modules in Standard Query Language (SQL) using SQL Server Management Studio to provide new functionality (requirements) and defect/bug fixes for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online IAW software engineering practices provided by the government and according to direction provided by the government lead.

3.2.2.4. Analyze requirements for new functionality and defects or bugs and then provide an estimate of the Level of Effort (LOE), a delivery date that would be required, and the approximate length of time it would take to design, develop, test, and field code that implements this new functionality, or defect or bug fix in the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

3.2.2.5. Analyze, troubleshoot and provide technical solution for new functionality (requirements) in order to design, develop, test, and field code that implements this new functionality for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

3.2.2.6. Analyze, troubleshoot and provide defect resolution and brief the results to the government lead for defects/bugs in order to design, develop, test, and field code that fixes the defect or bug for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

3.2.2.7. Communicate and brief system requirements, system capabilities, system limitations and risks with customers and senior leadership.

3.2.2.8. Quantify, categorize, and describe user requirements in a manner that enables the government to make an informed decision regarding the performance of new functionality.

3.2.2.9. Use government approved Commercial-Off-The-Shelf (COTS) tools such as Visio and PowerPoint or all other tools for systems design and

development for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

3.2.2.10. Ensure all developed code receive Risk Management Framework (RMF) cybersecurity authorization. The Contractor shall document their findings and provide to the AFPOA Technical Points of Contract (POC).

3.2.2.11. Develop code to be device agnostic (enables the code to run on different hardware from different manufacturers) to every extent possible by not using proprietary Application Program Interface (APIs). The Contractor shall provide a list of all APIs used to the AFPOA Technical Points of Contract (POC).

3.2.2.12. Develop all code necessary to perform any Extract Transform & Load (ETL) actions necessary for proper operation of the applications. The Contractor shall provide all C# code and SQL modules used.

3.2.2.13. Create a Test Plan IAW the government provided standard to guide testing. The Test Plan shall provide the following minimum information: what to test, how to test, when to test and who will do the testing of the software requirements. The standard is IEEE829 format and additional information will be provided upon execution of the task order.

3.2.2.14. Attend all code releases when code is migrated to the test, development and production environment's which often occur after standard duty hours of 0730 to 1630 hrs. CST.

3.2.2.15. Configure data mapping details documented in the design documents.

3.2.2.16. Review and validate government acceptance of technical requirements and design documents.

3.2.2.17. Participate in and coordinate upon meeting minutes for Integrated Requirements Team (IRTs) meetings, which may be in the form of Integrated Product Team (IPT) meetings, project lead meetings, working group meetings, or other government led sessions.

3.2.2.18. Required deliverables and the timeframe for their delivery are located in Section 6.0, Table 1 of this PWS.

3.3. <u>Task 3 Field Support (CLIN 0001 NETCENTS CLIN 1100/1300)</u>: The Contractor shall provide Tier 1 troubleshooting for incoming calls and email on a continuous basis and provide support for event and change management on the AFPOA production environment. The list of applications supported is provided in Appendix B AFPOA Application List. All Contractor personnel in support of the field support task shall have upon hire and maintain a SECRET security clearance with the exception of the Business Objects task. Additionally, the Contractor shall ensure that A1 Service Desk personnel meet the requirements of DOD and AF Cybersecurity policy. The A1 Service Desk personnel perform cybersecurity activities and must have Level I certification IAW DoD 8570-01.M, Information Assurance Workforce Improvement Program (http://www.dtic.mil/whs/directives) and AFMAN 17-1303,

Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil.)

The Contractor shall:

3.3.1. Provide a Help Desk Manager who provides leadership and management support for Contractor personnel assigned in support of the Field Support task. The Help Desk Manager shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service. The Help Desk Manager shall possess the Information Assurance (IA) Technical Level II certification IAW the Workforce Improvement Program (http://www.dtic.mil/whs/directives) and AFMAN 17-1303, Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil).

3.3.1.1. Utilize existing task instructions and procedural guidelines for use in instructing newly assigned personnel and administers recurring training for Contractors performing Service Desk Support.

3.3.1.2. Ensure existing Tactics, Techniques and Procedures (TTPs) are accurate and updated as changes in processes occur. Changes and updates will be provided by and/or coordinated with the Government.

3.3.1.3. Ensure Contractors are logged in to the telephone system and available to take incoming calls 24x7x361 (362 days during leap years).

3.3.1.4. Ensure the average "Not Ready" state is ≤ 22% on a daily basis for each Contractor.

3.3.1.5. Ensure each Contractor does not exceed five (5) "Ring on No Answer" (RONA) calls during all shifts, 7 days per week.

3.3.1.6. Ensure customers do not experience long wait times (considered to be > 3 minutes) in the phone queue.

3.3.1.7. Ensure Contractors are available to provide Common Access Card (CAC) support (CAC unlocks/resets) within 3 minutes of customer arrival in the A1SD during the CONUS shift, Monday through Friday.

3.3.1.8. Notify the Dashboard Operator and all Contractors performing service desk support when customers report an unscheduled incident impacting system availability and/or accessibility. In addition, the Help Desk Manager shall ensure Contractors are notified when the incident is resolved.

3.3.1.9. Ensure a TTP or knowledge article is created and coordinated with the Government within 5 business days when new systems/applications are assigned to the A1SD.

3.3.1.10. Provide quality control reports identifying open tickets, incidents over 30 days old, tickets not assigned and requests over 30 days old on Wednesday's each week

3.3.1.11. Provide trouble ticket report identifying category of tickets created and total tickets submitted no later than the 1st Thursday of each month.

3.3.2. **Account Management**: The Contractor supporting the account management task shall possess the IA Technical Level II certification in IAW the Workforce Improvement Program (http://www.dtic.mil/whs/directives) and AFMAN 17-1303, Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil).

The Contractor shall:

3.3.2.1. Provide customers with assistance to obtain a user account required to access the Air Force Network (AFNET) in accordance with existing TTPs.

3.3.2.2. Provide the customer with the policies, forms and guidance required for new application account requests.

3.3.2.3. Review all documents submitted for access to human resource applications, ensuring information assurance certification and appropriate signatures have been obtained on required documents. The forms shall be submitted to the appropriate point of contact for processing and then stored in the account management database.

3.3.2.4. Apply established security groups to specific shared files with the appropriate permissions in shared files and the global address listing.

3.3.2.5. Ensure accounts are created accurately and troubleshoot access and connectivity issues to the Air Force network and/or supported applications.

3.3.2.6. Implement IT security policies and procedures to ensure protection of information transmitted to the installation, among organizations on the installation, and from the installation using Local Area Networks (LAN), Wide Area Networks (WAN), the World Wide Web, or other communications modes.

3.3.2.7. Limit privileged access to systems/applications (i.e., operating system, system parameter and configuration files, and databases), utilities, and security-relevant programs/data files to authorized personnel and will maintain required supporting documents for each account created in the account management database on the restricted drive.

3.3.3. **Service Desk Support.** The Contractor shall provide service desk support for all three shifts: Contiguous United States (CONUS), Pacific Air Forces (PACAF) and United States Air Forces in Europe (USAFE).

The Contractor shall:

3.3.3.1. Answer incoming calls and respond to email incidents and requests for assistance in accessing or utilizing applications supporting the military and civilian human resource applications.

3.3.3.2. Create a trouble ticket in the incident management application for each phone call and email incident, problem, or request reported by the customer. Trouble tickets shall be categorized and assigned in accordance with established TTPs.

3.3.3.3. Create, reset and unlock user accounts and passwords for applications assigned.

3.3.3.4. Triage customer concerns and if the problem is determined not to be related to a technical issue with AFPOA managed applications, the caller shall be redirected to the appropriate point of contact. The Contractor shall include information and advice on how to communicate the problem to ensure the caller and the point of contact understands the problem.

3.3.3.5. Monitor the A1SD group email inbox daily and create trouble tickets for all incidents, requests and problems submitted and resolve or escalate trouble tickets to Tier II technical personnel.

3.3.4. Data Base Owner (DBO) Shift Support: The Contractor shall provide 24x7 dashboard operations support services during each of the three shifts: CONUS, PACAF and USAFE.

3.3.4.1. CONUS Shift DBO Support: The CONUS Shift DBO shall perform dashboard operations, event and change management support services. Event management occurs when the availability and/or accessibility of an AFPOA supported system or application is negatively impacted. Change management involves scheduling maintenance, patching and upgrades of systems and applications on the APFOA production environment.

The Contractor shall:

3.3.4.1.1. Review, modify, and store the DBO TTP on the restricted drive. The TTP shall be updated annually, or as processes change.

3.3.4.1.2. Facilitate processing of events, to include opening the event in the A1SD Dashboard, tracking and updating the event as status changes.

3.3.4.1.3. When required the CONUS shift DBO send the Notice to Airman (NOTAM) within 15 minutes of notification.

3.3.4.1.4. Ensure event information is reviewed and updated daily for accuracy. Incidents are reported or identified to the DBO via customer phone calls, email, and/or by AFPOA technical personnel.

3.3.4.1.5. Transfer event information from the A1SD Dashboard to the Unscheduled Interruption Log (located on the restricted drive) when the event is closed.

3.3.4.1.6. Review and monitor the A1SD Dashboard to ensure current and accurate data (on-call listing, critical server listing, functional system administrator listing, guidance, etc.) is entered no later than the second Monday of each month.

3.3.4.1.7. Ensure the PACAF and USAFE DBOs have the necessary information and guidance to manage incidents impacting application availability and/or accessibility prior to the

PACAF shift change Monday through Friday. All incidents shall be updated on the A1SD Dashboard and information and resource materials provided and briefed during shift change.

3.3.4.1.8. Update and provide the correct/updated information when the PACAF or USAFE shift DBO identifies information that is inaccurate or confusing on the A1SD Dashboard.

3.3.4.1.9. Update, review and post the daily System Status Report to SharePoint.

3.3.4.1.10. Prepare and deliver reports and metrics related to event management (metrics/trends) to include system availability, accessibility and unscheduled interruptions each month. The reports are saved on a shared drive for the monthly leadership meeting and are due on the 1st Thursday of each month.

3.3.4.1.11. Provide Authorized Service Interruption (ASI) assistance to Maintenance Control (MC) as needed (normally 3-5 days each month) when processing and coordinating ASIs.

3.3.4.1.12. Submit and track network change requests. This involves working to create positive relationships with AFNET and AFPOA mission partners to help facilitate discussions regarding network change requests with mission partners and other personnel.

3.3.4.1.13. Coordinate, submit, and modify network change requests and store information in the change sponsor Access database on the shared drive.

3.3.4.1.14. Provide assistance in MC. The Contractor review the AFPOA MC Plan (provided by the Government). The MC plan identifies the AFPOA processes and procedures to maintain control in the identification, coordination and scheduling of all maintenance actions and is located on the shared drive.

3.3.4.1.15. Assist with scheduling, processing, and coordinating authorized service interruptions. Review incoming ASIs for administrative and technical compliance and verify ASIs contain required information.

3.3.4.1.16. Assist the Government in updating the ASI database to include users, assets, sub-systems and organization information.

3.3.4.1.17. Assist the Government in preparation for the weekly Change Advisory Board (CAB). Upon completion of the CAB, the Contractor assists the Government in approving and scheduling ASIs for action.

3.3.4.2. **PACAF & USAFE Shift DBO Support:** The Contractor shall provide DBO support services to the PACAF (1400-2300) and USAFE (2230-0730) shifts. Additionally, PACAF and USAFE shifts shall provide event management support consisting of monitoring performance tools (currently using Hewlett-Packards Open View Manager) in addition to A1SD support.

The Contractor shall:

3.3.4.2.1. The PACAF and USAFE shift DBOs shall ensure a shift change is conducted 15 minutes prior to their shifts ending. The briefing shall include updates related to open incidents, changes in procedures, and/or questions that arise throughout their shift.

3.3.4.2.2. Ensure information related to event management is input to the DBO Bulletin Board. (The DBO Bulletin Board is an Excel spreadsheet on the shared drive that is used for situation awareness between DBOs and AFPOA technical personnel).

3.3.4.2.3. Perform A1SD support services for incoming calls and email when not actively working events.

3.3.4.2.4. Monitor the MC group inbox continuously throughout their shift to ensure responses are provided for messages identifying critical outages or events that may impact system/application availability and/or accessibility.

3.3.4.2.5. Review the A1SD Dashboard information, guidance, listings, etc., and if information is missing or is confusing, notify the CONUS shift DBO.

3.3.4.2.6. Update and/or open events on the A1SD Dashboard per TTP and A1SD Dashboard instructions.

3.3.4.2.7. Monitor and respond to messages on system monitoring tools (currently using Hewlett-Packard's Open View Manager). The Contractor shall ensure they are adhering to instructions in the A1SD Database and TTP.

3.3.4.2.8. When A1SD Dashboard instructions indicate a NOTAM is required, the Contractor shall send the NOTAM within 30 minutes of identifying an event.

3.3.4.2.9. Update and post the System Status Report to SharePoint when and event is opened and/or when requested by the Government.

3.3.4.2.10. Notify the CONUS shift DBO upon identification of outdated information in the A1SD Dashboard, or if there are questions related to processing Events, MC email, or TTP guidance.

3.3.5. Information & Knowledge Management Support: The Contractor performing this responsibility shall be proficient with applications used for these duties, which include, but are not limited to, Microsoft Active Directory, Microsoft Office (Front Page, Access, Excel, PowerPoint, SharePoint, Visio and Word).

The Contractor shall:

3.3.5.1.1. Open new databases, and create services through which content can be creatively combined, searched and correlated as directed.

3.3.5.1.2. Ensure ad hoc reports and metrics requested are provided are in an easy to read format and per established TTP guidelines. Reports shall be submitted to requestor within 5 business days of request.

3.3.5.1.3. Extract data from the incident management application, the VoIP system, or other A1SD databases and store them on the restricted drive for reporting and metrics purposes.

3.3.5.1.4. Make modifications to the A1SD Dashboard configuration within 10 business days when new requirements are identified by the Government.

3.3.5.1.5. Verify and validate and document configuration changes for each Access database as modifications are made and shall review and verify information accuracy annually (in December). The Contractor shall avoid duplication of data.

3.3.5.1.6. Maintain the A1SD SharePoint page and review/update on a monthly basis, to include the Frequently Asked Questions (FAQs), self-service information, and documents supporting the A1SD and mission partners.

3.3.5.1.7. Maintain a knowledge database on the shared drive for user guidance and that provides customers and A1SD support personnel with self-help solutions and assistance in resolving non-complex problems. Information will provided by the Government.

3.3.5.1.8. Review and validate the knowledge articles six months after creation and every six months thereafter.

3.3.5.1.9. Responsible for maintaining backups of all databases, metrics and process documents and making them accessible to the Government. A report identifying the databases and back-up dates shall be submitted to the Branch Chief on the last Friday of each month.

3.3.6. Database Operations Support: Contractor personnel supporting database operations shall require enhanced/administrative privileges as designated under DOD 8570.01-M as IAT-Level II which will be required to maintain 8570 certification. Database System Administrators may be required to provide 24 hours a day, 7 days per week, and 365 days per year on-site support with on-call support during evenings and on holidays. Weekend and shift work may be required on a rotational basis.

The Contractor shall:

3.3.6.1. Provide a Data Base Operations Support Senior Systems Administrator providing leadership and management support for Contractor personnel assigned in support of the Data Base Operations Support tasks. The Senior Systems Administrator shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service.

3.3.6.2. Provide technical and database system administration support for all AFPOA/AFPC Network Enterprise systems.

3.3.6.3. Support, maintain, and enhance the software environment supporting the AFPOA/AFPC Network Enterprise. The scope of this task includes: managing application software installations, configuration, and upgrades; establishing software test environments; and integrating software problem reporting procedures, plans and tools installation/integration. Research, analyze, test, document system issues and keep TTPs current.

3.3.6.4. Use various tools to monitor database instances and all other areas requiring database system administration oversight. Tasks to be performed consist of monitoring and ensuring that databases, associated storage systems, and peripheral equipment are operational as required; databases are backed up and restored as necessary and planning for future enhancements and upgrades to the existing systems.

3.3.6.5. Provide support to the Information Technology Disaster Recovery (ITDR) yearly exercise. System administration and location for the ITDR exercise will require unclassified and support.

3.3.6.6. Perform general IT Support and Database Administration (DBA) maintenance functions as required, including database performance tuning and trouble analysis and resolution to support key Air Force/A1, Personnel, Services, and Manpower applications, and to support the Air Force database tables that are used within Business Objects, and assistance with the maintenance of unique databases such as Trouble ticket application, and conversion of database applications into Oracle when needed.

3.3.6.7. Provide analysis and database administration support for deployment and sustainment of the Business Objects (BO) repositories and universes. The major work requirement will involve database additions and modifications as required to pull data from Human Resources (e.g. Defense Civilian Personnel Data System and Customer Service Unit) and other sources (e.g., USA Staffing, Manpower Programming and Execution System (MPES), etc.) to meet the needs of the Air Force.

3.3.6.8. Provide technical expertise to support the development of architecture and deployment plans best suited for BO applications.

3.3.6.9. Provide technical expertise to support the development of a strategy for maintaining and synchronizing the various Business Objects repositories and universes.

3.3.6.10. Provide technical expertise to support the development of a strategy for deploying BO throughout the Air Force civilian personnel community (internal and external users). The Contractor shall assist in the development of a strategy for implementing security within BO universes for both internal and external, personnel and non-personnel communities. The Contractor shall provide advice on maintaining and fine-tuning these strategies.

3.3.6.11. Provide technical expertise to support with the design of the BO universes by accomplishing DBA tasks such as creating stored functions and stored procedures to optimize BO performance.

3.3.6.12. Maintain change control on all database baseline scripts associated with the BO repositories and any additional Air Force unique Oracle database tables established to support the query and reporting needs of the Air Force. The Contractor shall install databases in various environments (e.g., development, test, acceptance, production, and training) as needed, and follow change control plan across environments.

3.3.6.13. Monitor and maintain database interfaces to HR databases to support the Air Force unique systems or databases.

3.3.6.14. Document any data schema changes (specific system configuration changes) that may affect either the Air Force unique civilian personnel systems or the BO repositories or universes. Documentation should contain identification of refresh data extraction changes from the appropriate source (e.g., DCPDS, USA Staffing, MPES, etc.) to include table/view and column/attribute references highlighting any changes resulting from patches or releases.

3.3.6.15. Plan and support the standup of the BO repositories and universes and other AF unique applications at a designated Disaster Recovery Site during practice or real- life events.

3.3.6.16. Provide expert technical analysis, options, guidance and support for projects such as data center consolidation, cloud initiative, application re-homing, and decommissioning of applications.

3.3.6.17. Provide technical services for the BO XI3/BI4 environment; troubleshoot and evaluate BO XI3/BI4 system and reporting performance issues.

3.3.6.18. Assess infrastructure to include platform impact, network impact, security authentication, access assignment mapping, and server sizing and performance as it pertains to the Performance Management environment.

3.3.6.19. Provide assistance with installation and configuration of BO BI4 in a Linux virtual environment, to include the single-sign-on solution and configuration for BO BI4.

3.3.7. Business Objects Consultant Support

The Contractor shall**:**

3.3.7.1. Perform all business object tasks identified in 3.3 Task 3 Field Support.

3.3.7.2. Conduct User Interface (UI) assessment as necessary.

3.3.7.3. Troubleshoot and evaluate BO (either BO versions XI3, BI4 or both) system performance issues if the BO Technical Support office is unable to evaluate and access infrastructure.

3.3.7.4. Assess infrastructure to include platform impact, network impact, security Public Key Infrastructure (PKI) authentication, access assignment mapping, and server sizing and performance as it pertains to BO, either XI3, BI4 or both to include Apache Tomcat configuration.

3.3.7.5. Assist with installation and configuration of BO BI4 development, test and production systems in a Linux virtual environment.

3.3.7.6. Assist in the conversion of metric and advance formatted existing BO Corporate Document Library reports from BO XI3 to BI4.

3.3.7.7. Assist with the BO BI4 design and maintenance of universe and univex.

3.3.7.8. Business Objects Consultant requirements for on-site Government work is only at the government's request.

3.3.7.9. Provide a written assessment on all work performed during the entire consultant visit. The assessment will be sent via email to AFPOA/DPOP (afpoa.dpop@us.af.mil). Due within 10 business days after consulting visit is completed. Assessment will be provided 100% of the time.

3.4. <u>Task 4 Operations Support & Data Center Operations (CLIN 0001 NETCENTS CLIN 1100/1300)</u>**:** The Contractor shall provide support for the following Operations & Data Center Operations tasks:

3.4.1. Senior Systems Administrator: The Senior Systems Administrator shall provide leadership and management support for Contractor personnel assigned in support of the Operations Support & Data Center Operations support tasks. The Senior Systems Administrator shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service.

