

2012

Application Services PWS Template



Version 1.2

16 October 2012



INSTRUCTIONS:

1. You must use this format for your Application Services Performance Work Statement
2. Save a copy of this template and modify it according to your requirements. Each time a PWS is accomplished, come back to the User's Guide and download the PWS template. The language, standards, and references will be updated over time.
3. All bold italic text within brackets [] is instructional information specific to the section.
4. Text not within brackets is information that you are **HIGHLY ENCOURAGED** to keep in your PWS; only apply modifications, introduce additional information, or include updates in the event that standards or instructions change, or when deemed necessary by your specific program's or organization's policies.
5. Do not deviate from the format of this template. Doing so could delay the acquisition of your services and support. Using a standard template will help the offerors in knowing where to look for requirements and will decrease the time required to solicit proposals for the Task Orders.
6. All citations to policies, directives, instructions, and reference material are included in [Appendix A5, Application Services Standards & References](#).
7. Before submitting your completed PWS, REMEMBER TO DELETE all instructional text contained within brackets. It is shown here for instructional purposes only and must not remain in the final document.



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

Name:	
Organization:	
Address:	<i>[physical mailing address]</i>

Executive Summary

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



NETCENTS-2 Application Services Task Order PWS
[Requesting Agency Task Order Title]

1. PURPOSE

[In this paragraph, define the overall purpose and objectives of the Task Order]

2. SCOPE

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

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

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

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

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



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



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



Factor	Data
Average help desk call volume	Provide by severity levels and the numbers that have passed from level 1 to 2 to 3.

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

3.1 Systems Sustainment **[Sections 3.1-3.5 are example requirements that will help facilitate the development of your PWS. Please modify the below requirements as necessary to help meet your overall program requirements. Please remove examples that are not applicable to your PWS]**

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

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

- Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases, and interfaces in compliance with applicable AF/DoD standards
- Support system sustainment activities to include maintaining existing legacy systems and environments and to sustain applications, databases, and interfaces
- Provide application services to support, maintain, and operate systems or services

3.2 Systems Development, Migration, and Integration

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

- Conduct software development, software security, web services development, web services testing, smart phone or other IT device applications and testing, security layer integration, database clean-up, data wrapping, and data conversion
- Develop, operate and maintain prototype applications, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. Develop schedules and implementation plans, including parallel operations, identification of technical approaches, and a description of anticipated prototype results.
- Perform system performance tuning, system re-hosting, and integration services



- Migrate legacy systems to an Enterprise Resource Planning (ERP) system or an existing standard infrastructure such as the Global Combat Support System (GCSS) or DoD Enterprise Computing Center (DECC)
- Utilize Government-Off-The-Shelf (GOTS) or approved Commercial-Off-The-Shelf (COTS) tools for systems design and development

3.3. Information Services

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

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

3.3.1 Development of New SOA Applications and Data Services

- Expose authoritative data, as defined, by re-engineering a business process, identifying the sources for the authoritative data, and establishing user roles and permissions for information access as directed by COI
- Support lifecycle management of new SOA-based applications that encapsulate business logic to provide new functional/operational mission capabilities

3.3.2 Create Aggregation Services

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

3.3.3 Create Presentation Services

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

3.3.4 Specify Information Assets for Exposure

- Generate specification for exposing authoritative data as information asset payloads
- Create semi-automated services that enable the specification of information assets by editing, sorting, filtering, and translating
- Utilize applicable data definitions and standards for information assets to be exposed



- Create schema/documentation for organizations to register for use throughout the DoD enterprise

3.3.5 Registering Services

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

3.3.6 Web Services

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

3.3.7 Service Lifecycle Management

- Generate necessary design and implementation artifacts that will support lifecycle management, defined as service development, testing, certification, registration, sustainment, and evolution aligned

3.3.8 Vocabulary Management

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

3.3.9 Register Vocabularies

- Support the alignment, articulation and registration of vocabulary artifacts

3.3.10 Data Stores

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

3.3.11 Information Exposure Services

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



3.4 Systems Operations

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

The contractor shall provide operational support services including, but not limited to, database administration, systems administration, customer training, and help desk support of both legacy and new applications and systems.

