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

NexGenIT ICS Support Contract

Task Order Performance Work Statement

Name:	
Organization:	
Address:	

Executive Summary

Provide service, troubleshooting, documentation and operation of information technology systems for the 330-personnel in the Civil Engineer Squadron tasked with supporting Global Hawk, Predator, and transient aircraft in an extreme climate; sustaining and repairing a $1.6B physical plant comprised of 1,600 base personnel, 547 housing units, 220 building and 344 dorm rooms; executing a $1.5M operating budget and $30M construction program. Oversees mission readiness/resources for environmental compliance, crash/fire/rescue, WMD, and disaster response and recovery forces.

NETCENTS-2 NetOps and Infrastructure F&O
TO PWS
NexGenIT ICS Tech Support

1. Purpose

The objective of this task order is to obtain contractor technical support and enable the 319 Civil Engineer Squadron to perform their mission.

2. Scope

The scope of this Performance Work Statement (PWS) is to provide the requirements for contractor sustainment support for the technical systems in 319 Civil Engineer Squadron (CES) (300+ users). The contractor shall provide Help Desk support for users, maintaining access and functionality of various software/hardware required in the performance of their duties. The contractor shall provide server administration support for CES specific applications.

The contractor shall provide all necessary managerial, personnel, expertise, and non-personal services necessary to perform enterprise-wide IT support as defined in this PWS and in accordance with (IAW) applicable 319 CES, Air Force (AF), Department of Defense (DoD) policies, processes and regulations. This support encompasses all technical services required to support the following enclaves: Non-secure Internet Protocol Router Network (NIPRNet), the Industrial Control Systems (ICS), NexGen IT, Automated Civil Engineer System (ACES) Automated Readiness Information System (ARIS), and Fire Department (FD).

3. Requirement/Description of Services

The contractor shall provide operational support services including, but not limited to, systems administration, customer training, and help desk support of both legacy and new applications and systems in accordance with AFI 33-115 Air Force Information Technology (IT) Service and supporting Methods and Procedures Technical Orders (e.g., Vulnerability Management MPTO, etc.), and DoD 8570.01M Information Assurance Workforce Improvement Program.

This is a non-personnel services contract to provide Information Technology (IT) Support Service to the 319th Civil Engineering Squadron (319 CES). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

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

Not Applicable

3.1.2 Enterprise Level Security (ELS)

3.1.2.1 Cyber Security Services

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

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

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

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

3.1.2.2 Information Assurance

Personnel performing Information Assurance (IA) activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with DoD 8570.01-M, *Information Assurance Workforce Improvement Program* (reference Tables C4.T1. IAM Workforce Requirements and Table C4.T2. IAM Level I Position Requirements), 19 December 2005 (with all current changes), and as stipulated in Section H, Clause H101 of the overarching Application Services RFP.

- Develop, implement, oversee, and maintain an organization cybersecurity program that identifies cybersecurity requirements, personnel, processes, and procedures

- Implement and enforce all Air Force cybersecurity policies and procedures using the guidance within this instruction and applicable specialized (COMSEC, COMPUSEC, TEMPEST etc.) cybersecurity publications
- Ensure all users have the requisite security clearance, supervisory need-to-know authorization, and are aware of their cybersecurity (via cybersecurity training) before being granted access to Air Force IT according to AFMAN 33-282, chapter 4, AFI 31-501 and AFMAN 33-152.
- Report cybersecurity incidents or vulnerabilities to the wing cybersecurity office
- In coordination with the Wing cybersecurity office.

3.1.2.3 Identity Management

The contractor shall provide services and solutions to accomplish identity management to enable users and applications to discover one another and utilize services provided by entities using methods such as the negotiated collaborative approach. The contractor shall also provide capabilities to selectively monitor interactions and manage all active identities to include user, services, machines and services identity based on PKI.

Create user accounts for CE based systems. Create profiles, make adjustments to user accounts and passwords, assign, modify, and delete passwords and user privileges according to AF Standard Procedures. Troubleshoot user sign-on and access problems. Establish user access rights to folders and databases. Conform to 319 CS policies for documentation and form processing as regards user accounts.