3.4.2. Windows Operation: The Contractor shall support, maintain, and enhance the Microsoft Windows-based Server Operating Systems and associated hardware environment supporting the AFPOA Network Enterprise. This task includes the following but is not limited to: managing Microsoft Windows-based Server Operating System installations, configuration, and upgrades; establishing Microsoft Windows-based operating system test environments; and integrating operating system and hardware problem reporting procedures, plans and tools installation/integration. Research, analyze, test, document system issues and keep

Technical, Tactics, and Procedures (TTPs) current. All Contractor personnel supporting the Windows Operations task shall possess a U.S. security clearance at the minimum level of "Secret." Contractor personnel will require administrative privileges as designated under DOD 8570.01-M as Information Assurance Technical (IAT)-Level II, and are required to maintain 8570 certification.

Tasks to be performed apply to all AFPOA Enterprise Windows and ESX-based systems being supported by the Windows Operations Branch. Normal duty hours are 0700hrs – 1600hrs Central Standard Time (CST), Monday through Friday. System administrators may be required to provide 24 hours a day, 7 days per week, and 365 days per year on-site support with on-call support during evenings and on holidays. Weekend and shift work may be required on a rotational basis.

The Contractor shall:

3.4.2.1. Provide senior level system administration support for all AFPOA enterprise Windows and ESX-based systems. The scope of this task consists of monitoring and ensuring that servers, associated storage systems, and peripheral equipment are operational as required, systems are backed up and restored as necessary, hardware is configured in an optimal manner, planning for future enhancements and upgrades to the existing systems, configuring new hardware once received, and other tasks as required by AFPOA.

3.4.2.2. Have Microsoft System Engineer (MCSE) or System Administrator (MCSA) certifications.

3.4.2.3. Have the VMware Certified Professional (VCP) 6 or higher certification.

3.4.2.4. Have experience with Microsoft Active Directory, Microsoft Internet Information Systems (IIS 7, 8, and 8.5)

3.4.3. Windows-Based Server Environment Support: The Contractor shall assist with installation, monitoring, and maintenance of the Windows-based server environment which consists of over 550 full form servers, blade servers (including virtual server hosts), and VMware vSphere virtual servers as well as over 300 VMware vSphere Virtual Desktop Infrastructure (VDI) virtual desktops. Some servers utilize Microsoft file and database clustering services. Tools and utilities to perform administration duties on all server types include, but are not limited to: Microsoft Active Directory Administration tools and utilities (including Microsoft Management Console (MMC)), Shavlik Netchk, ERDisk, Hewlett-Packard (HP) OpenView, Trouble Ticket application tools, HP Systems Insight Management, Veritas Storage Foundations, VMware vSphere, VMware vCenter Operations Management Suite, VMware Horizon Suite, VMware ESX/ESXi, SureSync, ARKIIS, McAfee Anti-Virus, and various server imaging software. All administration software and tools shall be provided.

The Contractor shall:

3.4.3.1. Provide technical and system administration support for Web applications using Microsoft Internet Information Systems (IIS) and Apache Tomcat for all AFPOA Network Enterprise systems in a tiered, multi-system, multi-web engine environment.

3.4.3.2. Provide Active Server Pages (ASP), Microsoft .NET Framework, Visual Studio (VS), C++, C Sharp, Java Server Pages (JSP), and Hypertext Markup Language (HTML) web application support to include configuration, maintenance, and troubleshooting through interaction and/or use of available tools.

3.4.3.3. Manage PKI certificates for new and existing operating system and web applications. Shall maintain and implement data sources, API integration, and extensions.

3.4.3.4. Maintain and troubleshoot the operation and performance of web applications and associated web application resources through IIS Manager and available tools.

3.4.3.5. Update, annotate, track and modify all trouble ticket application tickets submitted for Windows Operations Support.

3.4.3.6. Provide Windows administration support to include installation, support, and maintenance of Windows-based operating systems.

3.4.3.7. Maintain and enhance the computer hardware and Windows-based operating system environments for legacy and modern systems.

3.4.3.8. Provide configuration control, sustainment, performance and tuning on system peripherals and subsystems.

3.4.3.9. Maintain Windows-based operating system configuration using system tools, utilities and operating system commands.

3.4.3.10. Manage and coordinate hardware, software and application changes.

3.4.3.11. Perform and document configuration management changes on the application and software installations and plan and respond to service outages

3.4.3.12. Diagnose Windows-based software and hardware failures to resolution.

3.4.3.13. Use or assist in creating local documentation to establish Tactics, Techniques, and Procedures (TTPs) used to support, maintain, and enhance the Microsoft Windows-based Server Operating Systems and associated hardware environment supporting the AFPOA Network Enterprise.

3.4.3.14. Assist in the creation, installation and un-installation of applications, software releases and patches using sound Configuration Management practices.

3.4.3.15. Research, analyze, develop, test, and implement data integration system to system level in support of current or future AFPOA requirements to support continuous process improvement. The Contractor shall provide results to the technical lead.

3.4.3.16. Provide user account and group management for systems. This includes add/disable/delete user and group accounts, passwords, change permissions and access control.

3.4.3.17. Provide performance management support. This task includes using system diagnostics tools and reporting hardware or software problems with the appropriate vendor for support. The Contractor enhance the system performance, when applicable.

3.4.3.18. Support Windows file system management. This task includes modifying permissions on directories and files and creating and modifying file systems.

3.4.3.19. Provide Windows system security administration.

3.4.3.20. Maintain the system security by monitoring server access and reviewing necessary logs.

3.4.3.21. Implement and ensure security preventive measures are fully functioning.

3.4.3.22. Ensure all Windows servers in AFPOA maintain adequate security status and compliance IAW Air Force Manual 17-1301, Air Force Network Operating Instructions, AFNOSC TCNO/CTO/NTO/IAVM, and AFPOA direction. This task includes the installation of vendor operating system patches and firmware updates.

3.4.3.23. Mitigate vulnerabilities/security findings identified on Assured Compliance Assessment Solution (ACAS) Nessus scans, Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), and Security Content Automation Protocol (SCAP) Compliance Checker in preparation for Risk Management Framework (RMF) Authorization to Operate (ATO) package submissions.

3.4.3.24. Provide system support for scheduled functional system tests (FST).

3.4.3.25. Provide assistance to users of legacy and Windows systems.

3.4.3.26. Provide application system administration support required to perform System Administration functions.

3.4.3.27. Provide system design on hardware installation and configuration on servers.

3.4.3.28. Perform Windows disk management. This task includes disk mirroring and configuring internal and external disk storage with redundant access paths.

3.4.3.29. Create, modify and maintain scripting to automate Windows System Administration tasks and functions.

3.4.4. System Operations: All Contractor personnel supporting the System Operations task shall obtain a U.S. security clearance at the minimum level of “Secret.” Contractor personnel supporting paragraphs: 3.4.4.1, 3.4.4.2, 3.4.4.3, and 3.4.4.5, will require administrative privileges as designated under DOD 8570.01-M as Information Assurance Technical (IAT)-Level II, and are required to maintain 8570 certification. Contractor personnel supporting System Operations task paragraph 3.4.4. will not require administrative privileges as designated under DoD 8570.01-M, and are not required to maintain 8570 certification. The Contractor shall provide a single Contractor representative to act as a Senior

Systems Administrator for the System Operations task. The Contractor shall perform the following system operations support services:

3.4.4.1. UNIX Administration support: The Contractor shall provide senior level UNIX Administration support during normal duty hours, 0730-1630 Central Standard Time (CST), Monday through Friday. In addition, the Contractor shall provide minimal shift work coverage from 0700-1500 CST on weekends and holidays. The Contractor shall provide on-call support after duty hours to include evenings, weekends and on holidays.

The Contractor shall:

3.4.4.1.1. Provide UNIX Administration support to include installation, support, and maintenance of approximately 200 Linux, HP-UX, Solaris, and UNIX-based operating systems.

3.4.4.1.2. Maintain and enhance the computer hardware and UNIX-based operating system environments for legacy and modern systems as required.

3.4.4.1.3. Provide configuration control, sustainment, performance and tuning on system peripherals and subsystems. Maintain UNIX-based operating system configuration using system tools, utilities and operating system commands as required.

3.4.4.1.4. Perform configuration management activities to include any UNIX server hardware, software, and application changes.

3.4.4.1.5. Diagnose UNIX-based software and hardware failures to resolution. The Contractor shall use or assist in creating local documentation to establish procedures, and develop solutions to problems with UNIX-based systems.

3.4.4.1.6. Assist the application Functional System Administrator (FSA) as necessary in the installation/un-installation of applications, software releases and patches.

3.4.4.1.7. Provide user account and group management as required for systems. This management includes add/disable/delete user and group accounts, passwords, change permissions and access control.

3.4.4.1.8. Perform performance management as required. This management includes using system diagnostics tools and reporting hardware or software problems with appropriate vendor for support. The Contractor shall use the Hewlett-Packard Operations Manager (HPOM) software suite and/or other tools that may be available or become available for use to monitor and identify servers that are experiencing problems during shift. The Contractor shall enhance system performance when applicable.

3.4.4.1.9. Support UNIX file system management. This management includes modifying permissions on directories and files, and creating and modifying file systems.

3.4.4.1.10. Provide UNIX system security administration as required. Maintain system security by monitoring server access and reviewing necessary logs. The Contractor shall implement and ensure security preventive measures are fully functioning. Ensure all UNIX servers maintain adequate security status and compliance IAW Air Force MANUAL 17-1301, Cyberspace Computer Security (COMPUSEC), Air Force Network Operating Instructions, AFNOSC cyber orders to include TCNO/CTO/NTO/IAVMs, and AFPOA direction. Actions include installation of vendor operating system patches and firmware updates. The Contractor shall apply 95% of applicable TCNOs, IAVMs and security hotfixes successfully by mandated compliance date.

3.4.4.1.11. Provide RMF UNIX system administration support on ATO packages.

3.4.4.1.12. Provide system support for scheduled functional system tests (FST).

3.4.4.1.13. Provide assistance to users of legacy and UNIX systems as required.

3.4.4.1.14. Provide application system administration support required to perform System Administration functions.

3.4.4.1.15. Provide system design on hardware installation and configuration on servers when required.

3.4.4.1.16. Perform UNIX disk management. This management includes disk mirroring and configuring internal and external disk storage with redundant access paths.

3.4.4.1.17. Provide and review technical solutions when necessary. Analyzes requirements and assists in preparing implementation plans as required.

3.4.4.1.18. Create, modify and maintain shell scripting to automate UNIX/Linux System Administration tasks and functions.

3.4.4.1.19. Manage UNIX system print servers.

3.4.4.1.20. On a routine basis update, annotate, track and modify all application support tickets submitted for UNIX System Administration support as documented in the A1SD Ticket Priority Matrix. The Contractor shall ensure 95% of tickets are accurately updated and annotated as required until the ticket is remedied and closed.

3.4.4.2. Storage Area Network (SAN) Administration support: The Contractor personnel shall provide master level SAN support during normal duty hours, 0730-1630 CST, Monday through Friday. The Contractor will provide on-call support after duty hours to include evenings, weekends and on holidays.

The Contractor shall:

3.4.4.2.1. Install, manage, and maintain the onsite AFPOA Data Center SAN and the offsite Information Technology Disaster Recovery (ITDR) SAN consisting of 14 storage arrays (approximately 900 Terabytes of data) and associated data storage devices. The Contractor shall assist systems administrators and mission partners with AFPOA SAN issues.

3.4.4.2.2. Maintain and enhance the SAN environment for legacy and modern systems as required to accomplish all associated tasks to ensure its maximum operational uptime.

3.4.4.2.3. Install, support, maintain, manage, configure storage devices and associated firmware for optimum performance and grant storage access to servers as required.

3.4.4.2.4. Work in conjunction with the backup shop on configuration and maintenance of the Virtual Tape Library (VTL).

3.4.4.2.5. Install, support, configure, manage and maintain Fiber Channel switching and routing infrastructure supporting all SAN storage devices.

3.4.4.2.6. Install, manage and maintain the necessary device and software service packs, patches, firmware and hot fixes to ensure maximum enterprise storage platform stability. The Contractor shall diagnose SAN software and hardware failures to resolution.

3.4.4.2.7. Implement and ensure security preventive measures are fully functioning. Ensure all SAN devices maintain adequate security status and compliance IAW AIR FORCE MANUAL 17-1301, Cyberspace COMPUTER SECURITY (COMPUSEC), Air Force Network Operating Instructions, AFNOSC cyber orders to include TCNO/CTO/NTO/IAVMs, and AFPOA direction. The Contractor shall apply 95% of applicable TCNOs, IAVMs and security hotfixes successfully by mandated compliance date.

3.4.4.2.8. Provide Risk Management Framework (RMF) SAN administration support on ATO packages.

3.4.4.2.9. Manage and use SAN management tools; including but not limited to: Nimble Storage InfoSight web interface console, Brocade Fabric Manager, HP Storage Essentials, HP Command View, HP Storage Works (HP LeftHand), OnTap/OnCommand (NetApp), and Unisphere/Data Domain System Manager (EMC).

3.4.4.2.10. Coordinate the installation/placement of devices on the SAN with AFPOA Infrastructure Network Administrators.

3.4.4.2.11. Coordinate all storage device/software repairs with vendor.

3.4.4.2.12. Assist in preparing management briefings on current problems experienced with any storage issues. The Contractor shall plan and respond to any SAN service outages.

3.4.4.2.1.3. Provide configuration control, sustainment, and tuning for on-line, near-line, off-line and off-site storage subsystems and resident data.

3.4.4.2.1.4. Evaluate and advise on storage technology advancements.

3.4.4.2.1.5. Provide and review technical solutions when necessary concerning storage systems.

3.4.4.2.1.6. Implement and ensure SAN security preventive measures are fully functioning.

3.4.4.2.1.7. Use the HPOM software suite and/or other tools that may be available or become available for use to monitor and identify servers that are experiencing problems during shift.

3.4.4.2.1.8. On a routine basis update, annotate, track and modify all trouble ticket application support tickets submitted for SAN System Administration support as documented in the A1SD Ticket Priority Matrix. The Contractor shall ensure 95% of tickets are accurately updated and annotated as required until the ticket is remedied and closed.

3.4.4.3. Hewlett-Packard Operations Manager (HPOM) Administration support: The Contractor personnel shall provide senior level support during normal duty hours, 0730-1630 CST, Monday through Friday. The Contractor shall provide on-call support after duty hours to include evenings, weekends and on holidays.

The Contractor shall:

3.4.4.3.1. Provide HPOM software suite administration support for a variety of data systems consisting of approximately 327 nodes located in the Data Center. HPOM software suite includes OM, OVIS, SNVP, and Reporter. The HPOM software monitors UNIX, Linux-based and Windows operating systems. In addition, HPOM monitors databases, file systems, network, and the SAN. The HPOM Administrator shall provide training on the use of the client software.

3.4.4.3.2. Manage HPOM application software installation, configuration, upgrades, patching, to include hardware needs required by all HPOM application management servers.

3.4.4.3.3. Coordinate with Functional System Administrators (FSAs), Windows Administrators, Web Administrators, Backups and Recovery Administrators, Network Administrators and SAN Administrators to ensure their monitoring and messaging requirements are met.

3.4.4.3.4. Perform template administration and configuration. This entails establishing auto actions, creating/modifying instructions and validation of messaging.

3.4.4.3.5. Ensure administrators and customers have the required training, user accounts, permissions and profiles.

3.4.4.3.6. Ensure proper functioning of the Windows and UNIX operating systems, perform shell scripting and maintain necessary scripts.

3.4.4.3.7. Troubleshoot problems and issues on HPOM monitored nodes using remote system access tools.

3.4.4.3.8. Ensure proper functioning of both Java and Motif Graphical User Interfaces (GUI's) and use both tools for administrating HPOM on monitored nodes.

3.4.4.3.9. On a routine basis update, annotate, track and modify all trouble ticket application support tickets submitted for HPOM System Administration support as documented in the A1SD Ticket Priority Matrix. The Contractor shall ensure 95% of tickets are accurately updated and annotated as required until the ticket is remedied and closed.

3.4.4.4. Data Center Operations Maintenance support: The Contractor shall provide Tenant Management support during normal duty hours, 0730-1630 CST, Monday through Friday. The Contractor will provide on-call support after duty hours to include evenings, weekends and on holidays.

The Contractor shall:

3.4.4.4.1. Provide AFPOA Data Center Operational Maintenance Support to include maintaining the Heating, Ventilation, and Air Conditioning (HVAC) system; the maintain and ordering of correct Data Center power for Information Technology (IT) Hardware; maintaining Data Center physical access security system; and maintaining the master Data Center floor plan and general floor configuration. The AFPOA Data Center is approximately 11,459 square feet.

3.4.4.4.2. Provide oversight of the AFPOA Data Center operational maintenance.

3.4.4.4.3. Manage the transfer of IT hardware from the AFPOA Data Center from the loading dock.

3.4.4.4.4. Provide and review technical solutions on a routine basis. The Contractor shall analyze technical solutions and assist in preparing implementation plans pertaining to electrical and Data Center HVAC requirements of IT hardware.

3.4.4.4.5. Act as the point of contact for all hardware installation/relocation and discontinuance of IT equipment. The government will make the determination of what hardware will be discontinued.

3.4.4.4.6. Create and maintain current Data Center floor plans drawing using AutoCad software.

3.4.4.4.7. Ensure Data Center site preparation (electrical cables and plugs, cooling, floor panel cable access) for IT equipment hosted at the AFPOA Data Center. The Contractor will coordinate with Civil Engineers to request any new electrical cables and plugs.

3.4.4.4.8. Provide delivery and pre-staging activities for IT hardware.

3.4.4.4.9. Coordinate with Civil Engineers, vendor and users on any operational maintenance to the Data Center.

3.4.4.4.10. Monitor the AFPOA Data Center temperature and humidity levels to ensure that standards are maintained. The Contractor shall monitor temperature and humidity level machines at least two times per work day. The Contractor shall maintain 95% compliance of Review the Temperature and Humidity machine graphs output in the AFPOA Data Center.

3.4.4.4.11. Initiate and monitor the AFPOA Data Center operational maintenance actions.

3.4.4.4.12. Coordinate Data Center facility scheduled and unscheduled outages with AFPOA and civil engineers.

3.4.4.4.13. Provide the security monitoring for the AFPOA Data Center, receiving requests for access and generating/creating/coding access cards.

3.4.4.5. Backup and Recovery Administration support: The Contractor shall provide Backup and Recovery Administration Journeyman level support to the Swing and Mid shifts, 7 days per week, 365 days per year on-site support to include holidays. Swing Shift runs 1500-2300 CST and Mid Shift runs 2300-0700 CST.

The Contractor shall:

3.4.4.5.1. Monitor approximately 3,000 scheduled weekly backup jobs of UNIX-based and Windows-based operating systems and all related equipment in Data Center, optical storage juke boxes, disk arrays, clustered servers, virtual servers, NetApp NAS, VTL and an automated tape cartridge silo.

3.4.4.5.2. Accomplish daily, weekly, and monthly backups of databases and operating/file systems utilizing CommVault Simpana software and EMC DataDomain or any other available tools or software purchased by AFPOA. Backups and restores are performed on a routine basis.

3.4.4.5.3. Perform full and incremental backups of applications user files and databases and their transaction files as required by the customer using vendor’s manuals, documented instructions or trouble shooting procedures with assistance from system administrators or DBAs, on a routine basis.

3.4.4.5.4. Initiate UNIX commands/shell scripts using documented instructions or troubleshooting procedures as required backup, shutdown databases or rebooting individual servers.

3.4.4.5.5. Maintain full and incremental backups for an appropriate time period as determined by the needs of the customer and regulatory requirements of the data.

3.4.4.5.6. Manage and maintain a library of magnetic and /or optical backup media ensuring a complex rotation of media is followed and the correct media for each backup are scheduled for rotations to and from remote storage using documented instructions or trouble shooting procedures as required.

3.4.4.5.7. Manage and store optical and magnetic media in support of backing up and restoring various systems.

3.4.4.5.8. Perform as System Administrators on servers and related equipment to ensure operation is stable and continuous.

3.4.4.5.9. Use the HPOM software suite and other tools that may be available or become available for use to monitor and identify servers that are experiencing problems during non-core duty hours.

3.4.4.5.10. Identify system failures and equipment problems and take appropriate action according to operational instructions or vendor operating manuals within predetermined time frames. Servers that report critical or major error messages shall be remanded within 15 minutes of detection. This means that some action must be started to resolve the problem within the stated 15 minutes. The Contractor shall maintain 95% compliance of annotating HPOM of the initial corrective action taken within 20 minutes of a reported critical or major error messages.

3.4.4.5.11. Configure, manage, and maintain all hardware and software utilized to control backup storage devices, including drives, libraries, media and clustered server environments, including software patches and firmware upgrades.

3.4.4.5.12. Document and advertise known defects, quirks, tips, tricks and techniques useful in troubleshooting, configuring, managing and maintaining hardware and software utilized in the daily operation of the Backup and Recovery Environment in the form of TTPs.