3.4.1 Database Administration

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

3.4.2 Systems Administration

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

3.4.3 Customer Training

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

3.4.4 Help Desk Support

- Provide Help Desk Tier 1, Tier 2, and/or Tier 3 support for technical assistance, order processing, support of multiple software versions, training, warranty, and maintenance, 24-hours a day, 7-days a week, 365 days a year
 - Tier 1 – Basic application software and/or hardware support
 - Tier 2 – More complex support on application software and/or hardware
 - Tier 3 – Usually subject matter experts, support on complex hardware and OS software issues

3.5 Agent of the Certifying Authority (ACA) Support Services

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

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



- ACA support **with** IAM/IAO functions seeking an authority independent of the program to perform both **testing** and **validating** of any existing IS security controls put in place by the IS developers. If mitigations to remaining IS vulnerabilities are required, the ACA possesses the necessary skills to recommend additional security controls for program personnel to implement so that the ACA could subsequently re-test and validate.
- ACA support **without** IAM/IAO functions seeking an authority independent of the program to perform **validation** of security controls implemented and tested by IAM/IAO personnel before the AF-CA can certify the IS for accreditation at the appropriate Designated Accrediting Authority (DAA).

3.6 [Next Requirement]

4. ENGINEERING REQUIREMENTS

4.1 Systems Engineering [Sections 4.1-4.5.3 are example requirements that will help facilitate the development of your PWS. Please modify the below requirements as necessary to help meet your overall program requirements. Please remove examples that are not applicable to your PWS]

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

4.1.1 Life-Cycle Systems Engineering

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

4.1.2 Systems Engineering Process (SEP)

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

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

4.1.3 Reliability, Availability, Maintainability (RAM) – RISE Manual/Handbook

The contractor shall employ the practices prescribed and defined in the RISE Handbook to address RAM in their programs. The RISE Handbook sections provide information on recommended RAM activities and processes to be undertaken in each of the four main acquisition life cycle phases: Materiel Solution Analysis phase, Technology Development Phase, Engineering & Manufacturing Development Phase, and Production & Deployment Phase. The RISE Handbook is intended to provide acquisition managers insight into RAM activities and products so that they can staff their programs with the necessary RAM subject matter experts who will develop these products and provide the inputs required at each milestone review.



4.1.4 Service Development and Delivery Process (SDDP)

The contractor shall utilize and follow the SDDP as guidance when it has been approved for the definition, design, acquisition, implementation and delivery of warfighter capabilities. The SDDP is applicable to large and small scale problems and can be used to implement IT capabilities of all sizes and types across all mission areas and all security domains. The SDDP is captured in AFMAN 10-606 and implements AF Policy Directive 10-6, *Capabilities-Based Planning & Requirements Development* and AF Instruction 10-601, *Capabilities-Based Requirements Development*, by providing guidance for developing and implementing Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities DOTMLPF requirements, including IT capabilities.

4.2 Architecture and System Design

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

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

4.2.1 Department of Defense Architectural Framework (DoDAF) Guidance

The contractor shall provide all required design and development documents, and supporting architectural documentation in compliance with the latest Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance version 2.02 established in August 2010.

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

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

4.2.3 Capabilities Integration Environment (CIE)

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

4.2.4 DoD Mobility Strategy

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

4.2.5 Federal Desktop Core Configuration (FDCC)

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

4.3 Configuration Management

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



4.4 Testing

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

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

4.4.1 Test Lab

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

4.4.2 Regression Testing

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

4.4.3 Product/System Integration Testing

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



acceptance testing. The contractor shall provide a logical test process that minimizes interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing.