The contractor shall provide services and solutions to accomplish lifecycle entity identity management from user creation to user revocation. The contractor shall support user creation (identity confirmation, credentialing, enrollment), user management (provisioning across single or multiple systems and services, automated provisioning workflow and self-service), user access (identification, authentication and authorization) and user revocation (de-provisioning and disablement). The contractor shall enable the de-provisioning process through automated account disablements and token revocation. The contractor shall provide access controls with rights, roles and privileges.

3.1.2.4 Certification and Accreditation

The contractor shall provide services and solutions to help perform the initial security assessment, a scan of vulnerabilities, applying all relative Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) configurations. Import the scan results into eMASS, provide a copy of the scan results to the United States Air Force (USAF) CE unit, and mitigate the identified vulnerabilities prior to final acceptance by USAF through the RMF Methodology by uploading the evidence into eMASS.

Using templates provided by AFCEC/COOI, assist in completing the System Policy Document (SPD), Configuration Management Plan (CMP) and Contingency Plan (CP). The SPD when executed will assist in ensuring many of the controls are compliant.

3.1.2.4.1 Information System Security Officer (ISSO) Support
May include, but is not limited to, physical security, personnel security, incident handling, and security awareness and training.

May be called upon to assist in the development of the system security policy and to ensure compliance with the policy on a routine basis.

Will have an oversight responsibility to ensure proper access controls have been implemented for both system access and physical access to data processing facilities. Access controls apply to federal employees, contractors, and anyone else who has access to DHS systems or data.

Auditing (Logging) and Analysis; the purpose of auditing system activity is to capture sufficient information in audit logs to establish what events occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

- Should ensure audit logs are reviewed at least monthly, but more frequently if resources permit. When reviewing logs, some events will require follow-up inquiries to determine if a problem exists, whether corrective action is required, or if there is another explanation for unusual activity.

Needs to be aware of the status and expiration of the ATO. All systems must have a valid ATO prior to becoming operational. Systems not under OA must be re-authorized every three years (or earlier as determined by the AO) or when significant changes occur.

- Continuous Monitoring entails all activities conducted to ensure security controls remain effective over time. Specific continuous monitoring activities include:
    - Maintenance of a current ATO
    - Monitoring compliance
    - Conducting Annual assessments
    - Audit log reviews
    - Documentation updates
    - Vulnerability scanning
    - Account maintenance
    - Review of access lists
    - Third party compliance monitoring
    - Training
    - Incident response testing
    - Configuration management
    - System element inventory
    - Key/combination maintenance
    - Risk designations
    - Physical access monitoring

- Information Security Vulnerability Management (ISVMs)/patching

3.1.2.5 Enabling Security Capabilities
The contractor shall provide the following enabling capabilities to facilitate Warfighter access to critical mission capabilities:

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

2. Authorize access to data based on groups and roles.

3. Monitor and log all activities to provide for both real time assessment and historical analysis.

4. Use automated tools to analyze and detect anomalous behavior using real time/logged information to preclude and prevent internal attacks on AF information and computing resources.

5. Delegate roles and groups based on policy.

6. Mediate graduated access to data for various types of users.

3.1.2.6 System Operations
The contractor shall provide operational support services including, but not limited to, systems administration, customer training, and help desk support of both legacy and new applications and systems in accordance with AFI 33-115 Air Force Information Technology (IT) Service and supporting Methods and Procedures Technical Orders (e.g., Vulnerability Management MPTO, etc.), and DoD 8570.01M Information Assurance Workforce Improvement Program.

3.1.2.7 System Administation

1. Install, support, and maintain computer systems

    - Install, configure, and maintain all CE computer operating systems. CE systems include the Industrial Control Systems (ICS) with the Energy Management and Control System (EMCS), Automated Civil Engineering System (ACES) Automated Readiness Information System (ARIS) and all of its components, Fire Department ACES, NexGen IT, AutoCAD, Enterprise Military Housing Management System (eMH), E4Clicks and ArcGIS. Ensure all PCs, laptops, tablets, servers, printers, scanners, and monitors are available to support functioning of these systems weekdays between 0630-1700.

    - Maintain operability of user equipment. Image computers and deploy Operating System changes as well as the Standard Desktop configuration. Ensure user data is transferred to new setup. Format, partition, back-up, and restore hard drives. Perform timely distribution of equipment and software.