3.4.4.5.13. Respond to customer trouble calls and take appropriate action within 30 minutes on a routine basis.

3.4.4.5.14. Monitor organization virtual office inboxes for system action notifications and for requests every half hour.

3.4.4.5.15. Provide management with a report from each shift that provides a status of all backups and restores scheduled via web reporting, hardware, and software problems reported to the vendor. A status also be provided on any unscheduled backups and restores.

3.4.4.5.16. Annotate the Daily Operations Activity Report provided by the government to identify servers experiencing problems and actions taken by the system administrator to resolve the problem. The Contractor shall annotate any action taken to call out the vendor, or another point of contact, in the report. The Contractor shall log any HPOM notifications owned or

annotated and any unusual occurrences taking place in the Data Center floor shall be included in the Daily Operations Activity log shift turnover comments.

3.4.4.5.17. Provide a smooth handover from one shift to the next. The Contractor shall ensure that any problems existing when the shift changes be relayed to the next shift. Shift turnovers shall consist of an informal briefing from one shift to the next.

3.4.4.5.18. Monitor the AFPOA Data Center temperature and humidity levels during the Swing and Mid shifts to ensure that standards are maintained. The Contractor shall report to the appropriate government representative when the temperature and humidity levels are not within standards.

3.4.4.5.19. Maintain physical security of the data center by confirming all the data center access doors are closed and secure during the Swing and Mid shifts.

3.4.4.5.20. The Contractor shall provide Requirements & Technical Solution tasks:

3.4.4.5.20.1. Review applicable requirements and assist the Government in preparing technical solutions and implementation plans.

3.4.4.5.20.2. Create, modify and maintain shell scripting to automate Windows System Administration tasks and functions.

3.5. <u>Task 5 Cybersecurity and Software Management Support (CLIN 0001 NETCENTS CLIN 1300)</u>: The Contractor shall provide support to include assembling, developing, compiling or submitting Assessment and Authorization documentation for Contract Personnel performing Security Certification Phase, Security Accreditation Phase, and Continuous Monitoring Phase; A&A. There will be ~~no~~ administrative privileges as designated under DOD 8570.01-M as Information Assurance Workforce Improvement Program (IAM)- Level I (http://www.dtic.mil/whs/directives) and AFMAN 17-1303, Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil). Personnel shall have expertise in preparing, monitoring, controlling and processing written and electronic communications from creation to final disposition. Electronic communication will primarily be through email and established electronic workgroup areas (i.e., SharePoint). Written documentation shall be provided as a quality product with minimal editorial changes required. Personnel shall have expertise in project management and delivery of complex tasks (work-breakdown-structures) to meet published timelines as defined within applicable project plans.

Personnel shall have expertise in utilizing the Microsoft Office Suite of applications and Microsoft Visio for developing and editing technical documentation. Personnel shall store all documents created for the task on the appropriate restricted shared drive. No task documents created by the Contractor shall be stored on the Contractor's issued PC or laptop. The Contractor will comply with the filing folder

and document naming conventions on the restricted drive. Contractor personnel are required to have DoD IA Workforce certifications when initially reporting for duty to the task and maintain the appropriate certification level at all times while working on the task. Contractor personnel who do not maintain certifications shall be denied access to DOD information systems for the purpose of performing information assurance functions and not be allowed to perform on the task.

Senior level A&A personnel should have at a minimum 8 years of information systems security experience, 4 years of which must be specifically associated with system accreditation/authorization work, which may include RMF, DIACAP or a combination of those processes. Junior level A&A personnel should have at a minimum 5 years of information systems security experience, 3 years of which must be specifically associated with system accreditation/authorization work, which may include RMF, DIACAP or a combination of those processes. Both levels require IA Workforce certifications. Contractor personnel assigned to this associated task shall maintain a valid Secret security clearance. The Contractor must be able to be issued a SIPR token for use on the SIPRNet and be willing to sign a Non-disclosure Agreement (NDA).

The Contractor shall be responsible for training contract employees on cybersecurity/IT in the event new technology in hardware or software is implemented at the direction of the government. The training times and dates shall be coordinated with the government representative or the contracting officer before being scheduled.

The Software Management Contractor position requires the individual to have and maintain an IA Workforce certification to perform administrative-level actions and must be able to maintain an administrative account for testing in accordance with DoD Directive 8570.01-M, IAT Level II. The Software Management Contractor position should have at a minimum 3 years of Information Technology experience and 1 year testing experience which may include tools like Wireshark, MKRuntest and/or a combination thereof using similar tools or applications. Personnel must have basic knowledge of the RMF or DIACAP process or a combination thereof as well as knowledge of the NIST, Common Criteria, AFNIC and DISA certification programs. The Contractor must have the ability to handle multiple certification initiatives and or projects simultaneously and proactively manage each initiative in accordance with established AFNIC processes within established timelines. Contractor personnel assigned to this position shall maintain a valid Secret security clearance.

*****Loss of any required certification(s) will result in immediate removal from the task. The Contractor will provide a fully qualified replacement as soon as possible, but no later than 30 days from certification expiration.***

The DoD and the Air Force follows the RMF A&A process based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and

Organizations (NIST Publications www.CSRC.NIST.gov/publications, to get most current version). A listing of applications/systems with identified scoping information to determine level of effort applicable to the A&A portion of this PWS is provided in Appendix B, Table 2.

The Contractor shall support the Cybersecurity and Software Management tasks:

- A&A Project Management
- A&A Package Support
- Plan of Action and Milestones (POA&M) Support
- Continuous Monitoring
- Software Management

3.5.1. The Contractor shall provide an on-site Senior Information Assurance Engineer for the A&A and software management support tasks. In addition to accomplishing A&A analysis duties, the Senior Information Assurance Engineer shall provide leadership, training and management oversight of the Contractor personnel assigned to the AFPOA Cybersecurity Division. The Senior Information Assurance Engineer shall assign and oversee the execution of the A&A, software certification, and software license management tasks. The Senior Information Assurance Engineer shall ensure that the MSR is submitted each month.

3.5.2. Application Services Performance Parameters A&A Project Management: The Contractor shall provide project management services for the A&A task**.** The level of effort required to accomplish the A&A tasks depend upon:
(a) the size and complexity of the information system;
(b) the security category of the system;
(c) the security controls employed to protect the system;
(d) the specific methods and procedures used to assess the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome; and
(e) assessing and evaluating security requirements for each assigned application/system in accordance with the latest guidance governing the Air Force RMF A&A process (AFI 17-101, *RMF for Air Force Information Technology*; (http://www.e-publishing.af.mil)), and AF and DoD accepted software certification processes.

3.5.2.1. A&A and Software Management Support Project Plan (PP)

The Contractor shall:

3.5.2.1.1. Provide a project plan within 3 business days following the assignment of each task. The PP shall provide at a minimum details surrounding the specific tasks, milestones, delivery schedule, submission dates, and plan for tracking progress and

the execution of the A&A; annual security assessments/reviews and software management tasks. Changes to the project plan must be approved by the AFPOA Technical Points of Contracts prior to implementation.

3.5.2.1.2. Provide PP updates each week on the day and time as defined by the Government. Updates shall include changes to estimated completion dates, percentage of completion for each task and any issues that could impact task completion.

3.5.2.1.3. Meet delivery schedule or coordinated suspense date for the project plan with no more than 3 errors in the document requiring correction.

3.5.2.1.4. Meet delivery schedule or coordinated tasked suspense's with no more than 3 revisions to documents reporting changes to the AFPOA Information System Security Manager (ISSM) and subsequently to the AO to support an A&A decision.

3.5.3. A&A Package Support

The Contractor Shall:

3.5.3.1. Build the system A&A package using the current Air Force approved automated tool; currently the Enterprise Mission Assurance Support Service (eMASS). The Contractor shall have the ability to use the following A&A automation tools: eMASS, Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP).

3.5.3.2. Assist in the Information System Categorization process and creation of the STIG Applicability List using the Air Force's AFSPC Categorization, STIG, and Assessment Tool (ACSAT) or other method based on Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems (https://www.cnss.gov/CNSS/issuances/Instructions.cfm), and Federal Information Processing Standards Publication (FIPS PUB) 199 (https://csrc.nist.gov/publications/detail/fips/199/final), Minimum Security Requirements for Federal Information and Information Systems (http://csrc.nist.gov/publications/PubsSPs.html), as a part of the RMF activities for each application or system during their performance of A&A for these systems. Deliverables: Security Categorization Document and STIG Applicability List.

3.5.3.3. Assist in the selection of common security controls and the preparation of a comprehensive Security Plan to support a continuous monitoring strategy IAW NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems"(http://csrc.nist.gov/publications/PubsSPs.html).

3.5.3.4. Provide System Security Plan (SSP) Support. The Contractor shall identify the overlays to apply the appropriate security controls to the

system and shall document the implementation of these controls in the SSSP IAW NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", and NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans" (http://csrc.nist.gov/publications/PubsSPs.html).

3.5.3.4.1. The SSP provides an overview of security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents for the information system such as Network Boundary Configuration, Topology, Ports & Protocols System Matrix (PPSM), Users and User Groups, Threat/Risk Assessment, Privacy Impact Assessment (PIA), Contingency Plan, Incident Response Plan (IRP), Configuration Management (CM) Plan, security configuration checklists, and any system interconnection agreements.

3.5.3.4.2. Provide inputs to the approved SSP by updating documents within the Contractor's span of control and providing inputs to other/new documents as required.

3.5.3.4.3. Support the RMF Team in the assessment of selected security controls required to support the Security Control Assessor (SCA) in preparing a complete Security Assessment Report (SAR). Controls may be identified as Initial Phase (IP) and Final Phase (FP) and all IP controls are required to be answered prior to submission of the ATO package to the AO. FP controls must be fully answered within the first year following the award of the ATO as part of the initial Annual Federal Information Security Management Act (FISMA) Review. The Contractor will not fulfill the task if the FP controls are not completed within the first 12 months following the award of the ATO.

3.5.3.4.4. Assist in the preparation of a Risk Assessment Report (RAR) containing the results of all security testing, STIGs, and applicable automated vulnerability scans using the AF's tools of choice, currently Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP) Tools.

3.5.3.4.5. Prepare a comprehensive RAR, including mitigations for any unfixable non-compliant findings to determine residual findings and risk that must be addressed and documented within the A&A package.

3.5.3.4.6. PPSM. The Contractor ensure the system PPSM is registered with the AF PPS Office via the PPS Registration Tool on SharePoint or any other tool as directed by AF PPS Office. Once the system receives a new ATO, the Contractor shall update the expiration date of the PPSM using the same tool.

3.5.4. **Plan of Actions and Milestones (POA&M) Support**. The POA&M describes the measures that have been implemented or planned:

a) To correct any deficiencies noted during the assessment of the security controls
b) To reduce or eliminate known vulnerabilities in the information system.

The Contractor shall:

3.5.4.1. Document all identified non-compliant controls and non-applicable security into a POA&M in order to support the submission of the complete Security Authorization Package (System Security Plan, RAR, and POA&M) to the Authorizing Official (AO).

3.5.4.2. Upon AO signature of the authorization decision, the Contractor shall support continuous monitoring actions for the system and determine impact of any changes to the system and its environment that might generate an update to the A&A package and consideration for reauthorization actions.

3.5.4.3. Update the Security Plan, RAR and POA&M to support reporting security status to the AO.

3.5.4.4. Provide advice, recommendations and support for the required decommissioning actions for any system reaching end-of-life.

3.5.5. Continuous Monitoring

The Contractor shall:

3.5.5.1. Review and update system security controls according to the AF Information System Continuous Monitoring Guide.

3.5.5.2. Provide documentation created for the purpose of the Annual FISMA Review showing that all security controls to be monitored on an annual basis have been reviewed and/or tested and all documents in the System Security Plan have been validated as current or updated as necessary. The system POA&M will be updated accordingly by the Contractor. The Annual FISMA Review is due annually no later than the anniversary date of the system ATO during the continuous monitoring years of the ATO award period. If the ATO award is delayed, the Annual FISMA Review will occur but not in the place of the ATO.

3.5.6. Software Management Support: The Contractor shall provide software management support which encompasses two sub-tasks: Software Certification and Software License Management.

3.5.6.1. Software Certification: The Contractor shall meet delivery schedules or coordinated tasked suspense's with no more than 3 revisions to the software certification and evaluation testing documentation.

The Contractor shall:

3.5.6.1.1. Successfully complete the required AF software certification documentation and software testing actions for desktop (to include client/server applications) and web applications; and assist in expediting the software certification processing accomplished by Air

Force Network Integration Center (AFNIC). The Contractor shall comply with AFNIC's current guidance on Software Certification (https://cs3.eis.af.mil/sites/OO-SC-IA-01/Wiki/Software%20Certification.aspx, (may require login)).

3.5.6.1.2. Complete application request worksheets, applicable STIGs, conduct software testing, and ensure compliance with applicable guidance IAW AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) (http://www.e-publishing.af.mil) in order to obtain a Certification Decision.

3.5.6.1.3. Complete the Application Request Worksheet (ARW) and document application testing results as required on the CM.

3.5.6.1.4. Complete the software certification package which includes completing the ARW, CM, Ports, Protocols, Services Worksheets and answering all checklist questions.

3.5.6.1.5. Prior to submission to AFNIC for certification consideration, the Contractor shall submit software certification package to AFPOA/DFC for review and approval by the Information System Security Manager (ISSM).

3.5.6.1.6. Review the validation information for the software (as identified on the ARW) to include vulnerability assessments of any known vulnerabilities, and shall ensure that the software represents a good candidate for software certification testing.

3.5.6.1.7. Upon validation for the software certification process, the Contractor shall follow the complete process of tested software evaluation by AFNIC and provide assistance and consultation to AFNIC/NVI as required supporting the final issuance of a software certification decision for the software.

3.5.6.1.8. Execute software testing using AFNIC's current checklists. Any implementation documentation specific to COTS products currently available to the government will be provided to the Contractor. If the product is a GOTS product, the Contractor shall also conduct a code-scan using Air Force approved certified code-scanning software to verify no vulnerabilities exist within the code, and provide a final report of the code scan with the software certification package.

3.5.6.1.9. Upon identification of High and/or Moderate vulnerabilities during testing of an application, the Contractor shall notify the ISSM of the vulnerability within 1 business day and provide a mitigation plan. The mitigation plan shall be submitted within 3 business days upon vulnerability discovery and shall include the milestones and estimated completion dates.

3.5.6.1.10. Work with the software vendor, AFPOA technicians and Mission Partners to mitigate the finding(s) to the lowest level possible. Finding and mitigation results must be provided to AFPOA/DFC in writing, and documented on the CM for the application.

3.5.6.1.11. Use websites identified in the most current Application Request Worksheet (ARW), currently block 4.1 of ARW v3.4, to verify if any

vulnerabilities exist within the application. This information can be found on the Air Force Network Integration Center's (AFNIC) Software Certification page at: https://cs2.eis.af.mil/sites/10007/sc/SitePages/Home.aspx .

3.5.6.1.12. Work/coordinate with representatives from the AFPOA Cybersecurity Branch in preparing certification packages for submission of information assurance (IA)/IA-enabled software/hardware to National Information Assurance Partnership (NIAP) for Common Criteria certification.

3.5.6.1.13. Support the application sponsor (or program manager), Software License Manager and Contracting Officer's Representative in responding to any questions, attending meetings, and/or any other activities/tasks facilitating the development of the certification documentation.

3.5.6.2. Software License Management

The Contractor shall:

3.5.6.2.1. Support software license management functions of AFPOA IAW AFMAN 17-1203, Information Technology (IT) Asset Management (ITAM) (http://www.e-publishing.af.mil) which would include applications, license agreements, and software upgrades.

3.5.6.2.2. Support 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.

3.5.6.2.3. 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.

3.5.6.2.4. Support common practices for ordering assets, tracking orders and assets, and tagging the assets.

3.6. <u>Task 6 Lifecycle Management Support (CLIN 1100/ NETCENTS CLIN 1100/1300)</u>: The Contractor shall provide support for the following Lifecycle Management tasks:

3.6.1. Enterprise Architecture (EA): AFPOA EA utilizes Business Process Modeling (BPM) to capture business processes of the AFPOA enterprise in order to analyze current process, support documentation requirements for other processes, train personnel and make improvements to processes. AFPOA uses UNICOM System Architect environment to develop models at all levels of architecture (Operational, Solution Based, Domain Architecture, and Initiative level Architecture) in the DOD Architecture Framework (DoDAF) DoDAF Architecture v2.02 as described in http://dodcio.defense.gov/Library/DOD-ArchitectureFramework/ & DOD Information Enterprise Architecture (DOD IEA) as well as Business Process Model and Notation (BPMN) to enable the integration

of Human Resource (HR) business processes across the enterprise. This includes; tracing artifacts to higher levels of architecture such as the Deputy Chief Management Officer (DCMO) Business Enterprise Architecture (BEA), reacting to external factors such as changes in law, updates and replacement of legacy systems and the integration of capability to support Total Force and the ability to analyze, understand, and leverage opportunities afforded by emerging technologies.

The Contractor shall:

3.6.1.1. Develop and maintain the current 1559 AFPOA EA models and any future architecture models required to support AFPOA and the AFPOA requirements process.

3.6.1.2. Develop and maintain the AFPOA portfolio capability development roadmaps depicting the major delivery efforts anticipated or underway in and/or impacting the AFPOA Domain.

3.6.1.3. Provide Business Process Modeling (BPM) support to internal AFPOA support activities and analyze, identify and incorporate updates to guidance, policies, and procedures into the AFPOA business processes.

3.6.1.4. Coordinate and review the BEA and BPR compliance submissions and facilitate resolution of compliance issues supporting annual funding certifications.

3.6.1.5. Submit AFPOA Architecture to the EA Configuration Control Board (EACCB) for review and approval of architecture content for inclusion in AF/A1s repository's production environment.

3.6.1.6. Participate in regular EACCB review of architecture content being considered for changes and/or promotion to the production environment of the AF/A1 EA shared repository.

3.6.1.7. Facilitate a review of architecture for promotion from the repository's development environment to its production environment. The Contractor review architecture to ensure compliance with established standards, conventions, and structure. The Contractor produce/brief review findings as required.

3.6.1.8. Manage and maintain the AFPOA encyclopedias, to include version control, migration, and archiving of the AFPOA architecture products.

3.6.1.9. Develop RMF artifacts to support ATO packages.

3.6.1.10. Maintain awareness of AF and DOD strategy and plans for structure to support enterprise architecture and requirements toolsets.

3.6.1.11. Recommend and document courses of action that may include migration/transition of the central repository to other environments, software, or service platforms.

3.6.1.12. Review and recommend response to information support plans impacting the AFPOA Domain.

3.6.1.13. Attend EA related working groups, forums, and meetings to remain informed and engaged on latest activity, policies, and procedures.

3.6.1.14. Inspect compliance fields in the Information Technology Investment Portfolio System (ITIPS): pass data, list of interfaces, what BEA version asserted to, and BEA compliant.

3.6.1.15. Complete Weekly Activity Report detailing all activities and accomplishments for the week and meet delivery schedules or coordinated tasked suspense.

3.6.1.16. Required deliverables and the timeframe for their delivery are located in Section 6.0, Table 1 of this PWS.

3.6.2. **Asset Management:** The Contractor shall provide Asset Management support as the Equipment Control Officer (ECO) that is responsible managing all accountable IT assets utilized by AFPOA personnel as daily Office Automation (OA) equipment as well as the enterprise systems located in the AFPOA Data Center. All Asset Management activities will be executed IAW AF guidance to include AFMAN 17-1203 "IT ASSET MANAGEMENT (ITAM)" and AFI 23-111 "Management of Government Property in Possession of the Air Force. The ECO will be functionally aligned under the AFPOA Lifecycle Management Division AFPOA/DFL. The ECO will have the ability to react to changes in external factors such as advances in OA technology as well as large scale changes to the AFPOA Data Center.

The Contractor shall:

3.6.2.1. Be appointed by the AFPOA Director to perform as the AFPOA Equipment Control Officer in accordance with AFMAN 17-1203 section 1.2.11 with the exception of all inherently governmental functions in accordance with Federal Acquisition Regulation (FAR) Subpart 7.5, "INHERENTLY GOVERNMENTAL FUNCTIONS."

3.6.2.2. Provide overall management of IT assets to include local storage and distribution of IT property as well as leveraging emerging technologies by developing strategic plans for the lifecycle management of the AFPOA fleet of OA equipment.

3.6.2.3. Develop IT Refresh plan for all organizations supported Standard Office Automation equipment to include desktops/laptops, monitors and multi-function printers etc.

3.6.2.4. Plan, develop and execute deployment plan for strategic refresh (desktops, laptops, monitors and printers) annually.

3.6.2.5. Manage the local IT storage area.

3.6.2.6. Schedule necessary equipment logistics between Joint Base San Antonio Randolph Bldgs. 977, 493, 492, 494 as well as the Defense Logistics Agency – Disposal Services and 502nd CS. Vehicle and operator will be provided by the Government and will be made available for scheduling with one week notice.