4.4.4 Simulated Operational Testing

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

4.4.5 Acceptance Testing

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

4.4.6 System Performance Testing

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

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

4.5 Information Assurance

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

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

4.5.1 System IA

For those solutions that will not inherit existing network security controls, and thus integrate an entirely new application system consisting of a combination of hardware, firmware and software, system security assurance is required at all layers of the TCP/IP DoD Model. The contractor shall ensure that all system deliverables comply with DoD and AF IA policy, specifically DoDI 8500.2, *Information Assurance Implementation*, and AFI 33-200, *Information Assurance Management*. To ensure that IA policy is implemented correctly on systems, contractors shall ensure compliance with DoD and AF Certification & Accreditation policy, specifically DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, and AFI 33-210, *Air Force Certification and Accreditation Process (AFCAP)*. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public*



Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.5.2 Application IA

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 associated with SQL injections, cross-site scripting, and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.5.3 Personnel IA

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*, 19 December 2005 (with all current changes), and as stipulated in Section H, Clause H101 of the overarching Application Services RFP.

5. CONTRACTUAL REQUIREMENTS

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

5.1 Contractors Use of NETCENTS-2 Products Contract

The contractor shall obtain all products and associated peripheral equipment required of this task order from the NETCENTS-2 Products contract as stipulated in Section H Clause H098 of the overarching Application Services RFP.

5.2 Place of Performance

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

5.3 Normal Hours of Operation

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

The average workweek is 40 hours. The average workday is 8 hours and the window in which those 8 hours may be scheduled is between 6:00 AM and 6:00 PM, Monday through Friday or as specified in this TO, except for days listed in Clause G021, Contract Holidays, in the overarching ID/IQ contract. Billable hours are limited to the performance of services as defined in the TO. Government surveillance of



contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Work in excess of the standard 40 hour work week requires prior written approval by the Quality Assurance Personnel (QAP).

5.4 Government Furnished Property

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

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

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

Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the Task Order 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 period of performance.

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 COR upon request or completion of the Task Order.

5.5 Billable Hours

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

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

5.6 Non-Personal Services

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



The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the 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. These operating procedures may be superseded by Theater Commander's direction during deployments.

5.7 Contractor Identification

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

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

5.8 Performance Reporting

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

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

5.9 Program Management / Project Management

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

5.9.1 Services Delivery Summary

Reference Section 6, Services Delivery Summary, of this Task Order PWS for specific performance objectives.

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

5.9.2 Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/task order manager who will oversee all aspects of the task order.



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

5.9.3 Documentation and Data Management

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

5.9.4 Records, Files, and Documents

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

5.9.5 Personnel Security

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

This task orders may require personnel security clearances up to and including Top Secret, and may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed task order. The task orders may also require access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the 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 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.

5.9.5.1 Transmission of Classified Material

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

5.9.5.2 Protection of System Data

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

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

5.9.5.3 System and Network Authorization Access Requests

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

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

5.9.6 Travel

The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or Contracting Officer's Representative 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 task order 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.

5.9.7 Other Direct Cost (ODC)

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



5.10 Training

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

5.10.1 Mission-Unique Training

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

5.10.2 Other Government-Provided Training

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

- (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,
- (3) The Government incurs no additional cost in providing the training due to the contractor employees' participation, and
- (4) Man-hours spent due to the contractor employees' participation in such training are not invoiced to the task order

5.11 Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017, the Contractor shall disclose to the ordering 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.

5.12 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.

5.13 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>.

5.14 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, which would include applications, license agreements, and software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets, and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment and configuration control, to include the procurement of supporting software licenses.

5.15 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.

5.16 Section 508 of the Rehabilitation Act

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

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

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



IAW DODI 3020.37. Note: It is the responsibility of the Combatant Commander to determine mission-essential functions and to establish procedures to ensure that these standard support requirements and any additional requirements are met.

5.18 Anthrax Information

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

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

5.19 Incentives

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

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

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

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

6. SERVICES DELIVERY SUMMARY

[Modify to fit task order requirements. Make sure the services required have measurable outcomes. Refer to Appendix A3, “Application Services Sample Performance Parameters,” for sample performance parameters.]