- Perform System Security Administration (SSA) duties for EMCS, NexGen IT, all ACES modules to include Fire Department (FD) & ARIS, Enterprise Military Housing Management System (eMH).

- Execute backups on all assigned systems in accordance with agency procedures to prevent potential data loss from malfunctions and preserve database integrity. Ensure all backups are cataloged, labelled and stored properly for security and safety.

- Support preparation and roll-out of new CE applications (both computer based and server based).

2. Plan and respond to service outages

3. Diagnose software and hardware failures to resolution

    a. Support servers, including troubleshooting any repairs required. Coordinate repair issues with 319 Communications Squadron (CS) to resolve communications equipment malfunction. Coordinate with appropriate maintenance organization or company and track the trouble call until it is resolved.

4. Implement and ensure security preventive measures are fully functioning

    a. Analyze and implement methods to automate system updates, patches, and virus signatures.

    b. Support servers with maintenance that includes updating and installing antivirus software as well as monitoring and installing security patches to the operating system.

5. Monitor and enhance system performance

    a. Recommend procurement of hardware and software for the organization based on optimal use of applications and business needs.

3.1.3 Enterprise Service Management

The contractor shall provide services and solutions to accomplish Singularly Managed SMI-ELS service level management. The contractor shall provide operation and maintenance of information archival and backup, disaster recovery, Continuity of Operations (COOP) and Enterprise Support Desk (ESD). The ESD shall support users encountering issues in accessing mission capabilities.

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

3.1.3.1 Help Desk Support

Provide Help Desk Tier 1 and Tier 2 support for technical assistance, support of multiple software versions, training, warranty, and maintenance, 8-hours a day, 5-days a week, excluding Federal Holidays.

Provide customer assistance and information on warranty service, configuration, installation/implementation, systems administration, database administration, back-up/contingency planning, systems management, facilities management, operation of the contractor-provided software and hardware, and assistance to isolate, identify, and repair failures.

Tier 1 – Basic application software and/or hardware support

Tier 2 – More complex support on application software and/or hardware

Assist users in developing technical processes to streamline and adapt their work processes. Recommend or develop software solutions as well as possible hardware refinements for specific processes used within the 319 CES.

Provide technical assistance with process documentation/workflow knowledge articles and self-service guidance for the unit.

Understand project objectives and be able to apply understanding of how processes should work to operational improvement initiatives.

Provide recommendation in the facilitating process workflow modeling in order to collaborate on process improvements, automation capabilities and clearly defined end-to-end use cases.

Participate in the problem resolution.

Support users in setting up hardware systems including printers, microcomputers, and other peripheral devices.

Restore files and databases for users when requested.

3.2 Network Services and Solutions

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

3.2.1 Enterprise Information Management.

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

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

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

1. Web Content Directory – The ability to unit members access to their appointed SharePoint site

2. Web Content Delivery –The contractor shall provide the capability to assist CE SharePoint owners when standing up a SharePoint page and, providing assistance to maintain the site(s).

3.2.1.3 Database Administration and Automation.
The contractor shall provide services and solutions that accomplish or provide the following enabling capabilities:

3.2.1.3.1 Database Administration.
The contractor shall perform all industry standard database administration roles and responsibilities including creating, installing, configuring, modifying and tuning databases on the five AFOSI enclaves. Additional duties required include ensuring that databases are backed up and can be recovered, assigning user permissions and roles, troubleshooting, performance monitoring, and capacity planning.

Development and maintenance tools and technologies currently include the following:

1. Assist users in developing technical processes to streamline and adapt their work processes. Recommend or develop software solutions as well as possible hardware refinements for specific processes used within the 319 CES.

2. Provide technical assistance with process documentation/workflow knowledge articles and self-service guidance for the unit.

3. Understand project objectives and be able to apply understanding of how processes should work to operational improvement initiatives.

4. Provide recommendation in the facilitating process workflow modeling in order to collaborate on process improvements, automation capabilities and clearly defined end-to-end use cases.

5. Managing and maintaining database management systems (DBMS) such as Oracle and MS SQL in support of above mentioned applications

6. DBMS management tasks include creating and managing users and roles, assigning permissions, capacity planning, troubleshooting and restoration.