3.6.2.7. Track status and provide ad hoc reporting of status of all equipment.

3.6.2.8. Work with existing AFPOA Property Custodians and provide help with the management and inventory of all AFPOA assets.

3.6.2.9. Work to identify excess IT equipment and notify PCs for turn in.

3.6.2.10. Harvest, store and issue usable equipment as well as process and dispose of unusable equipment

3.6.2.11. Receive, store and reissue IT accessories such as keyboards, mice, Common Access Card (CAC) readers, speakers, microphones, cables and other non-accountable peripherals).

3.6.2.12. Recommend and document courses of action that may include migration/transition to new technology or ways of doing business.

3.6.2.13. Attend meetings, working groups and forums, to remain informed and engaged on latest activity, policies, and procedures within AFPOA and to support leadership.

4. Information Assurance (IA)

The Contractor shall ensure that all system or application deliverables meet the requirements of DOD and AF Cybersecurity policy. Furthermore, the Contractor shall ensure that personnel performing cybersecurity activities obtain, and remain current with, required technical and/or management level certifications.

4.1. System Cybersecurity

For those solutions that will not inherit existing network security controls, and thus integrate an entirely new application system consisting of a combination of hardware, firmware and software, system security assurance is required at all layers of the TCP/IP DoD Model. The Contractor shall ensure that all system deliverables comply with DoD and AF Cybersecurity policy, specifically DODI 8500.01, *Cybersecurity*, AFI 17-130, *Air Force Cybersecurity Program* Management (currently in draft), and AFM 17-1301, *Computer Security*. To ensure that Cybersecurity policy is implemented correctly on systems, Contractors shall ensure compliance with DOD and AF Assessment & Authorization policy, specifically DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, and AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT).* The Contractor shall also support activities and meet the requirements of DODI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.2. Application Cybersecurity

For those solutions that will be deployed to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inherit existing network security controls, application security assurance is required at the application layer of the TCP/IP DoD Model. The Contractor shall ensure that all application deliverables adhere to Public Law 111-383, which states the general need for software assurance. Specifically, the Contractor shall ensure that all application deliverables comply with the Defense Information Systems Agency (DISA) Application Security & Development Security Technical Implementation Guide (STIG), which includes the need for source code scanning, the DISA Database STIG, and a Web penetration test to mitigate vulnerabilities with findings such as SQL injections, cross-site scripting and buffer

overflows and others. The Contractor shall also support activities and meet the requirements of DODI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.3. Personnel Cybersecurity Workforce Certification

As stated in AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, Paragraph 1.4, Contractor personnel performing cybersecurity activities are required to have at the time of reporting for duty and maintain a DoD approved cybersecurity baseline certification(s) as outlined in DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, Paragraph C1.4.4.7 (T-0).

5. Contractual Requirements

5.1. Contractors Use of NETCENTS-2 Products Contract

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

5.2. Government Furnished Property

Since work will be performed at the Government facility, the Government will furnish or make available working space, network access and equipment to include:

- **5.2.1.** Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
- **5.2.2.** Telephone (local/long distance calls authorized as dictated by task order performance requirements)
- **5.2.3.** Facsimile
- **5.2.4.** Copier
- **5.2.5.** Printer

Copies of required Government furnished materials cited in the solicitation, PWS, and the DD Form 254 will be provided to the Contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the responsible Government QAP upon request or at the end of the task order PoP.

Equipment purchased by the Contractor with the approval of the Government and directly charged to this task order shall be considered government owned-Contractor operated equipment. The Contractor shall conduct a joint inventory and turn in this equipment to the AFPOA COR upon request or completion of the Task Order.

5.3. Post Award Orientation Conference

The contractor shall participate in a post-award conference for the purposes of making introductions, coordinating security requirements, discussing schedules,

prioritizing PWS requirements, and providing details regarding the transition of work requirements from the incumbent contractor.

The contractor shall commence work on the first day of the period of performance. The Post Award Orientation Conference shall occur at Randolph AFB, TX, 14 days after award. Attendance by the contractor shall be at no additional (direct) cost to the Government.

5.4. Transition Plan (Phase In and Out of Task Order)

The contractor shall comply with their submitted awarded/approved transition plan that outlines the designated time period and strategy to transition into the duties as the contractor and to transition out of the task order at the end of the period of performance.

Note: The transition period shall not exceed 30 days.

5.5. Personal Services

The client has determined that use of the NETCENTS II to satisfy this requirement is in the best interest of the government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled “Personal services contract”.

To counter the circumstances that infer personal services and to preserve the non-personal nature of the contract, the contractor shall adhere to the following guidelines in the performance of the task:

5.5.1. Contractor provides for direct supervision of all contract employees assigned to the task.

5.5.2. Refrain from discussing the issues such as skill levels and hours, salaries, cost and funding data, or administrative and personnel matters affecting contractor employees with the client.

5.5.3. Ensure close communication/coordination with the GSA PM, reporting problems to the PM as they occur (not waiting for a monthly meeting).

5.5.4. Do not permit government officials to interview potential contractor employees, discuss individual performance, approve leave or work scheduling of contractor employees, terminate contractor employees, assist contractor employees in doing their jobs or obtain assistance from the contractor in doing Government job.

5.5.5. Do not assign contractor personnel to work under direct government supervision.

5.5.6. Maintain a professional distance from government employees.

5.5.7. Provide contractor employees with badges, if appropriate, identifying them as contractors.

5.5.8. Ensure proper communications with the government (technical discussion and government surveillance is okay, but the Government cannot tell the contractor how to do the job).

5.5.9. Assign a Program Manager to the task order. The Program Manager or alternate should be the only one who accepts tasking from the assigned Government point of contact or alternative.

5.5.10. The government has the right to reject the finished product or result and this does not constitute personal services.

5.5.11. When travel is required for the performance on a task, the contractor personnel are only to travel as directed by their contract management.

5.5.12. Contractor Code of Business Ethics and Conduct. The Contracting Officer may require dismissal from work those employees which he/she deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment he/she deems contrary to the public interest or inconsistent with the best interest of national security. The Contractor shall not employ persons on this call order if such employees are identified to the Contractor by the Contracting Officer or the Contracting Officer's Representative (COR), as a potential threat to the health, safety, security, general well-being, or operational mission of the installation and its population.

5.5.13. The Contractor shall not employ persons on this task order if such employees are identified to the Contractor by the CO as a potential threat to the health, safety, security, general well-being, or operational mission of the installation and its population.

5.6. Contractor Identification

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

5.7. Program Management:

The Contractor shall identify a Program Manager who shall be the primary representative responsible for all work awarded under this task order, participating in

Program/Project Management Reviews and ensuring all standards referenced herein are adhered to.

5.7.1. System and Network Authorization Access Requests

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

5.8. Data Rights and Non-Commercial Computer Software

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

5.9. Software Support and Data Rights

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

5.10. COTS Manuals and Supplemental Data

The Contractor shall provide documentation for all systems services delivered under this Task Order. The Contractor shall provide COTS manuals, supplemental data for

COTS manuals and documentation IAW best commercial practices (i.e. CD-ROM, etc.). This documentation shall include users' manuals, operators' manuals, maintenance manuals and network and application interfaces if specified in the task order.

5.11. Enterprise Software Initiative

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

5.12. Software License Management

If developing and/or sustaining a system that requires and/or contains COTS, the Contractor shall provide maintenance and support of that software license to manage its relationship to the overall system life-cycle in accordance with AFI 33-114, Software Management, which would include applications, license agreements and software upgrades. The Contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The Contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The Contractor shall support common practices for ordering assets, tracking orders and assets and tagging the assets. The Contractor shall support application installation, operations, customer support, training, maintenance, and sustainment and configuration control, to include the procurement of supporting software licenses.

5.13. Transition and Decommissioning Plans

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

5.14. Section 508 of the Rehabilitation Act

The Industry Partner shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that

when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Applicable standards are 1194.21-1194-26.

The Industry Partner should review the following websites for additional 508 information:

http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

The contractor must indicate in its response package where full details of compliance to the identified standards can be found, such as vendor's website, etc.

6. Deliverables/Milestones

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

Table 1 List of Deliverables and the Performance Requirements Summary

Required Deliverables	Format	Required Due Date	Send TO	Planned Frequency	PWS Reference
Task 3.1 Program Management Deliverables					
Program Management Plan	Submit Word, PDF or Excel	Revised PMP 30 calendar days after contract award, living document with monthly updates after final plan is approved.	COR/CO via ITSS	Monthly	3.1
Quality Control Plan	Submit Word, PDF or Excel	30 calendar days after contract award, living document with monthly updates after final plan is	COR/CO via ITSS	Monthly	3.1

		approved.			
Activity Report Brief	Submit Word, PDF or Excel	At least one business day prior to the Status Meeting		No less than Monthly	3.1
Weekly Activity Report (WAR)	Electronically in MS Excel, MS Power point, or MS Word	Weekly	COR/CO via ITSS	Weekly	All major tasks in 3.1 through 3.6
Required Deliverables	**Format**	**Required Due Date**	**Send TO**	**Planned Frequency**	**PWS Reference**
Task 3.2 CCTK Deliverables					
All C-Sharp Code Modules	.cs, .exe, .dll, .asp, and .aspx	Each Deploy Cycle Freeze Date	COR/CO via ITSS	Prior to Cycle Code Freeze	3.2
All SQL Code Modules	.sql	Each Deploy Cycle Freeze Date	COR/CO via ITSS	Prior to Cycle Code Freeze	3.2
All Estimated LOE and Delivery Date	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All Status Reports and Analytics	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All Analytic materials and logs	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All presentation materials and Notes	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All updated requirement materials	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All reference material or links used	Electronically in MS Excel or MS Word or	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2

	PowerPoint				
All guides and scan results used	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All reference APIs used	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All C# Code and SQL Modules used	.cs, .exe, .dll, .asp, and .aspx	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All Test Plans and Steps for testing each requirement or defect/bug	Electronically in MS Excel or MS Word or PowerPoint	Each Deploy Cycle Freeze Date	COR/CO via ITSS	Prior to Cycle Code Freeze	3.2
All Design Document	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All Software Requirement Specifications	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
All Meeting Minutes and Integrated Technology Initiative Proposal (ITIP)	Electronically in MS Excel or MS Word or PowerPoint	Three cycles a year	COR/CO via ITSS	Scheduled three (3) times a year	3.2
DoDD 8570 Cyber Security Certification	CompTIA Defined	Permanent	COR/CO via ITSS	At each renewal	3.2
Required Deliverables	**Format**	**Required Due Date**	**Send TO**	**Planned Frequency**	**PWS Reference**
Task 3.3 Field Support Deliverables					
TTP and/or Knowledge Article	Electronically in MS Excel or MS Word or	As required	COR/CO via ITSS	As required	3.3

	PowerPoint				
Quality Control Reports for Trouble Tickets	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.3
Trouble Ticket Report for Leadership Meeting	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.3
Trouble Tickets	Electronically in MS Excel or MS Word or PowerPoint	Thursday (weekly)	COR/CO via ITSS	2nd Thursday each Month	3.3
Systems Status Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.3
Event Mgmt. for Leadership Meeting	Electronically in MS Excel or MS Word or PowerPoint	Thursday (Weekly)	COR/CO via ITSS	2nd Thursday each Month	3.3
Shift Briefings	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	Daily	3.3
Ad Hoc Reports	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.3
Database Backup Report	Electronically in MS Excel or MS Word or PowerPoint	As required	Branch Chief/COR /CO via ITSS	Last Friday of each month	3.3
Assessment	Electronically in MS Excel or MS Word or PowerPoint	As required	AFPOA/DPOP/COR/CO via ITSS	Within 10 business days after consulting visit is completed	3.3
Required Deliverables	**Format**	**Required Due Date**	**Send TO**	**Planned Frequency**	**PWS Reference**
Task 3.4 Operations Support & Data Center Operations Deliverables					

Configuration Mgmt. Change Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.4
Software & Hardware Failures Resolution Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.4
Results Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.4
Shell Scripting Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.4
Required Deliverables	**Format**	**Required Due Date**	**Send TO**	**Planned Frequency**	**PWS Reference**
Task 3.5 Cybersecurity & Portfolio Mgmt. Support Deliverables					
Project Plan	Electronically in MS Excel or MS Word or PowerPoint	Within 3 business days following the assignment of each task	AFPOA Technical Points of Contact/ COR/CO via ITSS	As required	3.5
A&A Package	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Project Plan Updates	Electronically in MS Excel or MS Word or PowerPoint	Weekly	COR/CO via ITSS	As required	3.5
Security Categorization Document	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
STIG Applicability List	Electronically in MS Excel or MS Word or	As required	COR/CO via ITSS	As required	3.5

	PowerPoint				
SSP	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
PPSM	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Threat/Risk Assessment	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
PIA	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Contingency Plan	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
IRP	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
CM Plan	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Security Checklists	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
ACAS Scans	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO	As required	3.5
SCAP Scan	Electronically in MS Excel or MS Word or	As required	COR/CO via ITSS	As required	3.5

	PowerPoint via ITSS				
Code Scans	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
PPS Worksheet	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
RAR	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Security Plan & RAR	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
AF software certification documentation & software testing actions	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Network Boundary Configuration	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
POA&M	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Security Plan, POAM & RAR updates	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Annual FISMA Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5

AF Software Certification Documentation & Software Testing Actions	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Application request worksheets	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
ARW & Application Testing Results	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	Shall be delivered in accordance with the milestone identified within the applicable Project Plan.	3.5
Certification Memo	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Software Certification Package	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Scan Results Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Mitigation Plan	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.5
Required Deliverables	**Format**	**Required Due Date**	**Send TO**	**Planned Frequency**	**PWS Reference**
Task 3.6 Lifecycle Management Support Deliverables					
AFPOA EA models	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.6
AFPOA Portfolio Capability	Electronically in MS Excel or	As required	COR/CO via ITSS	As required	3.6

Development Roadmaps	MS Word or PowerPoint				
RMF Artifacts	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.6
Courses of Action	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.6
IT Refresh Plan	Electronically in MS Excel or MS Word or PowerPoint	Quarterly by 1 Jan, 1 April, 1 July, 1 Oct	COR/CO via ITSS	Quarterly by 1 Jan, 1 April, 1 July, 1 Oct.	3.6
Deployment Plan	Electronically in MS Excel or MS Word or PowerPoint	Quarterly by 1 Jan, 1 April, 1 July, 1 Oct	COR/CO via ITSS	Quarterly by 1 Jan, 1 April, 1 July, 1 Oct	3.6
Report	Electronically in MS Excel or MS Word or PowerPoint	As required	COR/CO via ITSS	As required	3.6

The method of surveillance for each of the primary tasks the Contractor is required to perform under Section 3 of this PWS is disclosed/included in the attached Quality Assurance Surveillance Plan ((QASP) reference Attachment 3), which shall become binding upon the Contractor at the time of award.

6.1. Delivery Instructions

Copies of deliverables shall be furnished to the appropriate Government personnel per the chart in Section 6. The Contractor shall deliver each report in accordance with the direction in the chart in Table 1, Section 6. Deliverables are to be transmitted with a cover letter, on the prime Contractor's letterhead, describing the contents. Concurrently, a copy of the deliverable and the cover letter shall be attached to the task in GSAs Electronic Ordering System (ITSS).

Contractor must submit their required deliverables/reports as part of this task order through ITSS.

6.2. Inspection and Acceptance of Services

All reports and task deliverables shall be inspected, tested (where applicable), reviewed, or returned for comments prior to final acceptance by the Government within 5 business days. The contractor will have 3 business days to make corrections and provide a finalized report or deliverable. The Government will have 3 business days to provide final acceptance after review of all reports and task deliverables. Further inspection and acceptance details are outlined in the QASP **(Attachment 3).**

Inspection and Acceptance under the terms of this T&M order shall be performed in accordance with FAR 52.212-4, Alternate I (Jan 2017).

The Contractor shall only tender for acceptance those items that conform to the requirements of this task order. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or re-performance of nonconforming services at no increase in price. If repair/replacement or re-performance will not correct the defects or is not possible, the government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights.

6.2.1. Within a reasonable time after the defect was discovered or should have been discovered; and

6.2.2. Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

Only the client representative (CR), their designated alternate, the GSA Project Manager (PM) or GSA Contracting Officer (CO) has the authority to inspect, accept, or reject all deliverables. Final acceptance of all deliverables will be provided in writing, or in electronic format, to the GSA PM or GSA CO within 30 days from the end of the task order.

6.3. Contractor Quality Control Requirements

The task order is for performance based commercial services. The contractor shall develop and maintain a quality process to ensure services are performed in accordance with commonly accepted commercial practices and existing quality control systems throughout the life of the order.

The contractor shall develop and implement procedures to identify, prevent and ensure non-recurrence of defective services. However, the government reserves the right to perform inspections on services provided to the extent deemed necessary to protect the government's interests. The contractor must control the quality of the services and deliverables provided in support of this task; the contractor must maintain substantiating evidence that services conform to task order quality requirements and furnish such information to the government if requested.

The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the services are performed in accordance with PWS and commonly accepted commercial practices, throughout the life of the task order. The QCP shall include a Quality Control Matrix (QCM) that addresses all deliverables in Table 1, of Section 6. The QCM shall reflect the method by which the contractor will meet the level of required performance and quality reflected in Table 1 of Section 6.

7. Security Requirements

The Contractor must possess or obtain an appropriate facility security clearance (Secret) prior to performing work on a classified government task order. If the Contractor does not possess a facility clearance the government will request one. The government assumes costs and conducts investigations for Secret, and Confidential facility security clearances. The Contractor shall request personnel security clearances, at the company's expense, for employees requiring access to classified information within 15 days after receiving a facility clearance or, if the Contractor is already cleared, within 15 days after service award. Due to costs involved with security investigations, requests for personnel security clearances shall be kept to the minimum amount employees required to perform task order requirements.

7.1. Listing of Employees. The contractor shall maintain a current list of employees. The list shall be validated and signed by the company *Facility Security Officer* (FSO) and provided to the *Information Protection Office* (IP Office) at each performance site 30 days prior to the service start date. Updated listings shall be provided when an employee's status or information changes. A Visit Request for all employees with a security clearance is required to be sent through the Joint Personnel Adjudication System (JPAS), and must be updated at least annually. The contractor shall notify the Information Protection Office at each operating location 30 days before on-base performance of the service. The notification shall include:

7.1.1. Name, address, and telephone number of company key management representatives.
7.1.2. The task order number and contracting agency.
7.1.3. The highest level of classified information to which employees require access.
7.1.4. The location(s) of service performance and future performance, if known.
7.1.5. The date service performance begins.
7.1.6. Any change to information previously provided under this paragraph.

7.2. Suitability Investigations. Contractor personnel not requiring access to classified shall successfully complete, as a minimum, a Tier 1 (T1) investigation, before operating government furnished workstations. The contractor shall comply with the DoD 5200.2-R, *Personnel Security Program*, AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, and AFI 33-200, *Information Assurance (IA) Management*, requirements. T1 investigation requests are initiated using the Standard

Form (SF) 85 and are submitted to the installation Information Protection Office through the using agency's Unit Security Manager. T1 investigations are different from the Wants and Warrants checks, and are provided by the government at no additional cost to the contractor.

7.3. Pass and Identification Items: The contractor shall ensure the following pass and identification items required for service performance are obtained for employees and non-government owned vehicles.

a. Installation Access Pass (IAP) (DBIDS), Visitor/Vehicle Pass (AFMAN 31-116), used for contracts for less than six months to include one-day visits (i.e. warranty work)..

b. Installation Access Card (IAC) (DBIDS), (AFMAN 31-113), used for contracts for more than six months or more.

c. DoD Common Access Card (CAC), (AFI 36-3026), used for contracts for more than six months and requirement exists for access to the government computer systems and software. CAC applications are accomplished by Trusted Agents via the Trusted Agent Sponsorship System (TASS).

7.4. Security Manager Appointment. The Contractor shall appoint a security representative for the on base long term visitor group. The security representative may be a full-time position or an additional duty position. The security representative shall work with the host organization to provide employees with training required by DOD 5200.01, Information Security Program, and AFI 16-1404, Air Force Information Security Program. The Contractor shall provide initial and follow-on training to Contractor personnel who work in Air Force controlled/restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101, Integrated Defense.

7.5. Security Clearance Requirements. The contractor must possess or obtain an appropriate facility security clearance, (Secret) prior to performing work on a classified government contract. If the contractor does not possess a facility clearance the government will request one. The government assumes costs and conducts investigations for Top Secret, Secret, and Confidential facility security clearances. The contractor shall request personnel security clearances, at the company's expense, for employees requiring access to classified information within 15 days after receiving a facility clearance or, if the contractor is already cleared, within 15 days after service award. Due to costs involved with security investigations, requests for personnel security clearances shall be kept to the minimum amount employees required to perform contract requirements.