7. DATA DELIVERABLES

[Define deliverables required for individual task orders. This section contains information on data requirements, such as reports or any of those items contained within a Contract Data Reports List (CDRL). Strive to minimize data requirements that require government approval and delivery. Only acquire data that are absolutely necessary. The usual rule of thumb is to limit data to those needed by the government to make a decision or to comply with a higher level requirement. Refer to Appendix A4, “Application Services Task Order Data Item Description Deliverables,” for sample data item deliverables. Deliverables should relate directly to the Services Delivery Summary in Section 6. Detailed CDRL requirements and formats should be provided IAW DFAR 204.7105 on DD



Form 1423-1, FEB 2001. Note, the number and complexity of required Deliverables need to correlate to the size and complexity of requirements contained in the Task Order.]

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

8. APPLICABLE STANDARDS AND REFERENCES

[Refer to Appendix A5, “Application Services Standards & References,” for applicable certifications, specifications, standards, policies and procedures that are required for compliance on individual Task Orders. Tailor the list as needed for 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.]

9. PRODUCTS STANDARDS AND COMPLIANCE REQUIREMENTS

[Tailor this list of products standards and compliance requirements depending on the required hardware and software required of this task order.]

Information Assurance (IA) Technical Considerations

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

DoD IPV6 Requirement

All Products must meet the criteria in DoD IPV6 Standard Profiles for IPV6 Capable Products version 5.0 July 2010 (http://jitic.fhu.disa.mil/apl/ipv6/pdf/dsr_ipv6_50.pdf). Some example IPV6 mandated products from the DoD IPV6 Standards Profile are listed below:

- Host/Workstations - a desktop or other end-user computer or workstations running a general purpose operating system such as UNIX, Linux, Windows, or a proprietary operations system that is capable of supporting multiple applications
- Network Appliance or Simple Server - Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A Simple Server supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol



(SIP)11 servers, a “web camera” appliance that serves pictures via an embedded web server, and a network time server appliance that solely functions to serve NTP requests. Advanced Server - End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network

- Intermediate Nodes – Routers, Switches, IA or IA enabled devices
- IPV6 Capable Software - a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform.

Energy Star

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

ENERGY EFFICIENCY IN ENERGY-CONSUMING PRODUCTS (DEC 2007)

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

(1) Means a product that—

- (i) Meets Department of Energy and Environmental Protection Agency criteria for use of the Energy Star® trademark label; or
- (ii) Is in the upper 25 percent of efficiency for all similar products as designated by the Department of Energy's Federal Energy Management Program.

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

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

- (1) Delivered;
- (2) Acquired by the Contractor for use in performing services at a Federally-controlled facility;
- (3) Furnished by the Contractor for use by the Government; or
- (4) Specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance.

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

- (1) The energy-consuming product is not listed in the ENERGY STAR Program or FEMP; or
- (2) Otherwise approved in writing by the Contracting Officer.

(d) Information about these products is available for—

- (1) ENERGY STAR at <http://www.energystar.gov/products>; and
- (2) FEMP at www.femp.energy.gov/technologies/eep_purchasingspecs.html.

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

http://www1.eere.energy.gov/femp/technologies/eep_purchasingspecs.html

Encryption Mandates



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

BIOS Mandate

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

Biometric Mandate

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

Special Asset Tagging

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

- Items for which the Government’s unit acquisition cost is less than \$5,000, when identified by the requiring activity as DoD serially managed, mission essential or controlled inventory;
- When the Government’s unit acquisition cost is less than \$5,000 and the requiring activity determines that permanent identification is required;
- Regardless of value, (a) any DoD serially managed subassembly, component, or part embedded within an item and, (b) the parent item that contains the embedded subassembly, component or part.

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

Software Tagging

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

Radio Frequency Identification (RFID)

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



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.

Hardware and Associated Software and Peripherals

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

Authorized Resellers

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

Technical Refresh

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

Trade Agreement Act (TAA)

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

Items on Backorder

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



Installation

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

Warranty

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

Customer Support

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

Product Maintenance

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