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

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

9. Database Management - Perform loads, upgrade, patches, data recovery, backups.

3.2.1.4 Technology Insertion
The Contractor shall investigate and analyze innovative and emerging technologies that in the most economic and efficient manner improve not only IT system performance and support but also mission performance.

3.2.1.4.1 Compliance and Vulnerability
Changing technology, changing laws and compliance, internal governance requirements, evolving best practices and operational risk analysis all contribute to systems being in varying states of compliance and vulnerability. Systems, when deployed or refreshed default to a vulnerable or non-compliant status and must be actively configured in order to mitigate vulnerabilities and achieve compliance. Maintaining a secure environment requires continuous process improvement (CPI). CPI requires experienced personnel to constantly evaluate the existing and planned information technology environment, assess areas for improvement, make recommendations and implement directed changes.

The Contractors shall:

1. Perform IT strategic planning with the government

2. Investigate emerging technologies and present alternatives to the Government.

3. Document alternatives in the Technology Insertion Plan.

4. Develop and coordinate detailed proposals for implementation of new technologies to the PAB for approval and funding

5. Ensure recommended alternatives are in concert with overall AF recommended and proposed technologies.

6. Provide the Government with a Life Cycle Support Plan (LCSP) for all new technologies.

7. Implement approved plans.

3.2.1.5 Software/Hardware Maintenance and Warranty.
When Government purchased software/hardware maintenance packages are available, the contractor shall utilize the software updates and patches for software and hardware replacements as needed. The contractor shall utilize these maintenance agreements as necessary and provide feedback to the Government if any issues are experienced with unsupported technology or unresponsive services. As the party responsible for software upgrades and hardware replacements, the contractor shall utilize OEM support, track hardware in the Equipment Tracking Report, and maintain a five (5) year hardware, software, and cert refresh schedule for all equipment/applications.

Maintain inventory and device management lists and databases for 319 CES. Notify the unit Automated Data Processing Equipment (ADPE) Equipment Custodian (EC) of any hardware relocation. Ensure a current list of software/hardware is maintained reflecting changes. Perform annual inventory of equipment and software. Maintain paperwork for equipment swapped while under warranty, using hand receipts and appropriate equipment tracking procedures. Prepare turn-in documents for hardware for disposal when needed.

Provide software application assistance to users for commonly used office applications purchased from standard Air Force infrastructure support contracts.

Maintain physical control of original software and images or working copies of software including all Software licensing agreements

Help users maintain an understanding of and adhere to all Air Force policies and processes.

Any issues outside of technical support shall be referred to the Acquisition Program Manager. Contractor shall follow AFI 33-112 for all equipment transfer. Any transfer of IT equipment (Blackberry devices, VoIP phones, PCs, laptops, servers, routers, etc.) must be coordinated through the FSS IT Equipment Custodian (ITEC) prior to the equipment leaving contractor control (i.e., being issued, installed or shipped). Contractor shall provide type of equipment, manufacturer, model, serial number and gaining point-of-contact information to the FSS ITEC when applicable. Contractor shall not accept any equipment from users other than for temporary troubleshooting and a Temporary Issue Receipt (AF Form 1297) shall be provided to the user. All faulty equipment must be returned to the user with instructions to contact their ITEC for proper disposition procedures.

3.3.1 Contractors Use of NETCENTS-2 Products Contract

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

3.3.2 Software License Management

The contractor shall provide maintenance and support to control the entire asset lifecycle, from procurement to retirement, which includes applications, license agreements as well as software upgrades. The contractor shall provide asset inventory and services that track the asset, contract management, leases, maintenance agreements and service contracts. The contractor shall support common practices for ordering assets, tracking orders and assets and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment and configuration control, to include the procurement of supporting software licenses.

3.3.3 Training

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

- Minimum certification requires Information Assurance Technical Level II, Information Systems Security Office (ISSO), Security + certified, or higher in compliance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005 (with all current changes).

3.3.3.1 Other Government-Provided Training

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

1. The Contractor employees' participation is on a space-available basis,

2. The Contractor employees' participation does not negatively impact performance of this task order, and

3. The Government incurs no additional cost in providing the training due to the Contractor employees' participation.

4. Specific events related to acquiring information and training can be pro-rated and paid for by the contractor at the discretion of the government and contractor, including information gathering trips to other work sites and base training events to keep all communications technicians current with new policies or methods.