Additional Security Requirements: In accordance with DoDM 5200.01, *Information Security Program* and AFI 16-1404, the contractor shall comply with AFSSI 7700, *Emission Security* (EMSEC) Program; applicable AFKAGs, AFIs, and AFSSIs for Communication Security (COMSEC); and AFI 10-701, *Operations Security (OPSEC) Instructions*. The contractor will comply with DoD Standard 22/Force Protection Condition Measures, DoD Standard 25/Level I-AT Awareness Training, and associated tasking contained in AFI 10-245, Antiterrorism (AT) standards. Level I AT Awareness training is available for contractor personnel and can be requested by calling the local installation AT Office.

7.6. Security Facility Clearance Requirements

The Contractor must possess or obtain an appropriate facility security clearance as identified below prior to performing work on a classified government task order:

( ) Top Secret

(X) Secret

If the Contractor does not possess a facility clearance the government will request one. The Contractor shall notify the 502nd Security Forces Squadron, Plans and Programs Flight, Information Protection (502 SFS/S5X/IP) before on-base performance of the service. The notification shall include:

7.6.1. Name, address and telephone number of company representatives.
7.6.2. The task order number and contracting agency.
7.6.3. The highest level of classified information which Contractor employees require access to.
7.6.4. The location(s) of service performance and future performance, if known.
7.6.5. The date service performance begins.
7.6.6. Any change to information previously provided under this paragraph.
*** See Section 7.18 on how to complete this action***

7.7. Personnel Security Clearance Requirements

Some or all of the personnel performing work on this task order will require a security clearance as identified below:

( ) Top Secret

(X) Secret

7.8. Additional Investigation Requirements

Anyone working on the task order that does not require a security clearance must have at a minimum a favorably adjudicated National Agency Check with Written Inquiries (NACI) investigation to access a government furnished information system or

environment. This investigation must be submitted by the task order company. Note: AFI 31-501, and AFI 31-601 for unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/or sensitive equipment.

7.9. Visit Requests

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

7.10. Pass and Identification Items

The Contractor shall ensure the following identification items as required for task order performance are obtained for employees:

7.10.1. DoD Common Access Card (AFI 36-3026).

7.10.2. Base-specific identification as required by local base and/or building security policies.

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

The Contractor shall ensure the following pass and identification items required for service performance are obtained for employees and non-government owned vehicles:

7.11. Installation Access Pass (IAP) (DBIDS), Visitor/Vehicle Pass (AFI 31-113), used for task orders for less than six months to include one-day visits (i.e. warranty work).

7.12. Installation Access Card (IAC) (DBIDS), (AFI 31-113), used for task orders for more than six months or more.

7.13. DOD Common Access Card (CAC), (AFI 36-3026), used for task orders for more than six months and requirement exists for access to the government computer systems and software. CAC applications are accomplished by Trusted Agents via the Trusted Agent Sponsorship System (TASS).

7.14. Visitor Group Security Agreement (VGSA)

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

7.14.1.1. Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, *Industrial Security Regulation,* Air Force Policy Directive 16-14, *Security Enterprise Governance,* and Air Force Instruction 16-1406, *Air Force Industrial Security Program.*

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

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

7.15. Obtaining and Retrieving Identification Media. As prescribed by the AFFAR 5352.242-9000, Contractor access to Air Force installations, the Contractor shall comply with the following requirements:

7.15.1. The Contractor shall obtain installation access passes for all Contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the task order. Contractor personnel are required to wear or prominently display installation identification badges or Contractor-furnished identification badges while visiting or performing work on the installation.

7.15.2. No later than three working days prior to task order commencement, the Contractor shall submit a written request on company letterhead to the Government POC listing the following: task order number, location of work

site, start and stop dates, and names of Contractor employees needing access to the base. The authorized Government POC will endorse the request and forward it to the issuing base pass and registration office or security forces for processing. Contractors will present government (state or federal) issued ID, and INS Form 9 (I9), before being issued a pass to enter the installation. Before being issued a pass to enter the installation, a Wants and Warrants check will be conducted for every individual requesting a pass. Personnel employed by the Contractor must get a pass for their privately owned vehicles at the installation Visitor Reception Center, with proof of following:

7.15.2.1. Liability Insurance
7.15.2.2. Current License Plates
7.15.2.3. Current State Inspection Sticker (If Required)
7.15.2.4. Valid State Driver License
7.15.2.5. A phone number for sponsor on base

7.15.3. Vehicles owned by the Contractor with the company name permanently printed on them are not required to obtain a pass as long as a current work order is presented at the time of entry. However, current liability insurance, state inspection sticker, and registration is required. The person driving the vehicle must have a valid operator license for the type of vehicle.

7.15.4. Upon completion or termination of the task order or expiration of the identification passes, the Contractor shall ensure that all base identification credentials issued to Contractor employees are returned to the issuing office. If a Contractor employee has been terminated, the credentials will need to be retrieved and returned to issuing activity so that employee does not have base access. If the credential is not retrieved then SF will need to be notified so base access is not allowed.

7.15.5. Failure to comply with these requirements may result in withholding of final payment.

7.16. Reporting Requirements

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

7.17. Physical Security

Areas controlled by contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and local search/identification requirements. The contractor shall safeguard all government property, including controlled forms, provided for contractor use. At the close of each work period, government training equipment, ground aerospace vehicles, facilities, support equipment, and other valuable materials shall be secured. During increased FPCONs, contractors may have limited access to the installation and should expect entrance delays.

7.18. Operating Instructions

For controlled areas used exclusively by the contractor, the contractor shall develop an Operating Instruction (OI) for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations. The OI shall be written in accordance with AFI 31-101, the local base Operations Plan usually referred to as an OPLAN and AFI 10-245, *Air Force Antiterrorism (AT) Standards*, and coordinated through the Information Protection (IP) office.

7.19. Government Authorization Key Control

The contractor shall establish and implement key control procedures in the Quality Control Plan to ensure keys issued to the contractor by the government are properly safeguarded and not used by unauthorized personnel. The contractor shall not duplicate keys issued by the government. Lost keys shall be reported immediately to the contracting officer. The government replaces lost keys or performs re-keying. The total cost of lost keys, re-keying or lock replacement shall be deducted from the monthly payment due to the contractor. The contractor shall ensure its employees do not allow government issued keys to be used by personnel other than current authorized contractor employees. Contractor employees shall not use keys to open work areas for personnel other than contractor employees engaged in performance of duties, unless authorized by the government functional area chief.

7.20. Security Lock Combinations

7.21. The contractor shall establish procedures in local OIs ensuring lock combinations are not revealed to unauthorized persons and ensure the procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional area chief. Records with written combinations to authorized secure storage containers or Secure Storage Rooms (SSR), shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers. The contractor shall comply with DoDM 5200.01, Vol

3 security requirements for changing combinations to storage containers used to maintain classified materials. **Freedom of Information Act Program (FOIA*)***
The contractor shall comply with DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom Of Information Act Program,* requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding *For Official Use Only (FOUO)* material. The contractor shall comply with AFI 33-332, *Privacy Act Program*, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall remove or destroy official records only in accordance with AFI 33-322 *Records Management*, or other directives authorized in AFI 33-364, *Records Disposition—Procedures and Responsibilities*.

7.22. Traffic Laws

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

7.23. Healthcare

Healthcare provided at the local military treatment facility on an emergency reimbursable basis only.

8. Required Skills and Knowledge

8.1. Key Personnel

The offeror shall submit a staffing plan/manning table showing full and part-time positions to include the proposed labor categories and skills matched to the skill requirements and hours estimated by the government and listed in the Appendix F-Pricing Worksheet. The staffing plan shall link the proposed labor categories to the specific areas of support they will be working. Key Personnel resumes shall be submitted with the Staffing Plan. The following positions will be considered to be key positions under this PWS:

8.1.1. Program Manager: This is a key personnel position. The program level Program Manager should have no less than 10 years of experience managing programs, developing plans, implementing and controlling assigned portions of relevant programs. Establishes performance objectives for assigned programs. Ensures cost, technical and schedule objectives are met. Reports program progress and status. Serves as primary contact between AFPOA and the Contractor.

8.1.2. Help Desk Manager: This is a key personnel position. Should have no less than 3 year of experience for overall responsibility of help desk operations associated with the identification, prioritization and resolution of reported

problems. Ensures that all phases of help desk support are properly coordinated, monitored, logged, tracked and resolved appropriately. May maintain responsibility for development, maintenance and integrity of help desk software.

8.2. Additional Labor Category Descriptions

The additional labor categories and years of experience in this PWS Section 8.2 represent the Government's recommendations only. The descriptions of the labor categories provided are the expected work to be performed by the position. Contractors may deviate from the labor categories when responding to this proposal however deviations must be identified in the proposal.

Additionally, contractor may deviate from the recommended years of experience so long as the employee can meet the requirements in the labor descriptions.

8.2.1. **Computer Analyst:** Applies systems analysis and design skills in an area such as a record keeping or scientific operation. A system of several varied sequences or formats is usually developed, e.g. the analyst develops systems for maintaining depositor accounts in a bank, maintaining accounts receivable in a retail establishment, maintaining inventory accounts in a manufacturing or wholesale establishment, or processing a limited problem in a scientific project. This position requires competence in most phases of system analysis and knowledge of pertinent system software and computer equipment and of the work processes, applicable regulations, workload, and practices of the assigned subject-matter area. Job duties require the incumbent to be able to recognize probable interactions of related computer systems and predict impact of a change in assigned system.

8.2.2. **Business Objects Consultant:** Applies solid, fundamental skills and IT technical expertise for Business Objects (BO) versions XI3, or XI4. Provides knowledge of SAP Business Intelligence (BI) Suite with enhanced implementation abilities including PKI authentication, Single Sign On using Apache Tomcat and BI SDK experience. Applies strong industry background to support complex migration, upgrade and performance tuning methods and tools. Analyze and interpret system architecture, problem reports and data to reveal problem areas and develop best practice solutions. Organize and execute assigned projects according to requirements.

8.2.3. **Enterprise Architect:** Supports complex projects applying the organizing principles, methods and tools of enterprise architecture. Enterprise Architects provide subject matter expertise in industry, process and/or technology areas

an possess capabilities in specific methods including, architecting enterprise strategy, enterprise architecture development & management, business process design & re-engineering, investment decision making and support for solution architecture development/management. They support the attainment of business strategy and its alignment with processes and information technology strategy.

8.2.4. **Information Assurance (Cybersecurity) Analyst:** Provide support to plan, coordinate, and implement AFPOA's Risk Management Framework (RMF) processes for authorizing AFPOA IT systems. Performs risk analyses which also includes risk assessment. Have experience of the RMF Authorization and Assessment (A&A) process as defined in the DOD and Air Force implementation guidance. Personnel shall be highly experienced in conducting A&A, analyzing any findings, and have the requisite skill sets and experience needed to produce and or assist AFPOA's associated customers and subordinate units in producing the required RMF documentation. Personnel shall have expertise in working DOD policy and procedures related to the PWS requirements. Information Assurance Analyst V should have is no less than 8 years of experience.

8.2.5. **System Administrator:** Ensures long-term requirements of systems and database operations and administration are included in the overall information systems planning of the organization. Responsible for the installation, maintenance, configuration, and integrity of computer databases and software. Implements operating system enhancements that will improve the reliability and performance of the system.

8.2.6. **Senior Application Developer:** Recommend experience of no less than 5 years writing C# using Microsoft Visual Studio and be able to design, create, modify, debug, correct, combine, refactor, and field web applications, web services, stand-alone executables and dynamic link libraries. Should have no less than 5 years of experience writing Structured Query Language using Microsoft SQL Server Management Studio and be able to design, create, modify, debug, correct, combine, refactor, and field database tables, views, stored procedures, and triggers. Should have no less than 3 years of experience writing multi-threaded applications using Microsoft Visual Studio Structured Query Language and be able to design, create, modify, debug, correct, combine, refactor, and field multi-threaded applications and modules.

8.2.7. **Senior Enterprise Architect:** Recommend experience of no less than 7 years applying management skills and specialized functional and technical expertise to support complex projects applying the organizing principles, methods and tools of enterprise architecture. Senior Enterprise Architects provide subject matter expertise in industry, process and/or technology areas and have specific knowledge of specific methods including, architecting enterprise strategy, enterprise architecture development & management, business process design & re-engineering, investment decision making and support for solution architecture development/management. They are versed in interfacing with senior program and functional leadership in the development and subsequent management of organizational plans. They support the development of business strategy and its application to and alignment with processes and information technology strategy.

8.2.8. **Senior Information Assurance Engineer:** Recommend experience of no less than 8 years in Information Security of which at least 4 years of experience must be Information Assurance experience. Must have experience in information systems security auditing, vulnerability assessment, risk assessment, and penetration testing. Knowledgeable of federal information security and information assurance policies, standards, and regulations. Gathers and organizes technical information relevant to an organization's information security policies, training, security awareness, IT infrastructure, existing security posture, continuous monitoring strategies. Provides technical guidance and assists the customer in improving information security, knowledge, and awareness.

8.2.9. **Senior System Administrator:** Performs all of the Systems Administrator duties and able to integrate new technologies into new and existing systems, including the transition and migration of systems. The isolation and resolution of complex hardware and software problems involving the application, the operating system, the hardware, the communications infrastructure, or any combination thereof.

8.2.10. **Senior Systems Engineer:** Shall have Certifications in OpenText LiveLink Server Administration, A+, Security+, MCSE and recommended experience of no less than 10 years. Senior Systems Engineers shall perform system administration, backup and recovery tools and techniques, storage management and storage devices, security assessment and preventative measures, user account management, network connectivity and communications, performance measure and management, system tuning,

hardware technologies including latest trends. Functional Responsibility: System Administration, Acquisition, Change Management, Asset Management, CRM / Helpdesk, Information Assurance, Product and Proposal Evaluation.

8.2.11. **Asset Management Specialist:** Reviews and coordinates complex activities related to real properties, financial instruments and operating businesses or other equity. Tracks and monitors all real properties and operating businesses and related issues; assists in monitoring all real property, financial instruments operational businesses and related issues. Attends client meetings and briefings related to equity asset management.

8.2.12. **Tenant Manager-1:** Directs daily tenant service operations for small/single accounts to ensure employees have appropriate equipment and resources to perform their jobs and meet goals and deadlines. Ensures proper operations of building(s) through managing, maintaining and regulating systems. Probes potential problems and apprises manager or client (as appropriate) of status on resolution of problems or issues, using appropriate resources when necessary. Supervises day-to-day tenant service work activities by delegating authority, assigning and prioritizing activities and monitoring operating standards. Manages by providing positive and constructive feedback to employees in order to reward, coach, correct and motivate. Establishes a safe work environment for employees by providing safety-related training with standards and procedures for the handling and storage of furniture, inventory, etc. Establishes operating standards, implements quality improvements and communicates them to employees and client. Reviews and evaluates incoming requests for small moves within service level agreement timelines. Identifies existing furniture solutions currently in place and develops standard operating procedures for all furniture activity. Provides customer interface to validate office vacancies, floor plans and proper occupancy information. Creates move packets and necessary work orders for move vendors. Participates in all major facility project meetings. Conducts analysis and assists project managers in developing furniture budgets and solutions. Coordinates strategic planning for moves, additions and/or changes, and delivers budgetary forecasting and assists with invoice coding. May coordinate audio-visual and telephone equipment for conference room and event setup within the assigned facility.

8.3. Time and Materials (T&M) Labor

The Government estimates that the base year plus four option periods will involve a Time and Materials (T&M) per year delineated below. This estimated workload is based on past needs and projected requirements. Offerors shall quote only those personnel possessing qualifications and experience requirements which reflect an ability to perform all responsibilities for the specified labor category. The estimates in

Appendix F: PRICING WORKSHEET is only a "guide" and is not intended to limit or require a proposal submission based on these figures.

Labor shall be performed at the rate agreed to at the time of task order award for the base period (and option periods, if applicable), and no additional rate increases shall be allowed after award. All awarded rates shall be fully-burdened FFP rates, and the rates shall not be subject to "finalized audited rates" by the Defense Contract Management Agency (DCAA) or other third party auditor.

The awarded estimate for each labor category is considered a labor category ceiling. After award, the contractor must not utilize and subsequently bill above each awarded labor category ceiling without a written modification from the Contracting Officer. Within those labor category ceiling amounts, the contractor must not independently decide which labor categories may be utilized and subsequently billed in support of the client's requirements without prior written approval from the client and GSA COR. The contractor understands that neither the funded amount, ceiling value, nor the hours on the T&M, is a guarantee to the contractor. The total task order ceiling value may not be exceeded without a written modification from the Contracting Officer.

9. Order Requirements Information

9.1. Type of Task

This is a performance based, commercial task order issued in accordance with FAR Part 12 and 16.5. This task order is an incrementally funded hybrid Time and Materials (T&M) and fully funded Firm Fixed Priced (FFP) task order. Award will be executed against the NETCENTS-2 Applications Services IDIQ contract vehicle.

9.2. Period of Performance (PoP) and FAR Clauses in Full Text or by Reference

The period of performance for this task is a one-year (12-months) base period with four one-year (12-months) option periods. The following FAR clauses pertain to the PoP, and are incorporated herein by reference and by full text:

9.2.1. This order will be placed against a NETCENTS-2 Application Services contract. All of the clauses and provisions contained in the NETSCENT-2 contract will apply to this task order. In addition to the applicable clauses contained in the NETCENTS-2 contract, the following FAR clauses are included in this task for added emphasis of their applicability:

Table 3 – Applicable Clauses

52.212-4, Alternate I	Contract Terms and Conditions – Commercial Items **(JAN 2017),** Times and Material or Labor Hour Contract
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)

9.2.2. Evaluation of Options:

Options shall be evaluated in accordance with the provision (as included herein) at FAR 52.212-2(b), Evaluation – Commercial Items.

9.2.3. FAR Clause 52.217-8 Option to Extend Services (NOV 1999):

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within thirty (30) calendar days prior to the expiration of the contract.

9.2.4. FAR Clause 52.217-9 Option to Extend the Term of the Contract (Mar 2000):

The Government may extend the term of this contract by written notice to the Contractor at least 60 days prior to the expiration of the current period of performance provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

If the Government exercises this option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed five year and six months (if the Option to Extend is exercised).

9.2.5. GSAR 552.217-71 Notice Regarding Option(s) (NOV 1992):

GSA has included an option to *extend the term of this contract* in order to demonstrate the value it places on quality performance by providing a mechanism for continuing a contractual relationship with a successful Offeror that performs at a level which meets or exceeds GSA's quality performance expectations as communicated to the Contractor, in writing, by the Contracting Officer or designated representative. When deciding whether to exercise the option, the Contracting Officer will consider the quality of the Contractor's past performance under this contract in accordance with 48 CFR 517.207.

9.3. Performance Specifics

9.3.1. Performance Location

Work shall be performed onsite at the primary Government place of performance. Travel to other Government or Contractor facilities may be required at the Government's request.

1960 1st Street West, Bldg. 977
JBSA Randolph, TX 78150-4453

Contractor personnel will not report to Government facilities to work nor remain at the work locations any time the Government is unexpectedly required to close their offices. The contractor will not be compensated for these unexpected or expected Government closures. The contractor is responsible for all notification of their contractor staff during times of closure.

9.3.2. Performance Time/Days

The Government site is open during normal business hours Monday through Friday (0700-1630), except Federal holidays. The Contractor shall also provide 24/7 support and support other individual Tasks 1-6 business hours identified in Section 3 Requirements.

The dates/times the contractor personnel work to support the objectives of this requirement are at the contractor's sole discretion however onsite work at the Government facility must fall within above business hours. This order is performance based, and all tasks must be completed timely and at the level of quality identified herein.

9.3.3. Observed Federal Holidays**

The following Federal holidays are observed by the Government and affect the contractor's ability to access Government's facilities or Government personnel:

New Year's Day:	January 1st
Martin Luther King's Birthday:	3rd Monday in January
President's Day:	3rd Monday in February
Memorial Day:	Last Monday in May
Independence Day:	July 4th
Labor Day:	1st Monday in September
Columbus Day:	2nd Monday in October
Veterans Day:	November 11th
Thanksgiving Day:	4th Thursday in November
Christmas:	December 25th (and possibly the day after or before, depending on an executive order)

9.3.4. Productive Labor Hours

If personnel have to obtain a background check prior to being able to perform under the terms of the order, the contractor is not permitted to bill (in the case of a T&M order type) until the contractor's personnel are fully able to perform the requirements of the PWS.

9.4. Homeland Security Presidential Directive-12 (HSPD-12)

Homeland Security Presidential Directive 12 (HSPD-12) was issued to implement the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). Under this directive, the heads of executive departments and agencies are required to implement programs to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. This policy can be found at the following website:

http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html .

In performance of services under this task, contractor shall insure all its personnel who require physical access to federally controlled facilities and access to federally controlled information systems by 27 October 2007, have been issued identification in compliance with HSPD-12 policy. In their solicitation response packages, offeror's shall confirm they will comply with the government client's identification procedure that is implementing HSPD-12 policy. The Security/Identification point of contact for the client agency that is responsible for implementing their HSPD-12 compliant policy is:

POC Name	AFPOA Security Manager
Email address	Afpoa.security.manager@us.af.mil

All costs associated with obtaining necessary clearances shall be borne by the contractor.

9.5. Federal Information Security Management Act (FISMA) of 2014 Compliance:

FISMA compliance is access through annual accreditation and certification as required by Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) governed by Department of Defense Instruction 8510.01, dated March 12, 2014. Note: This requirement must be met on any

procurement, IT, PS, etc., where the contractor will have access to government electronic information.

In order to satisfy this requirement, GSA requires FISMA point of contact for the client agency that is responsible for maintaining their annual FISMA accreditation and certification:

Agency official for FISMA compliance below:

POC - Name	Becky Thompson
Office Symbol	AFPOA/DFCC
Telephone #	(210) 565-4249
Email	rebecca.thompson.5@us.af.mil

9.6. Organizational Conflict of Interest (OCI)

The guidelines and procedures of FAR Subpart 9.5 and GSAM Subpart 509.5, Organizational and Consultant Conflicts of Interest, and FAR Part 3 and GSAM Part 3, Improper Business Practices and Personal Conflicts of Interest, will be used in identifying and resolving any issues of a conflict of interest under this task order.

In the event that this task order requires activity that would create an actual or potential conflict of interest, the Contractor shall immediately notify the Ordering Contracting Officer (OCO) of the conflict, submit a plan for mitigation, and not commence work until specifically notified by the OCO to proceed; or, identify the conflict and recommend to the OCO an alternate approach to avoid the conflict. The Contractor shall not contract with Government prime Contractors or first-tier subcontractors in such a way as to create an organizational conflict of interest. Offerors are required to disclose any existing or potential Conflict of Interest (COI) in their quotes as well as submit a COI Mitigation Plan proposing measures to avoid, mitigate or neutralize identifies COI's.

Definitions. "Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract. "Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

9.7. Applicability of Terms and Conditions from the Base Contractual Vehicle(s):

All applicable terms and conditions from the contactor's basic NETCENTS II Indefinite Delivery Indefinite Quantity (IDIQ) Contract, and the additional terms of this task order, shall become legally binding upon the contractor at the time of award and through the period of performance.

10. Travel (CLIN 0002/ NETCENTS CLIN 1700)

The Contractor shall coordinate specific travel arrangements with the AFPOA COR to obtain advance, written approval for the travel about to be conducted. Reference Appendix F, Pricing Worksheet for estimated travel costs.

10.1. Travel Requirements

Travel Time (T&M Tasks): In support of this task order, contractor personnel may be required to travel to various locations and work in excess of 40 hours/week on occasion. During performance, only actual travel costs are reimbursed in accordance with the Federal Travel Regulations (FTR) and other applicable regulations, subject to the Government's approval. On the first and last day of approved contractor personnel travel, the rate is 75 percent of the appropriate Meals and Incidental Expenses (M&IE) rate regardless of the departure and return time.

10.1.1. Trip Reports

10.1.1.1. For all travel required under the terms of this PWS, the contractor shall submit Trip Reports when submitting monthly invoices after completion of a trip for all long distance travel and for local travel when requested by AFPOA COR. Trip reports shall be uploaded into ITSS once a month when invoices are uploaded.
The Trip Report shall include the following information:

10.1.1.1.1. Personnel traveled
10.1.1.1.2. Dates of travel
10.1.1.1.3. Destination(s)
10.1.1.1.4. Purpose of Trip; task effort supported and Task Order ID number; Government Agency supported (if applicable), explain the benefits of the travel to the Government.
10.1.1.1.5. Actual Trip Costs
10.1.1.1.6. Approval Authority
10.1.1.1.7. Summary of events

10.1.2. Approval for Travel

All travel shall be scheduled at least two weeks in advance whenever possible to maximize savings to the Government through receiving the best travel rates available. Emergency requirements shall be defined and approved by the COR. All travel shall be in accordance with the Federal Travel Regulation (FTR) and shall be at or below per diem unless approved via CTP. The contractor is required to ensure good stewardship of travel funds, and shall seek rates lower than per diem whenever possible.

The contractor shall make every effort to locate the airport that will provide the lowest cost of air travel possible. Travel shall be at the allowable per diem rate. In the event travel charges are above per diem, the contractor shall submit a "**Consent to Purchase (CTP)" form (Attachment 2)** with a complete explanation to explain the circumstances to the COR and GSA CO for approval. Travel charges above the per diem shall be approved by the GSA CO. Travel charges over and above per diem without proper approval, shall be at the expense of the contractor.

After travel is incurred, documentation/receipts shall be uploaded to ITSS with the invoice submittals. NO PAYMENT WILL BE MADE WITHOUT DOCUMENTATION/RECEIPTS. See Section 11.4 for further details regarding invoicing for travel.

The COR shall approve all CONUS travel in advance (in writing on the CTP form). The GSA CO shall approve all travel expenses for all overseas travel.

NOTE: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel, materials, and ODC procurements (travel) made on behalf of the Government under the terms of the task order.

11. Invoicing/ Procedures for Payment

11.1. Electronic Posting of Invoices

Contractors shall electronically transmit/submit invoices and supporting documentation for invoices through the GSA web-based procurement system, through the Central Invoice Service (CIS), the contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. This is the only acceptable means for invoice submissions. **No paper invoices shall be accepted.** For additional assistance contact the ASSIST Helpdesk at 877-472-4877.

11.2. Invoicing Instructions Based on Order Type

The contractor shall submit only one invoice per month for the task order. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

11.2.1. The end of the invoiced month (for services) or

11.2.2. The end of the month in which the products (commodities/materials) or deliverables (fixed-priced services) were delivered and accepted by the Government.

11.3. Invoice Content

The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum:

11.3.1. GSA Task Order Number

11.3.2. Task Order ACT Number (see the front of the SF300 document)

11.3.3. Prompt Payment Discount

11.3.4. Remittance Address

11.3.5. Period of Performance for Billing Period
11.3.6. Point of Contact and Phone Number
11.3.7. Invoice Amount
11.3.8. Skill Level Name and Associated Skill Level Number (for T&M or Labor Hour)
11.3.9. Actual Hours Worked During the Billing Period (for T&M or Labor Hour)
11.3.10. Travel Itemized by Individual and Trip (if applicable)
11.3.11. Training Itemized by Individual and Purpose (if applicable)

NOTE: ***Normally, the Government does not pay for contactor training. Training will need to be coordinated and approved (via CTP form) by the COR, prior to the training being taken.***

Support Items Itemized by Specific Item and Amount (if applicable) The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

11.4. Travel Invoicing

Travel shall be approved per the terms and conditions of the task order. Signed/approved Consent to Purchase (CTP) forms shall be submitted with the invoice, and all receipts for airfare, rental car, lodging, and all receipts directly being charged for over $75.00 shall be submitted as support/back up documentation with the invoice submittal. NO PAYMENT WILL BE MADE WITHOUT DOCUMENTATION/RECEIPTS. NO PAYMENT WILL BE MADE for travel that is non-conforming to the FTR.

11.5. Receiving/Client Agency's Acceptance

The Client Agency must accept the services and/or products provided under the terms of the task order.

The client agency will accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

The Client Agency may also generate a hard copy acceptance document.

Regardless, of the method of acceptance the contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. (Written acceptances will be posted as an attachment along with any other supporting documentation.) After acceptance of the

invoice by the Client Agency, the Contractor shall submit a proper invoice to GSA Finance not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item. In the absence of Government acceptance within thirty (30) days, the contractor shall submit an invoice.

NOTE: The acceptance of the authorized Client Agency representative (which is normally the COR) is REQUIRED prior to the approval of payment for any invoiced submitted.

NOTE: If the required documentation including, (A) the customer's signed written acceptance OR (B) the customer’s electronic acceptance, is not received within 15 calendar days from the date the invoice was submitted to GSA Finance, the invoice may be rejected in whole or in part as determined by the Government.

11.6. Final Invoice

Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA PM/COR before payment is processed, *if necessary.*

11.7. Order Close-out Procedures

The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. All invoices shall be received within this period. The contracting officer shall not extend the period of performance, or the invoice submittal period to wait on subcontractors to bill the prime contractor. All rates are negotiated at the time of award, and the contractor shall control and account for all time by their own personnel and their subcontractor or CTA personnel to allow for timely billing in accordance with the terms expressed in this section. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims form to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

The Government reserves the right to require a release of claims at the end of each performance period, after all payments have been completed. **NOTE: No rates agreed to under the terms of this order are subject to DCAA or other “final” audited rates.

11.8. Unilateral Close Out Modifications

FAR clause 52.212-4(c) is hereby amended as follows: The Government reserves the right to issue unilateral close out modifications to close out commercial contractual agreements, after the contractor has acknowledged the order is closed and that no further liability exists on behalf of the parties. The Government also reserves the right under the unilateral close out modification to deobligate money after full payment has been made to the contractor for their services/materials under this order.

11.9. Contract Performance Evaluation

IAW FAR 42.15 and FAR 16, the Government will provide and record Past Performance Information for acquisitions over $150,000 utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS process allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

Contractors are required to register in the CPARS, so contractors may review and comment on past performance reports submitted through the CPARS.

CPARS **https://www.cpars.csd.disa.mil/**
PPIRS **http://www.ppirs.gov**

11.10. Third Party Schedule Delays

GSA does not warrant and cannot guarantee that the site will remain free from interference by third parties, with whom the Federal Government has no contractual relationship. Only delays determined to be caused by the Federal Government that affect the contractor's ability to complete the task order work on time will be considered for time extensions and equitable adjustments.

12. PWS Attachment List:

ATTACHMENT 1: GOVERNMENT and CONTRACTOR FURNISHED PROPERTY, EQUIPMENT, AND SERVICES DOCUMENT
ATTACHMENT 2: CONSENT TO PURCHASE FORM (CTP) (Separate Excel Attachment)
ATTACHMENT 3: QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

ATTACHMENT 1:
GOVERNMENT and CONTRACTOR FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

A1. GOVERNMENT FURNISHED ITEMS AND SERVICES:

Facilities: The Government will provide the necessary workspace for the Contractor staff to provide the support outlined in the PWS to include desk space, telephones, computers, and other items necessary to maintain an office environment.

Equipment: The Government will provide access to scanners, fax machines and printers.

Documents: The Government will provide the AFPOA server details, AFPOA SOC services details, the contractor managed services document and the CSSP services document.

If the Government is furnishing Government Property in support of this contract, the contractor shall comply with FAR 52.245-1 and it's Alternates as appropriate. All Government Furnished Property shall be properly controlled/inventoried per the terms of this PWS.

A1.1 CONTRACTOR FURNISHED or ACQUIRED ITEMS AND SERVICES CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

General: The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not specifically listed in this PWS.
Secret Facility Clearance: The Contractor shall possess and maintain a SECRET facility clearance from the Defense Security Service. The Contractor's employees, performing work in support of this contract shall have been granted a SECRET security clearance from the Defense Industrial Security Clearance Office. The DD 254 is provided as Attachment 5.

Materials: The Contractor shall furnish materials, supplies, and equipment necessary to meet the requirements under this PWS in accordance with Section 3 of this PWS. If the contractor is acquiring materials after award of this contract under a material line item, the contractor shall comply with FAR 52.245-1 and it's Alternates as appropriate. All Contractor acquired property shall be properly controlled/inventoried per the terms of this PWS.

ATTACHMENT 2

Consent to Purchase Form-Separate Excel Document

ATTACHMENT 3

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

1.0 Introduction

This Quality Assurance Surveillance Plan (QASP) provides a systematic method to evaluate performance for AFPOA support. This QASP explains the following:

- What will be monitored.
- How monitoring will take place.
- Who will conduct the monitoring.
- How monitoring efforts and results will be documented.

This QASP does not detail how the contractor accomplishes the work. Rather, the QASP is created with the premise that the contractor is responsible for management and quality control actions to meet the terms of the contract. It is the Government's responsibility to be objective, fair, and consistent in evaluating performance. In addition, the QASP will recognize that unforeseen and uncontrollable situations may occur.

This QASP is a "living document" and the Government may review and revise it on a regular basis. However, the Government shall coordinate changes with the contractor. Updates shall ensure that the QASP remains a valid, useful, and enforceable document. Copies of the original QASP and revisions shall be provided to the contractor and Government officials implementing surveillance activities.

2.0 Objectives: The objective of this task order is to provide information technology (IT) solution support services.

3.0 ***Project Scope:*** The scope of this requirement is to acquire IT support services in the following task areas:

Task 1: Program Management
Task 2: Requirements Support
Task 3: Field Support
Task 4: Operations & Data Center Support
Task 5: Cybersecurity and Software Management Support
Task 6: Lifecycle Management Support

4.0 Quality Evaluation Areas

The contractor will be evaluated in the following areas:

- Technical Performance
- Schedule and Timeliness of Deliveries
- Contractor Resource Control (Cost)

- Customer Satisfaction (including: Communication Flow/Management, Business Relations Management, and Subcontractor Management (if applicable))
  In addition, each office or Directorate supported by Contractor personnel will provide an independent performance evaluation. Any discrepancies will be brought to the attention of the contracting officer.

5.0 Technical Performance

The contractor will be evaluated quarterly as to the quality of the output of their work and results will be documented in Contracting Officer's Representative's (COR's) file. The contractor's personnel should be technically competent in the tasks identified in the Performance Work Statement (PWS) or other ordering document under the contract. Included in the technical performance is the contractor's contribution in meetings and reviews, the quality of the contractor's technical reports, contractor's productivity and the overall quality of the technical support provided.

6.0 Schedule and Timeliness of Deliveries

The contractor shall be responsive to Government tasking's' and submit their monthly reports, technical reports, trip reports, etc. as required by the contract.

7.0 Contractor Resource Control (Cost)

The contractor shall use the funding authorized to provide support throughout the period of performance. The contractor will be evaluated in the successful control of resources devoted to the task or order. The COR shall compare monthly the contractor's rate of labor and funds usage with those allocated for the effort. Any discrepancies will be brought to the attention of the contracting officer.

8.0 Customer Satisfaction

The contractor shall put the appropriate effort in place to most efficiently perform the requirements provided in the PWS to the Governments satisfaction and standards. The Government shall perform surveillance to determine if the contractor exceeds, meets or does not meet these standards by providing periodic surveys to all customers and the results of these surveys shall be recorded by the COR. Any negative results shall be brought to the attention of the contractor for resolution.

Additionally, communication, business relations and subcontract management shall be considered under the area of customer satisfaction.

9.0 Quality Management Method

- **Quality Plan Processes**
- **Quality Assurance**
  Quality Assurance (QA) activities will focus on the processes being used to manage and deliver the solution to evaluate overall project performance on a regular basis. QA will ensure the project satisfies the quality standards and will define and record quality reviews, test performance, and customer acceptance.

- **Quality Control**
  Quality Control (QC) activities will be performed by the vendor to verify that project management and project deliverables are of high quality and meet quality standards. These standards are identified as part of vendor's proposal.

- **Quality Standards**

  Quality will be measured in accordance with meeting the objectives stated in the PWS. Therefore, acceptance of deliverables and satisfactory work performance shall be based on the objectives described in Table 1, QASP Performance Matrix.

Table 1 QASP Performance Matrix

Required Deliverables	Unsatisfactory	Marginal	Satisfactory	Exceptional	Surveillance Method
Quality of Delivered Services/Products	95% of the time contractor provides satisfactory quality of all deliverables as expected by the Government. Government intervention is necessary and significant; variances are not explained to satisfaction of the Government.	96% of the time contractor provides satisfactory quality of deliverables as expected by the Government. Government intervention is not necessary and variances can be explained to satisfaction of the Government.	98% of the time contractor provides satisfactory quality of all deliverables as expected by the Government. Government intervention is not necessary and variances can be explained to the satisfaction of the Government.	Performance meets contractual requirements 100% of the time and exceeds many to the Government's benefit. The contractual performance of the element or sub-element being assessed was accomplished with few minor problems for which corrective actions taken by the contractor was highly effective.	COR monitors performance through observation during weekly meetings and daily interaction at the work site. COR conducts inspection of deliverables.
Schedule	Contractor does not provide program support services on a timely manner	Performance meets contractual requirements 95% of the time and exceeds many to the Government's benefit. The contractual performance of the element or sub-element being assessed was accomplished	Performance meets contractual requirements 98% of the time and exceeds many to the Government's benefit. The contractual performance of the element or sub-element being assessed was accomplished	Performance meets contractual requirements 100% of the time and exceeds many to the Government's benefit. The contractual performance of the element or sub-element being assessed was accomplished	COR monitors performance through observation during weekly meetings and daily interaction at the work site. COR conducts 100% inspection of deliverables.

		with few minor problems for which corrective actions taken by the contractor was highly effective	with few minor problems for which corrective actions taken by the contractor was highly effective	with few minor problems for which corrective actions taken by the contractor was highly effective.	
Cost control	Contractor does not perform as proposed. There are cost overruns.	Contractor is partially performing with no cost overruns. No innovative techniques are used to bring overall expenditures within limits.	Contractor performance is consistent with the task order terms and conditions and PWS requirements. No cost overruns or invoice issues observed by the Government.	Costs are at or below original proposal. The contractor has identified efficiencies and innovations leading to the reduction of costs.	COR monitors performance through observation during weekly meetings and Monthly Status reports. COR conducts 100% inspection for compliance of all invoices.
Management of personnel, business relationships, and communication.	Contractor staff does not possess required skills and experience to perform the PWS tasks. Contractor does not respond to the Government's inquiries as required. Contractor does not alert the Government as required upon discovery of a technical or programmatic issue, which can significantly impact the cost, schedule, or technical performance. Contractor does not provide recommended corrective actions to the COR.	Contractor staff possesses required skills and experience to perform the PWS tasks. Contractor responds to the Government's inquires in more than one work day. Contractor alerts the Government within more than 5 days of discovery of a technical or programmatic issue, which can significantly impact cost, schedule or technical performance. Contractor provides recommended corrective actions to COR.	Contractor staff possess required skills and experience to perform the PWS tasks. Contractor responds to the Government's inquiries typically w within one work day. Contractor alerts the Government within 5 days of discovery of a technical or programmatic issue which can significantly impact cost, schedule or technical performance. Contractor provides recommended correction actions to the COR.	Contractor staff possesses or exceeds required skills and experience to perform the PWS tasks. Contractor responds to the Government's inquiries in less than one work day. Contractor alerts the Government in less than 5 days of discovery of a technical or programmatic issue, which can significantly impact, cost, schedule, or technical performance. Contractor provides recommended correction actions to the COR.	COR monitors contractor performance through Monthly Status Reports, staffing reports and staffing plan. COR conducts weekly inspections to monitor contractor personnel interactions with the Government. Periodic Inspection and 100% Inspection