3.3.3.1 Other Required Technical Travel Expense

The Contractor personnel may be required to travel in performance of the PWS (see Travel Requirements). The Contractor shall coordinate specific travel arrangements with the Government MPES Program Manager and the COR to obtain advance, written approval (Contractor needs to submit request three (3) weeks in advance) for the travel about to be conducted. The Contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel.

3.3.4 Place of Performance

Work shall primarily be performed at 319 CES Information Management Section Bldg 410, 525 Tuskegee Airmen Blvd, Grand Forks AFB ND 58205-3464. Some travel to other buildings on site will be required to troubleshoot user issues, download and review log files, and maintain files in backup storage locations.

3.3.5 Normal Hours of Operation

The average work week is 40 hours. The average workday is 8 hours and the window in which those 8 hours may be scheduled is between 6:30 AM and 5:00 PM, Monday through Friday, except for days listed in Clause G021, Contract Holidays, in the overarching ID/IQ contract. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Work in excess of the standard 40 hour work week requires prior written approval by the Quality Assurance Personnel (QAP).

3.3.6 Government Furnished Property

No Government Furnished Property is being provided to the Contractor in support of this Task Order (TO). This TO requires the contractor to work in a Government facility, the Government will provide or make available working space, network access, and equipment to include:

- Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, SharePoint etc.)

- Telephone (local/long distance calls authorized as dictated by Task Order performance requirements)

- Facsimile
- Copier
- Printer

All facilities, equipment and information will remain the property of the Government and will be returned to the Contracting Officer Representative (COR) or other designated representative upon request or at the end of the TO period of performance.

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

3.3.8 Non-Personal Services
The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Task Order (TO) Contracting Officers CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government.

3.3.9 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.

3.4 Performance Reporting

The contractor's task order performance will be monitored by the Government and reported in a Customer Survey. Performance standards shall include the contractor's ability to provide or satisfy the following:

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

3.4.1 Program Management/Project Management

The contractor shall identify a Program Manager or a Project Manager, in writing, 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.

3.4.2 Documentation and Data Management

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

4.0 SERVICE DELIVERY SUMMARY

Performance Objective	Performance Threshold	
	Target	Tolerance
System security compliance	3.1.2.2 Information Assurance	Maintain Assessment & Authorization compliance IAW applicable DoD and AF policy and instruction, particular DoD Instruction 8500.2 – Information Assurance
Patches and Updates: Ensure all updates and patches are applied	3.1.2.4.1 Information System Security Officer (ISSO) Support	Working within 30 days of patch release. Any problems with patches shall be resolved within one business day.
Application security compliance	3.1.2.4.1 Information System Security Officer (ISSO) Support	Maintain application security compliance IAW applicable DoD Policy and instruction, particularly the Security

		Technical Implementation Guide (STIG)
Auditing (Logging) and Analysis	3.1.2.4.1 Information System Security Officer (ISSO) Support	Monitor/log: ICS log files every 30 days
Maintain CP, CMP, and SPD for organizations	3.1.2.4.1 Information System Security Officer (ISSO) Support	Plans updated with changes ≤ 10 business days 95% of the time
Install, configure, and maintain all CE computer Operating Systems	3.1.3.1 Help Desk Support	No more than 1 valid complaint per month. Contractor will provide COR written notification of any customer service delay over 24 business hours and/or service problem.
Respond to customer help requests	3.1.3.1 Help Desk Support	Provide problem resolution for assigned calls, 90% of assigned calls have a problem resolution.
Backup and Restore Requirements	3.2.1.3.1 Database Administration	Backups completed as scheduled 98% of the time.

4.2.2 Task Order (TO) Management

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

4.2.4 Records, Files and Documents

All physical records, files, documents and work papers, provided and/or generated by the government and/or generated for the government in performance of this PWS, maintained by the contractor which are to be transferred or released to the government or successor contractor, shall become and remain government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense

Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the government or the contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the NetOps and Infrastructure Solutions contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

The Contractor shall make available in a timely manner, any permits, reports, or general performance data required in the PWS/SOW.