Application Services Performance Parameters

Performance Requirements	Performance Threshold	Monitoring Method
SOFTWARE DESIGN, DEVELOPMENT & TESTING		
Software design	Produce or update all design documentation requested by the government within the time frame allotted and meeting standards	Documentation provided on time and within standards >90% of the time
Software implementation	Provide all code modules, test plans, and documentation for any change by code freeze date for each cycle. Update and change all required products as requested by government.	Items implemented into production must have <2 bugs for each 10 items.
Software testing	Work with appropriate government personnel to produce test plans when requested for any change	Provide within the time frame as requested by the government >90% of the time
Software delivery	Assist in creating the delivery plan for each deployment cycle	All steps provided in correct order >95%
Cybersecurity		
System security compliance	Maintain A&A compliance IAW applicable DoD and AF policy and instruction, particularly DoD Instruction 8500.01 – Cybersecurity	Random sampling, 100% inspection, periodic sampling
Application security compliance	Maintain application security compliance IAW applicable DoD and AF policy and instruction, particularly the Security Technical Implementation Guide (STIG)	Random sampling, 100% inspection, periodic sampling
Source Code Scanning	Source code scanning for applications is performed with software that can certify	Random sampling, 100% inspection, periodic

	quality application source code, e.g., Sonar.	sampling
Source Code Scanning	Source code scanning for applications is performed with software that can certify secure application source code, e.g., Fortify.	Random sampling, 100% inspection, periodic sampling
Database Scanning	Database scans will be performed to identify, mitigate, and/or resolve any issues using the DoD Database STIG.	Random sampling, 100% inspection, periodic sampling
System A&A compliance	Maintain A&A compliance IAW applicable DoD and AF policy and instruction, particularly DoD Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)* and AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*.	Random sampling, 100% inspection, periodic sampling
Common usability standards	Requirements to conform to common usability standards, i.e., IBM's CUA or Microsoft's GUI	Random sampling, 100% inspection, periodic sampling
Use Information Technology Investment Portfolio System (ITIPS) to conduct virtual evaluation of systems security and maintain program portfolio data	Used to conduct virtual evaluations of a program's Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information, input is required into ITIPS 100% of the time	Random sampling, 100% inspection, periodic sampling
Use Enterprise Mission Assurance Support Service (eMASS) to conduct virtual evaluation of systems security	Used to conduct virtual evaluations of a programs Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information, input is required into eMASS 100% of the time	Random sampling, 100% inspection, periodic sampling
Communities of Interest (COI) Compliance	Exposed data and information assets in the Metadata Environment (MDE) comply with COI ontology and requirements	Random sampling, periodic sampling
TRAINING		
Training	Specify the required training time for normal users and power users to become productive at particular operations; dependent on mission	Random sampling, 100% inspection, periodic sampling
Training materials	Timely training materials are provided on	Random sampling, 100%

	time as required by a CDRL or contract requirement	inspection, periodic sampling
Training materials	Quality training materials are provided to the customer that accurately reflect and correspond to processes and services	Random sampling, 100% inspection, periodic sampling
HELP DESK SUPPORT		
Telephone Support: Agent Not Ready Time	CONTRACTOR shall ensure the average "Not Ready" state is ≤ 22% on a daily basis.	QAE monthly review of call system metrics
Telephone Support: Agent Ring on No Answer	CONTRACTOR shall not exceed five (5) "Ring on No Answer" (RONA) calls during any shift on any day.	QAE monthly review of call system metrics
Common Access Card (CAC) Support	Support for walk-in customers requiring CAC assistance should wait no more than 3 minutes for assistance during any one visit	QAE monthly review of customer feedback
Trouble Tickets	99% of the time, a trouble ticket will be created for every phone call and 'initial' email requesting support for incidents and/or requests. Email that results in additional "follow-up" email do not require a new trouble ticket.	QAE monthly review of trouble ticket system reports
Monitor the A1 Service Desk "In" Box	95% of the time, no more than ten (10) email messages should remain unassigned/unprocessed in the A1SD inbox by 0700 each day.	QAE monthly review of Contractor metrics and customer feedback
Event Initiation	95% of the time, incidents involving critical applications shall be documented in the A1SD Dashboard according to established procedures and within 10 minutes of notification.	QAE daily review of the A1SD dashboard and customer feedback
Monitor the Maintenance Control "In" Box (PACAF/USAFE Shift specific)	The Contractor will monitor the Maintenance Control inbox during PACAF/USAFE Shifts and process email related to incidents, authorized service interruptions and scheduled/unscheduled maintenance actions from mission partners. No more than 2 email per month are identified as 'unread' by	QAE daily review of the Maintenance Control inbox

	Contractors on PACAF/USAFE shifts.	
Monitors Systems and Applications	95% of the time, no more than 1 critical alert will be left un-assigned during the PACAF/USAFE shifts each month	QAE daily review of the A1SD dashboard and customer feedback
Metrics & Reports	Non-recurring requests for data reports/metrics will be provided within 1 week of request and be 95% free of errors.	QAE random review of reports/metrics provided
Database Support	Documentation on the configuration and modification of each database will be updated as modified, and annually in December. An accuracy rate of 98% must be maintained in all databases and configuration documentation.	QAE random review of A1SD Access Databases configuration

13. LIST OF SOLICITATION APPENDICES

Appendix A: APPLICATION SERVICES STANDARDS & REFERENCES
Appendix B: AFPOA APPLICATION LIST
Appendix C: EVALUATION CRITERIA FOR AWARD
Appendix D: INSTRUCTIONS TO OFFERORS
Appendix E: PAST EXPERIENCE INFORMATION SHEET
Appendix F: PRICING SPREADSHEET

Appendix A – Application Services Standards & References

Instruction: This document serves as a one-stop-shop for easy reference of applicable certifications, specifications, standards, policies and procedures that may be placed on individual contract task orders. Tailor the list as needed when individual task orders may impose additional standards to those required at the contract level. The list is not all-inclusive and the most current version of the document at the time of task order issuance will take precedence. Web links are provided wherever possible. Include your tailored list in Section 8 of the Performance Work Statement, Applicable Standards and References.

Documentation	URL	Description
ENTERPRISE STRATEGY		
DoD CIO Net-Centric Data Strategy	http://dodcio.defense.gov/Portals/0/documents/Net-Centric-Data-Strategy-2003-05-092.pdf	This document describes the Net-Centric Data Strategy for the Department of Defense (DoD), including DoD intelligence agencies and functions. It describes a vision for a net-centric environment and the data goals for achieving that vision. It defines approaches and actions that DoD personnel will have to take as users—whether in a role as consumers and producers of data or as system and application developers.
DoD CIO Net-Centric Services Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf	The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.
DODI 8320.02, Data Sharing in a Net-Centric Department of Defense	http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf	Establishes policies and responsibilities to implement data sharing, in accordance with DoD Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002.
DoD Discovery Metadata Specification (DDMS)	http://metadata.ces.mil/dse/irs/DDMS/	Visibility, accessibility, and understandability are the high priority goals of the DoD Net-Centric Data Strategy. Of these goals, visibility and discovery are intimately linked. Visibility of a resource is, in a practical sense, useless, if the resource is not easily discoverable. With the express purpose of supporting

		the visibility goal of the DoD Net-Centric Data Strategy, the DDMS specifies a set of information fields that are to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers 11.0by laying a foundation for Discovery Services.
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf	This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain).
CJCSI 6212.01F, Interoperability and Supportability of Information Technology and National Security Systems	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf	Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs. Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs and systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment.
Netcentric Enterprise Solutions for Interoperability (NESI)	https://nesix.spawar.navy.mil/home.html	NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application.
DoDI 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS)	http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf	Establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of IT and NSS pursuant to sections 2222, 2223, and 2224 of Title 10, United States Code (Reference (c)). Establishes a capability-focused, architecture-based approach for interoperability analysis. Establishes the governing policy and responsibilities for interoperability requirements development, test, certification and prerequisite for connection of IT, including NSS (referred to in this instruction as “IT”). Defines a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) approach to enhance life-cycle interoperability of IT. Establishes the requirement for enterprise services to be certified for interoperability. Incorporates and cancels DoDD 4630.05, DoDI 4630.8, and DoD Chief Information Officer (CIO) memorandum (References (d), (e), and (f)).
Joint Vision 2020	http://www.fraw.org.uk/files/peace/us_dod_2000.pdf	Strategic Guidance: Joint Vision 2020 builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing transformation of America’s

		Armed Forces.
ENTERPRISE ARCHITECTURE		
DoD Global Information Grid Architectural Vision	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&Location=U2&doc=GetTRDoc	The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information – the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.
DOD Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework.aspx	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.
AFPD 17-1, Information Dominance Governance and Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd17-1/afpd_17-1.pdf	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.

AFI 17-140_AFGM2017-01, *Air Force Architecting*	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance and Cyberspace Governance and Management*. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.
GiG Technical Guidance Federation GIG-F	https://gtg.csd.disa.mil/uam/registration/register	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.
SYSTEMS ENGINEERING		
Business and Enterprise Systems (BES) Process Directory	https://acc.dau.mil/bes	The BES Process Directory (BPD) is a life cycle management and systems engineering process based on the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System; as tailored for Information Technology (IT) systems via the Defense Acquisition Process Model for Incrementally Fielded Software Intensive Programs
AFI 10-601, Capabilities-Based Requirements Development	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.
AFI 63-101, Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi6	The purpose of this instruction is to implement direction from the Secretary of the Air Force as outlined in Air Force Policy

	3-101_20-101/afi63-101_20-101.pdf	Directive (AFPD) 63-1/20-1, Acquisition and Sustainment Life Cycle Management. The primary mission of the Integrated Life Cycle Management (ILCM) Enterprise is to provide seamless governance, transparency and integration of all aspects of weapons systems acquisition and sustainment management.
AFI 99-103, Capabilities-Based Test and Evaluation	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature sys-tem designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.
DoD Open Technology Development Guidebook		This roadmap outlines a plan to implement Open Technology Development practices, policies and procedures within the DoD.
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	http://www.sei.cmu.edu/library/assets/soabest.pdf	This document was developed under the Net-Centric Operations Industry Forum charter to provide industry advisory services to the Department of Defense (DoD), Chief Information Officer (CIO). It presents a list of industry best practices in achieving Service Oriented Architecture (SOA).
INFORMATION ASSURANCE		
ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.dni.gov/files/documents/ICD/ICD_503.pdf	This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.
DoDI 8500.01 Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) Cybersecurity through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
DoDD 8140.01, *Cyberspace Workforce Management*	http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf	Establishes policy and assigns responsibilities for Department of Defense (DoD) Cyberspace workforce management.

DoD 8570.01-M, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf	Provides guidance for the identification and categorization of positions and certification of personnel conducting Cybersecurity functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.01. The DoD Cybersecurity Workforce includes, but is not limited to, all individuals performing any of the Cybersecurity functions described in this Manual. Additional chapters focusing on personnel performing specialized Cybersecurity functions including A&A and vulnerability assessment will be published as changes to this Manual.
DoDI 8510.01,Risk Management Framework (RMF) for DoD Information Technology (IT)	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf	Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).
AFI 33-200, *Air Force Cybersecurity Program Management*	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-130/afi33-200.pdf	This AFI provides general direction for implementation of Cybersecurity and management of Cybersecurity programs according to AFPD 17-1. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process.
AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf	This AFI implements RMF for authorizing the operation of Air Force ISs consistent with federal, DoD, and Air Force policies. It is used to ensure Cybersecurity and Continuous Monitoring for all Air Force procured Information Systems, and Guest systems operating on or accessed from the AF-GIG.
Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.
Air Force Guidance Memorandum (AFGM), End-of-Support Software Risk Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2015-33-01/afgm2015-33-01.pdf	This Guidance Memorandum supersedes AFGM 2014-33-03, Microsoft Windows XP End-of-Life, and highlights current policies and SAF/CIO A6 authorities to mitigate cybersecurity vulnerabilities introduced by unsupported software. Compliance with this Memorandum is mandatory.
AFMAN 17-1301, COMPUTER SECURITY (COMPUSEC)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1301/afman17-1301.pdf	This AFMAN implements Computer Security in support of AFPD 17-1, *Information Dominance and Governance Management* and AFI 33-200, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 33-200.

AFMAN17-1303_AFGM2016-01, Air Force Guidance Memorandum to AFMAN33-285 Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1303/afman17-1303.pdff	This rewrite identifies cybersecurity baseline certification requirements for the AF cybersecurity workforce; stipulates minimum certification requirements for various cyber roles and risk management positions; sets qualifications criteria; clarifies the cybersecurity-coding position process; and codifies the waiver policy for baseline certification requirements.
DoDI 8540.01, Cross Domain (CD) Policy	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf	Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) in accordance with the authority in DoD Directive (DoDD) 5144.02
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.
INFORMATION TECHNOLOGY STANDARDS		
Federal Information Processing Standards (FIPS)	http://www.nist.gov/itl/fipscurrent.cfm	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
IEEE/EIA 12207.0, "Standard for Information Technology	http://www.ieee.org/	IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes", is a standard that establishes a common framework for software life cycle process. This standard officially replaced MIL-STD-498 for the development of DoD software systems in May 1998.[1] Other NATO nations may have adopted the standard informally or in parallel with MIL-STD-498.This standard defines a comprehensive set of processes that cover the entire life-cycle of a software system—from the time a concept is made to the retirement of the software. The standard defines a set of processes, which are in turn defined in terms of activities. The activities are broken down into a set of tasks. The processes are defined in three

		broad categories: Primary Life Cycle Processes, Supporting Life Cycle Processes, and Organizational Life Cycle Processes.
DoDD 8000.01 Management of the Department of Defense Information Enterprise	http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf	Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense
AFI 10-208 Air Force Continuity of Operations (COOP) Program	http://www.fas.org/irp/doddir/usaf/afi10-208.pdf	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs); and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).
US Government Configuration Baseline (USGCB)	http://usgcb.nist.gov/	The United States Government Configuration Baseline (USGCB) is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. USGCB continues to be one of the most successful government IT programs aimed at helping to increase security, reduce costs, and accelerate the adoption of new government technologies, while creating a more managed desktop environment.
DoD Mobile Application Strategy	http://www.defense.gov/news/dodmobilitystrategy.pdf	It is intended to align the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from such activities and aligns with efforts composing the Joint Information Environment.
ISO/IEC 20000	http://www.iso.org/iso/home.html	ISO/IEC 20000 is an international standard for IT Service Management (ITSM). It allows IT organizations to ensure the alignment between ITSM processes and their overall organization strategy. It requires the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system (SMS). ISO/IEC 20000 consist of 5 separate documents, ISO/IEC 20000-1 through 20000-5
QUALITY ASSURANCE		
AFMAN 33-363_AFGM 2017, Management of Records	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf	This manual implements DoDD 5015.2, *DoD Records Management Program*, and Air Force Policy Directive (AFPD) 33-3, *Information Management*. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records

		(regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.
DoD Instruction 5015.02, DoD Records Management Program	http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic
AFI 33-364, Records Disposition – Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management*, by listing program objectives and responsibilities, guiding personnel in disposing of special types of records, retiring or transferring records using staging areas, and retrieving information from inactive records.
DoDI 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoDD_523024.pdf	This Directive updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
AFI 61-204, Disseminating Scientific and Technical Information	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-204/afi61-204.pdf	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.
AFMAN 33-152 Communications and Information	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-152/afman33-152.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*, AFPD 33-2, *Information Assurance (IA) Program*, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities.
AFMAN 33-402 - Service Development and Delivery Process (SDDP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-402/afman33-402.pdf	This Air Force Manual (AFMAN) provides guidance for the definition, design, acquisition, implementation and delivery of Business Mission Area (BMA) capabilities using the Service Development and Delivery Process (SDDP). The SDDP is end user-centric to better align the assistance required by an end user to address a process-based problem across a holistic set of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P)

		solutions. The SDDP details the processes and procedures by which Information Technology (IT) capabilities supporting Air Force (AF) processes are identified, defined, developed and delivered in a way that ensures IT capabilities are necessary, and maximize the potential for successful implementation of IT investments. The SDDP is applicable to large and small scale problems and can be used to implement IT capabilities of all sizes and types.
AFMAN 33-153 Information Technology (IT) Asset Management (ITAM)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-153/afman33-153.pdf	This is a total revision to replace and incorporate Air Force Instruction (AFI) 33-112, Information Technology Hardware Asset Management, and AFI 33-114, Software Management, into a single IT asset management manual. This revision incorporates the PWCS asset management portions of AFI 33-106, Managing High Frequency Radios, Personal Wireless Communications Systems, and the Military Affiliate Radio System, to remove that guidance; and identifies Tiered waiver authorities for unit level compliance items.
DoDD 5205.02E, Operations Security (OPSEC) Program	http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf	Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations.
AFI 10-701, Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf	This publication provides guidance for all Air Force personnel (military and civilian) and supporting Contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.
DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).
DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf	This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their Contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access

		Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
Section 508 of the Rehabilitation Act of 1973	http://www.opm.gov/html/508-textOfLaw.asp	On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.
DoDI 1100.22 Policy and Procedures For Determining Workforce Mix	http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf	In accordance with the authority in DoD Directive 5124.02, this Instruction establishes policy, assigns responsibilities, and prescribes procedures for determining the appropriate mix of manpower and private sector support. It implements policy established in DoDD 1100.4 and incorporates and cancels DoDI 3020.37. This Instruction provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently governmental (IG); commercial (exempt from private sector performance); and commercial (subject to private sector performance). It reconciles and consolidates the definitions and examples of IG from section 306 of title 5, U.S.C.; sections 501 (note), 1115, and 1116 of title 31, U.S.C., Attachment A of OMB Circular A-76; and Subparts 2 and 7.503(c) of the FAR into a set of criteria for Defense-wide use. This Instruction also implements aspects of sections 113, 188(b), 129a, and 2463 of title 10, U.S.C., and reissues and cancels DoDI 1100.22.
DoDD 8320.1 Data Administration	https://acc.dau.mil/adl/en-US/33650/file/6823/DoDD83201%20Data%20Admin.pdf	This Instruction applies to the administration and standardization of DoD standard data elements generated within the functional areas of audit and criminal investigations for DoD. It also applies to the administration of DoD standard and non-standard data elements generated, stored, or used by the DoD. Data elements will be administered in ways that provide accurate, reliable, and easily accessible data throughout the DoD, while minimizing cost and redundancy. Data elements will be standardized to meet the requirements for data sharing and interoperability throughout the DoD. Data administration will be encouraged and promoted within the DoD.

AFI 33-332, Air Force Privacy and Civil Liberties Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf	Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
AFI 31-501, Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi31-501/afi31-501.pdf	Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5 to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013.
AFI 16-1404, Air Force Information Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf	This publication implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance; Department of Defense (DoD) Directive 5210.50, Management of Serious Security Incidents Involving Classfied Information, DoD Instruction (DoDI) 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual (DoDM) 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDm 5200.45, Instructions for Developing Security Classification Guides.
FISMA 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	FISMA was enacted as part of the E-Government Act of 2002 to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets," and also to "provide for development and maintenance of minimum controls required to protect Federal information and information systems." FISMA requires Federal agencies to: •designate a Chief Information Officer (CIO), •delegate to the CIO authority to ensure compliance with the requirements imposed by FISMA, •implement an information security program, •report on the adequacy and effectiveness of its information security policies, procedures, and practices, •participate in annual independent evaluations of the information security program and practices, and •develop and maintain an inventory of the agency's major information systems. FISMA requires the Director of the Office of Management and Budget (OMB) to ensure the operation of a central Federal information security incident center. FISMA makes the National Institute of Standards and Technology (NIST) responsible for "developing standards, guidelines, and associated methods and techniques" for information systems

		used or operated by an agency or Contractor, excluding national security systems.
ISO/IEC 19770-2, Software Tagging	http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670	ISO/IEC 19770-2:2009 establishes specifications for tagging software to optimize its identification and management. (http://en.wikipedia.org/wiki/ISO/IEC_19770)
FAR CLAUSES		
DFARS 252.227-7015 Technical Data Commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1079_80393	Provides the Government specific license rights in technical data pertaining to commercial items or processes. DoD may use, modify, reproduce, release, perform, display, or disclose data only within the Government. The data may not be used to manufacture additional quantities of the commercial items and, except for emergency repair or overhaul and for covered Government support Contractors, may not be released or disclosed to, or used by, third parties without the Contractor's written permission.
DFARS 252.227-7014 Rights in Noncommercial Computer Software	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P683_47378	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.
DFARS 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1182_92447	Provides requirements for the identification and assertion of technical data.
DFARS 252.227-7013 Rights in Technical Data---Non-commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P295_15657	Provides guidelines for rights in technical data on non-commercial items

Appendix B - AFPOA Application List

Applications Supported by the A1 Service Desk. The tasks and responsibilities for the applications listed below in Table 1, involve two main areas of support: (1) Technical Support includes, but is not limited to, incident and request management for user accounts and Tier I troubleshooting for incidents. If tickets aren't resolved at the Tier I level, the ticket is escalated to Tier II for advanced technical support. (2) "Information Only" includes customer questions or concerns regarding services and applications not hosted or supported by AFPOA, but customers are provided alternate phone numbers and/or guidance on how to address their issues with the office that provides resolution.

TABLE 1 AFPOA Application List

ACRONYM	APPLICATION	SUPPORT
User Account Management	Multiple Applications	Technical Support
ADP	Airmen Development Plan	Technical Support
AEF (NIPR/SIPR)	Air and Space Expeditionary Forces	Technical Support
AF Reconanalysis		Technical Support
AFCAPS	AF Classification & Assignment Preference System	Technical Support
AFFMS II	AF Fitness Management System	Technical Support
AFPC Secure		Technical Support
AFPROMS	AF Promotions	Technical Support
AMS	Assignment Management System	Technical Support
API	Airmen Powered by Innovation	Technical Support
ARMS	Automated Records Management System	Technical Support
ARP	Aviator Retention Pay	Technical Support
ASINet	Authorized Service Interruption.Net	Technical Support
B&E Forms	Benefits and Entitlements	Technical Support
BaseMDB		Technical Support

BLSDM	Base Level Service Delivery Model	Technical Support
BO	Business Objects	Technical Support
Burdensome		Technical Support
CAC Reset	Common Access Card PIN reset	Technical Support
CAFM	Computer Aided Facilities Management	Technical Support
CallRex	Phone Recording used by TFSC	Technical Support
CCB	Civilian Career Brief	Technical Support
CCTK (NIPR)	Commanders Tool Kit	Technical Support
Civilian Printview	DCPDS Print Documents	Technical Support
ACRONYM	**APPLICATION**	**SUPPORT**
CLRP	College Loan Repayment Program	Technical Support
CMS	Case Management System	Technical Support
DCIPS mil	Defense Casualty Info Processing System (Military)	Technical Support
DCIPS PAA	Defense Casualty Info Processing System (PAA)	Technical Support
DCPDS	Defense Civilian Personnel Data System (MyBiz+)	Technical Support
DEPCON EOM	Enterprise Output Manager (MilPDS)	Technical Support
Discoverer		Technical Support
DMZ Web Applications		Technical Support
EARL	Electronic Automated Records Libraries (formerly DM5)	Technical Support
EBIS	Employee Benefits & Entitlements System	Technical Support
eBOSS	Electronic Board Operations Support System	Technical Support
EOM	Enterprise Output Manager (MilPDS)	Technical Support

EPROM	Enlisted promotions	Technical Support
Genesys		Technical Support
GRB Platform	Government Retirement Benefits	Technical Support
HP OM	Hewlett-Packard Output Manager	Technical Support
HPERB	Heath Professions Education Requirements Board	Technical Support
IDE/SDE	Intermediate/Senior Developmental Education	Technical Support
Mil-Interfaces		Technical Support
Millenium		Technical Support
MilPDS	Military Personnel Data System	Technical Support
Mil-PrintView		Technical Support
MilSH	Military School House - Keesler	Technical Support
ACRONYM	**APPLICATION**	**SUPPORT**
MilXTRAC	Military Personnel Data System Extract	Technical Support
MS Office Suite	Microsoft Office Suite Software	Technical Support
myBIZ	My Business	Technical Support
myPers	My Personnel Services	Technical Support
myPers Admin Console	My Personnel Services	Technical Support
OATS	Officer Accession Tracking System	Technical Support
OPUS	Document Management System	Technical Support
PARIS	Personnel Automated Records Information System	Technical Support
PASCODE	Personnel Accounting System Code Lookup	Technical Support
PCSM	Pilot Candidate Selection Method	Technical Support

PD Access for RPA Generators		Technical Support
PRDA	Personnel Records Display Application	Technical Support
PRISM	AFPROMS-Program Resources Integrated Solution Management	Technical Support
RAW	Retrieval Applications Website	Technical Support
Reconalysis (Payroll Recon)		Technical Support
RetSepCalcNet	Retirement Separation Calculator	Technical Support
RIPROD	Reporting Instance on Production	Technical Support
RMVS	Reserve Management Vacancy System	Technical Support
RPA Tracker		Technical Support
SAS Data Management		Technical Support
SNCOAS	Senior NCO Academy Allocation System	Technical Support
SOA	Service Oriented Architecture	Technical Support
STARS	Statistical &Analysis Reporting System	Technical Support
System Architect		Technical Support
ACRONYM	**APPLICATION**	**SUPPORT**
vMPF	Virtual Military Personnel Flight	Technical Support
vPSC RBA	Role Based Application	Technical Support
WAPS	Weighted Airmen Promotion System	Technical Support

TABLE 2- AFPOA Application List related to the A&A task 3.5

SYSTEM	RESPONSIBILITY
CRSC	AFPOA Systems Primary Responsibility

SLCMS	AFPOA Systems Primary Responsibility
CRM SaaS-MyPers	AFPOA Systems Primary Responsibility
BO	AFPOA Systems Primary Responsibility
PARIS	AFPOA Systems Primary Responsibility
PCSM	AFPOA Systems Primary Responsibility
TDE	AFPOA Systems Primary Responsibility
VTL	AFPOA Systems Primary Responsibility
AFPC PUBLIC WEB APPS	AFPOA Systems Primary Responsibility
AEF ONLINE (U)	AFPOA Systems Primary Responsibility
CAFM	AFPOA Systems Primary Responsibility
AEF ONLINE(S)	AFPOA Systems Primary Responsibility
SYSTEM	**RESPONSIBILITY**
AFPOA NETWORK	AFPOA Systems Primary Responsibility
AFPC-ICMS	AFPOA Systems Primary Responsibility
EBIS v1.0	AFPOA Systems Primary Responsibility
STARS	A1 Systems Review and Consult

CIV PRINTVIEW	AFPOA Systems Primary Responsibility
AFFIRST	A1 Systems Review and Consult
AFPAAS	AFPOA Systems Primary Responsibility
M4S	A1 Systems Review and Consult
MOMS	A1 Systems Review and Consult
MyVector	A1 Systems Review and Consult
MPES-U	A1 Systems Review and Consult
AFAEMS	A1 Systems Review and Consult
MPES-S	A1 Systems Review and Consult

APPENDIX C
Evaluation Criteria

52.212-2 Evaluation - Commercial Items (October 2014)

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

Technical /Management approach (TMA) and past experience (PE) are greater than price. TA is more important than PE.

Non-price factors, when combined, are more important than Price. As the difference in non-price factors becomes closer, Price may become more important. Non-price factors will be evaluated first, then price.

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award. (End of Provision)

C1.0 Evaluation Information

Failure to comply with any of the requirements identified in the PWS may render the contractor's quote unacceptable.

GSA will evaluate all quotes to determine the best value to the government. GSA will make that determination based on each vendor's quote using the following evaluation criteria, listed in their order of importance:

- **Technical/Management Approach (TMA)** and its feasibility, practicability and appropriateness in accomplishing PWS requirements. The technical/management approach shall include the Staffing Plan, Key Personnel Resumes', Schedule, Program Management Plan and Transition Plan.

- **Past Experience (PE)** is *what specific work was performed* and its relevancy to the scope, size, and duration of requirements identified in the PWS within the last 3 years.

- **Price:** Evaluated to determine that the price is fair and reasonable. The Government reserves the right to conduct a price realism analysis to see if the vendor's prices are

unrealistically low, compared to the other price offerings received in response to this solicitation and overall fair and reasonable market pricing (based on independent Government market research). Unrealistically low pricing represent a performance risk, and an offer may be determined in eligible for award if the pricing offered is unrealistically low.

A debriefing may be requested by the vendor, and shall be conducted by GSA in accordance with the requirements of 52.212-1(l).

If any of the evaluation factors (TMA/PE) receives a rating of less than acceptable, the response package may not be reviewed any further and therefore may not be considered for award.

C1.1 Technical and Management Approach (TMA)

This factor considers the extent which the offeror understands the specific requirements of the PWS, and the offeror's technical approach to meeting those requirements.

Each offeror will be evaluated on their demonstrated understanding of the task order requirements, the adequacy of the proposed solution/approach, the quality and completeness of their technical solutions to these objectives, and the overall qualifications and skill mix of the contractor workforce proposed to address these task order objectives.

The following PWS sections and their subsections shall be stated and clearly addressed in the Technical/Management Approach response:

- 3.1 Task 1: Program Management
- 3.2 Task 2: Requirements Support
- 3.3 Task 3: Field Support
- 3.4 Task 4: Operations & Data Center Support
- 3.5 Task 5: Cybersecurity and Software Management Support
- 3.6 Task 6: Lifecycle Management Support

NOTE: An offeror must not simply state that it is willing to perform the solicitation requirements. Vendors must show they are capable of performing the work described in the solicitation. Simply stating they are willing to perform the work without demonstrating their approach may result in a rating of "unacceptable."

C1.2 Past Experience (PE)

This factor considers the extent of the offeror's past experience in carrying out similar work. The government must have confidence in the offeror's ability to complete a project with similar scope, size, and duration with minimal risk.

- Similar in Scope is defined as a measurable range of operations such as the major requirement areas as detailed in Section 3.0 of the PWS.

- The contractor shall demonstrate the ability to meet requirements as detailed in Section 3.0 of the PWS.
- Similar in Size is defined as dollar value, number of personnel in similar skill sets, and/or number of users/hardware supported.
- Similar in Duration is identified the length of time required to show the vendor can support a requirement of similar length. The POP for this requirement is the one base year and four (4) option periods. Thus, vendors should provide PE similar to this POP.

C1.3 Past Performance (PP)

While past performance is not a formal evaluation factor for this procurement, the GSA CO will review the Federal Awardee Performance and Integrity Information System (FAPIIS) and the Excluded Parties Lists System (EPLS) (within System for Award Management (SAM)) information on the awardee in order to make a past performance responsibility determination in accordance with FAR 9.104-6 FAPIIS and FAR 9.105-1, "Obtaining Information."

The Government reserves the right to review information contained in the Past Performance Information Retrieval System (PPIRS) (http://www.ppirs.gov/), and other applicable Government systems and sources in an effort to make an informed responsibility determination prior to award.

C1.4 Price

Price will be evaluated to determine the fairness and reasonableness of proposed pricing. Price will be evaluated separate from the technical elements of the quote. A rating will not be assigned to the evaluation of price.

In the pricing section of your response to this PWS, contractor shall include specific skill category(s) with labor rates the contractor expect to invoice and the number of positions with estimated total hours for each position. The contractor will provide fully burdened labor costs for each proposed skill proposed. The pricing information shall be in a spreadsheet format and it must include a total price for the base and option periods in addition to overall price (inclusive of base period and options). (See Appendix F, Pricing Worksheet).

In an effort to receive the highest quality solution at the lowest possible price the government requests all available discounts on all services offered by the contractor for this requirement. The offeror is encouraged to offer discounts below contract rates. When offering discounts, the quote must clearly identify both the contract and the discount price for each discounted labor rate.

The vendor will provide prompt payment terms in their quote.

C1.5 Organizational Conflict of Interest Plan: The offeror's Organizational Conflict of Interest Plan will be evaluated as acceptable or unacceptable based on meeting the requirements identified in this PWS. An offeror with an unacceptable Organizational Conflict of Interest Plan will have until time of award to submit an acceptable plan or that offeror will be removed from consideration.

The plan should consist of the following sections:

- A Table of Contents
- Part 1 – Disclosure of existing or potential OCI's
- Part 2 – Detailed descriptions of the specific measures that are proposed to avoid, mitigate, or neutralize each one of the OCI's described in Part 1 of the plan.

[END]

APPENDIX D

Instructions to Offerors

D1.0 Response Package Instructions

The contractor's response package must include the following information and must not exceed the following page limitations:

Title	Includes	Format	Page Limit
Contract Documentation			
Cover Letter/Executive Summary	Including contractor's DUNS, Tax ID, and Prompt Payment Discount	Microsoft Word**	Max 3 pages
Technical Portion			
Technical Management Approach	Covers all requirements defined in Appendix C1.1 and shall include the Staffing Plan, Schedule (Reference PWS Section 3.1.4), and Transition Plan (Reference PWS Section 5.4) (This section does not include the page count for Key Personnel Resumes')	Microsoft Word**	Max 40 pages
Key Personnel	Key Personnel Resumes'	Microsoft Word**	Max 3 pages per person
Program Management Plan	Includes overall methods used to meet the PWS requirements as described in PWS section 3.1.3.	Microsoft Word **	Max 5 pages
Past Experience			
Past Experience Information	Reference Appendix E, Past Experience Information Sheet	Microsoft Word **	Max 6 pages
Pricing			
Pricing Appendix F	Pricing shall be submitted as a Microsoft Excel document separate from the Technical Portion and shall contain Labor Categories and Rates with Discounts for the entire period of performance (See attached Appendix F, Pricing Worksheet)	Microsoft Excel (Do not PDF this document)	No page limit
Additional Required Information			
Tax Liability Letter	FAR 52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016) Submitted on company letterhead	PDF Format**	Max 2 pages
Organizational Conflict of Interest Certification and OCI Mitigation Plan	The OCI Mandatory Certification is found in Section 9.6. The OCI Mitigation Plan shall be submitted in the response package, if an OCI has been identified and requires mitigation.	PDF Format**	No page limit

**Quote shall be 8.5" x 11" page size in Times New Roman font with minimum of 10-point font (8-point font in tables) with the exception of the Excel pricing spreadsheet which must be legible.

D1.1 Required TMA Information

In support of the evaluation of the TMA each offeror must submit the following:

- Description/narrative of the vendor's knowledge and understanding of the requirements

as outlined in the PWS. The following PWS sections and their subsections shall be stated and clearly addressed in the Technical Approach:

- 3.1 Task 1: Program Management
- 3.2 Task 2: Requirements Support
- 3.3 Task 3: Field Support
- 3.4 Task 4: Operations & Data Center Support
- 3.5 Task 5: Cybersecurity and Software Management Support
- 3.6 Task 6: Lifecycle Management Support

- The methodologies and techniques proposed to be used to fulfill the PWS requirements including the management of the task.
- In support of the Technical/Management Approach, the vendor shall provide a matrix for the staffing plan that identifies the labor category, PWS sections and labor hour ceiling (Reference Section 8.2 of the PWS). See staffing plan matrix template for T&M & FFP Labor below. The staffing plan shall address how the team will be structured for this task order. Failure to provide a staffing plan that supports your technical/management approach to the requirements in the PWS may render the contractor's quote as unacceptable.

  Staffing Plan matrix template for T&M:

Proposed Labor Category	Prime or Subcontractor	Section of PWS	Labor Hour Ceiling

  Staffing Plan matrix template for FFP:

Proposed Labor Category	Prime or Subcontractor	Section of PWS	Labor Hour Ceiling

NOTE: ***An offeror must not simply state that it is willing to perform the PWS requirements. Vendors must show they are capable of performing the work described in the PWS.***

D1.2 Required Past Experience (PE) Information

Using the Past Experience Information Sheet (*PWS/Appendix E*) provide the recent and relevant PE information for three (3) past or current contracts/task orders executed **and/or completed** within the past 3 years with comparable (same or similar scope, size, duration) requirements to the solicited task.

The offeror may use subcontractor experience as well as prime contractor past experience, as long as it is recent and relevant and of similar size and scope to the work described in the PWS.

Prime level experience may be given greater consideration than subcontract level experience, depending on the project scope (value, Period of Performance, and type of work performed and its applicability to the current requirement). The offeror must identify whether it was the prime or a subcontractor for each project.

Note: In rating this factor, the Government will evaluate the firm's similar experience. The government's consideration of experience will include the offeror's organizational experience but will not include specific consideration of the offeror's proposed, current, or former contractor personnel experience as part of the offeror's organizational experience.

Relevancy is defined as work that has been/is being performed for prior or current customer contracts/task orders/projects that are of comparable scope, size, and duration which is similar to the requirement described herein.

Recency is defined as current/former task orders/contracts/projects executed within the past three (3) from the closing date of the solicitation. The work can be in progress at the time of solicitation submission; however, the project must be far enough along to have a documented record of successful experience.

D1.3 Required Pricing Information

This requirement is a hybrid T&M and FFP task order with pricing based on the NETCENTS II contract. In the pricing section of the response to this PWS, offerors shall include specific skill category(s) with rates the contractor expects to invoice and the number of positions with estimated total hours for each position. These rates shall be fully burdened, and not subject to DCAA or other finalized audited rates. After award, this order shall not be considered a Forward Pricing Rate Agreement (FPRA).

In an effort to receive the highest quality solution at the lowest possible price the government requests all available discounts on all services offered by the contractor for this requirement. The offeror is encouraged to offer discounts below contract rates. When offering discounts, quotes must clearly identify both the contract and the discount price for each discounted labor rate.

The vendor will provide/offer prompt payment terms in their quote, ensuring that any prompt payment terms included in the basic contract.

D1.4 Required PP Information

Although Past Performance (PP) is not a formal evaluation factor for ward, the GSA CO will review the Federal Awardee Performance and Integrity Information System (FAPIIS) and the Excluded Parties Lists System (EPLS) (within System for Award Management (SAM)) information on the awardee in order to make a past performance **responsibility determination** in accordance with FAR 9.104-6 FAPIIS and FAR 9.105-1, "Obtaining Information."

There is no additional information required for submittal by the contractor with their offer.

D1.5 Travel

Travel is anticipated for this task. The vendor shall include travel costs in accordance with the terms identified in the PWS.

The travel ceiling that is provided is estimation for evaluation purposes only. No G&A, OH or other indirect costs shall be allowable under the terms of the solicitation or resultant awarded order.

D1.6 Organizational Conflict of Interest

In response to this solicitation the vendor shall identify any potential conflicts of interest associated with the requirements of this procurement, per FAR 9.5. This disclosure shall be submitted on a separate signed letter on company letterhead. If no OCI exists, the letter shall state that fact, and shall be signed by an authorized signatory of the company, and submitted in the quotation package.

D1.7 Required Tax Certification Letter

Please submit the following in accordance with the Department of Justice's policy certifying that your company does not have any unpaid federal tax delinquencies or, within the preceding 24 months, has a felony criminal conviction under any federal law or state law.

Response is required on your company letterhead identifying the project title, and ID07180006. Date the document, and ensure the document is signed by an official of the company who is authorized to represent the company on this topic.

FAR 52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that--

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that--

(1) It is [ ] is not [ ] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and (2) It is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

D 4.0 FAR 52.209-12 Certification Regarding Tax Matters - Certification Regarding Tax Matters (Feb 2016)

(a) This provision implements section 523 of Division B of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts

(b) If the Offeror is proposing a total contract price that will exceed $5,000,000 (including options), the Offeror shall certify that, to the best of its knowledge and belief, it--

(1) Has [ ] filed all Federal tax returns required during the three years preceding the certification;

(2) Has not [ ] been convicted of a criminal offense under the Internal Revenue Code of 1986; and

(3) Has not [ ], more than 90 days prior to certification, been notified of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a non-frivolous administrative or judicial proceeding.

(End of provision)

D 5.0 52.227-15 Representation of Limited Rights Data and Restricted Computer Software. (DEC 2007)

As prescribed in 27.409(c), insert the following provision:

(a) This solicitation sets forth the Government's known delivery requirements for data (as defined in the clause at 52.227-14, Rights in Data—General). Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at 52.227-16, if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data—General clause at 52.227-14 included in

this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.
(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and **s**tates **[*offeror check appropriate block*]—**

[ ] (1) None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or
[ ] (2) Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows:
(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror.

D1.8 Response package Development Instructions

The contractor must submit the response by the date and time established in the notice provided via email to latasha.goines@gsa.gov .

If a contractor decides to submit a "No Bid" in response to the solicitation, GSA requests a reason be provided.

All questions concerning this solicitation package will be submitted to the GSA CO via email to latasha.goines@gsa.gov by 10 April 2018 at 2:00 p.m. CST. The GSA CO will compile all questions and responses and issue all questions and answer received to all solicited vendors via email.

The only method by which any terms of this solicitation (to include the PWS) may be changed is by a formal amendment to the solicitation generated by the issuing office. No other communication made whether oral or in writing (e.g., at any Pre-offer submittal conference, Industry Questions & Answers prior to response closing date and time, clarifications, etc.), will modify or supersede the terms of the PWS. No contact with anyone other than the responsible CO is allowable after the release of the solicitation.

The Government reserves the right to make a selection based upon initial submittal packages; therefore the offeror should submit its best terms in its initial submission. The Government also reserves the discretion to confer with offerors/interested parties and request revised submittal packages if needed. The Government reserves the right to make no award.

Offeror's shall thoroughly examine all solicitation documents and instructions. Failure to do so will be at the Offeror's own risk. Failure to comply with all of the terms and conditions of the solicitation, to include the PWS, may result in the Government's elimination of the submittal package received in response to the solicitation, from further consideration for award.

[END]

APPENDIX E

PAST EXPERIENCE INFORMATION SHEET

Provide the information requested in this form for each contract/program being described. Provide concise comments regarding your performance on the contracts you identify. Provide a separate completed form for each contract/program submitted. Limit the number of past efforts submitted and the length of each submission to the limitations set forth in the task order, *Section* B1.1.3, *Past Experience*, of this solicitation.

A. Offeror Name (Company/Division): _____
CAGE Code: _____
DUNS Number: _____
(NOTE: If the company or division performing this effort is different than the offeror or the relevance of this effort to the instant acquisition is impacted by any company/corporate organizational change, note those changes.)

B. Program Title: _____

C. Contract Specifics:
1. Contracting Agency or Customer:_____
2. Contract Number:_____
3. Contract Type:_____
4. Period of Performance: _____
5. Total Contract $ Value: _____(Total cost to inlcude all options)
6. Current Contract $ Value: _____(Do not include unexercised options)

D. Brief Description of Effort as Prime or Subcontractor
(Please indicate whether it was development and/or production, or other acquisition phase and highlight portions considered most relevant to current acquisition):_____

E. Milestones:
1. Start Date: _____
2. Completion Date: _____

F. Primary Customer Points of Contact: (For Government contracts provide current information on both individuals. For commercial contracts, provide points of contact fulfilling these same roles.)

Client Program Manager and/or Site Manager Information	Name	
	Office	
	Telephone	
	E-Mail	
Contracting Officer Information	Name	
	Office	

	Telephone	
	E-Mail	

G. Describe **<u>in as much detail as possible</u>** why this experience is relevant with respect to the scope of the overall task and to the requirements as described in Sections 3of this SOW/PWS. Scope is defined as the range of work/skills being referenced is similar in nature to the requirements identified in the SOW/PWS. Please reference back to Appendix C, Section C1.2 Past Experience (PE) "similar" language.

H. Describe **<u>in as much detail as possible</u>** why this experience is relevant with respect to the size of the overall task and to the requirements as described in Sections 3 of this PWS. **Size is defined as dollar value, number of personnel in similar skill sets, and/or number of users/hardware supported** is similar in nature to the requirements identified in the PWS. Please reference back to Appendix C, Section C1.2 Past Experience (PE) "similar" language.

APPENDIX F

Separate Excel Pricing Worksheet