The contractor shall create, handle and maintain records for the Air Force, regardless of medium, (in a pre agreed medium that can be used by the Air Force) in accordance with the requirements established in AFRIMS Records Disposition Schedule (RDS), AFI 33-322, Records Management program, AFI 33-364, Records Disposition Procedures and Responsibilities, and AFMAN 33-363, Management of Records. Full text versions of these publications are available for download at http://www.epublishing.af.mil

The contractor's records person should obtain a Records Management AFRIMS account certification by completing the POC training provided by the Base Records Manager. Inquiries as to the specific actions necessary to meet the requirements established in the above referenced publication may be directed to the GFAFB Records Management Office at (701) 747-4658 or 319th CS/SCXK, Bldg 314, GFAFB, ND, 58205-6436.

4.2.5 Travel Requirements

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

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

4.2.6 Personnel Security

Individuals performing work under these task orders shall comply with applicable program security requirements as stated in the task order.

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

The contractor and, as applicable, subcontractor shall not employ persons for work on this contract if such employee is identified as a potential threat to the health, safety, security, general well-being or operational mission of the installation and its population, nor shall the contractor or subcontractor employ persons under this contract who have an outstanding criminal warrant as identified by the National Crime Information Center (NCIC). NCIC checks will verify if a person is wanted by local, state, and federal agencies. All contractor and subcontractor personnel must consent to NCIC background checks. Contractor and subcontractor personnel who do not consent to an NCIC check will be denied access to the installation. Information required to conduct an NCIC check includes: full name, driver's license number, and/or social security number, date of birth of the person entering the installation, and completion of a background check questionnaire. The contractor shall provide this information using the Grand Forks AFB Form 41, Contractors Consent for Background Check, and shall submit it in conjunction with the contractor's request for either base or vehicle passes. Completion of a successful NCIC check does not invalidate the requirement for an escort when contractor or subcontractor personnel are working within controlled or restricted areas. Contractors shall ensure their employees and those of their subcontracts have the proper credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens will be remanded to the proper authorities. The contractor shall not be entitled to any compensation for delays or expenses associated with complying with the provisions of this clause. Furthermore, nothing in this clause shall excuse the contractor from proceeding with the contract as required. A list of contractor employees, along with all required personal data, shall be provided to the Contracting Officer at least 15 calendar days prior to commencement of work by individuals. Any turnover in contractor employees shall immediately be provided in writing to the Contracting Officer.

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

4.2.7 Other Direct Cost (ODC)

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

4.2.8 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 task order 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 Task Order. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

4.2.9 Section 508 of the Rehabilitation Act

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

4.3.1 Security Requirements

4.3.1.1 Security Facility Clearance Requirements

Not Applicable

4.3.1.2 Personnel Security Clearance Requirements

All of the personnel performing work on this contract will require a security clearance as identified below:

(X) Secret

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

4.3.1.3 Additional Investigation Requirements

Not Applicable

4.4.1 Obtaining and Retrieving Identification Media

The contractor shall comply with the procedures outlined in AFFARS 5352.242-9000, Contractor Access to Air Force Installations. The contractor shall ensure contractor employees obtain a DOD Common Access Card (CAC) as required for contract performance in compliance with AFI 36-3026. The contractor must comply with the requirements set forth and prescribed by AFFARS 5352.242-9001, Common Access Cards for Contractor Personnel.

4.4.2 Pass and Identification Items

Contractor personnel shall apply for a Base Identification Card to be carried while on GFAFB. Contractor personnel shall be issued an SFMIS AF Form 75 (Visitor Pass) from the commercial visitor control center (S. Gate). Upon completion of screening process the contractor and employees shall be issued a pass for the duration of the contract (not to exceed 1 year). While

on the installation, contractor and employee vehicles are subject to search, only company vehicles are allowed access to restricted/controlled areas. All Government properties (identification cards, restricted area badges) must be returned within 24 hours after employment is terminated. It is the responsibility of the contract manager to retrieve, turn-in, or report any loss or misuse of such items to the Base Pass and Identification office.

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

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

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

4.4.3 Visitor Group Security Agreement (VGSA)
Not Applicable

4.4.4 Information Security
The contractors performing duties associated with this task order must adhere to all the standards for protecting classified information as specified in DoDM 5200.01, volumes 1-4, *DoD Information Security Program*, Air Force Instruction 31-401, *Information Security Program Management* and all applicable supplements and operating instructions.

4.4.5 Unescorted Entry to Secure Rooms
Not Applicable

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

(X) AIS-II Position - Noncritical-Sensitive Positions. Security Clearance: SECRET

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

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

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

4.5.1 Wireless Electronic Devices
The following devices are not allowed in areas where classified information is discussed, briefed or processed: cell phones, camera cell phones, cordless telephones, wireless microphones, wireless keyboards, wireless mice, wireless or Infrared Local Area Networks (LANs). The term ***"Area"*** above refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed or processed, wireless pointer/mice devices are allowed for presentations only. This is an acceptable EMSEC risk. All other Personal Electronic Devices, PEDs. All other wireless PEDs not specifically addressed above, that are used for storing, and processing and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed or transmitted.

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

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

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

4.5.5 Key Control
The contractor will adhere to the Air Force activity Operating Instructions Key Control, procedures if provided a key. Contractor must properly safeguarded all keys and not allow any unauthorized personnel to have access to the keys. The contractor shall not duplicate keys issued by the government. All government issued keys will be returned at the end of contract employment or when no longer needed. Lost keys shall be reported immediately to the Air Force activity that issued the keys and Gunter Security Office. The government may replace lost keys or perform re-keying.

The total cost of lost keys, re-keying or lock replacement shall be deducted from the monthly payment due to the contractor.

4.5.6 Security Combinations
Not Applicable

4.5.7 Security Alarm Access Codes
Not Applicable

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

4.6.1 Traffic Laws:
The contractor and their employees shall comply with all installation traffic regulations.

4.6.2 Cellular Phone Operation Policy
The contractor shall comply with local base policies regarding cellular phone operation.

4.6.3 Security Education and Training
The contractors are required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system. Annually, all contractors will complete all required security training. Required annual training includes Force Protection (FP), Information Protection (IP), Cybersecurity and OPSEC

The contractor will arrange to receive for its employees to attend Anti-terrorism Awareness, AT Level I training during their initial 60 days of employment. This training will be coordinated by the government QAP personnel. The training will be in accordance with the standards outlined in AFI 10-245 Table 2.1.

Appendix 1: Applicable Standards & References

Purpose:

The following certifications, specifications, standards, policies and procedures in Table 2 represent documents and standards that may be placed on individual contract task orders. Individual task orders may impose additional standards to those required at the contract level. The list below is not all-inclusive and the most current version of the document in the AF Standard Center of Excellence Repository (SCOER) at the time of task order issuance will take precedence. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant Task Order, such as specific FIPS, NIST, or MIL-Standards. Web links are provided wherever possible.

Documentation	URL
INFORMATION ASSURANCE	
DoDD 8500.01E Information Assurance (IA)	https://acc.dau.mil/CommunityBrowser.aspx?id=22214
DoDI 8500.2, Information Assurance (IA) Implementation	https://acc.dau.mil/adl/en-US/378014/file/51140/ref%20e_DODI850002p_Info%20Assure%20Implementation.pdf
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf
DoD 8570.01-M, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
AFI 33-200, Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf
Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/index.html
AFI 10-245, Antiterrorism	
QUALITY ASSURANCE	
AFMAN 33-363, Management of Records	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf

Documentation	URL
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
AFI 133-115, Air Force Information Technology (IT) Service Management	
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
DoDD 5205.02, Operations Security (OPSEC) Program	http://www.fas.org/irp/doddir/dod/d5205_02.pdf
AFI 10-701, Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf
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
DoDI 2000.16, Antiterrorism Standards	http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf
DoD 5400.7-R, Freedom of Information Act Program	http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf
Section 508 of the Rehabilitation Act of 1973	http://www.opm.gov/html/508-textOfLaw.asp
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
AFI 31-501, Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi31-501/afi31-501.pdf
, Information Security Program Management	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi31-401/afi31-401.pdf
Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma
FAR CLAUSES	
DFARS 252.227-7014 Rights in Noncommercial Computer Software	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P683_47378

Documentation	URL
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
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