



## Systems Sustainment PWS Template

### INSTRUCTIONS:

1. If your program falls under AFPEO BES, you must use this format for your Systems Sustainment Performance Work Statement.
2. Save a copy of this template and modify it according to your requirements. Each time a Systems Sustainment PWS is accomplished; make sure to download the newest version of the PWS template from the NETCENTS-2 website. 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 Section 8, *Applicable 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**  
**Systems Sustainment**  
**Performance Work Statement (PWS)**

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

**EXECUTIVE SUMMARY**

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



**NETCENTS-2 Systems Sustainment 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.]***

***[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 Dependencies**

***[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.]***



### 3.2 System Details

If the number and types of releases are known, even for the first 12 month period, provide that information. The following table provides system information that can be used to provide needed context in order to propose technical and pricing information for the work outlined in the task order.

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



Factor	Data
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 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	Provide a complete list of the OS and all COTS/GOTS utilities including Development Tools along with the version numbers of each.
Platform	Provide the list of the HW baseline for servers along with capacity, model numbers, etc.
Programming Languages	See first row above. Also provide the programming language versions being used (i.e. Java 1.6, TCL/TK 8.4.x, COBOL 85, Oracle 11G, etc.)
Programs	See row 1 above. This need to be expanded to show the profile of all the types of development components (i.e. copy books, libraries, JCL, scripts, screen definitions, etc.) and not just the number of programs.



Factor	Data
Database	See row 1 above on the database information needed.
COTS	Provide complete list and version numbers. Also provide any licensing restrictions/limitations that my prohibit exploitation by a bidder on the use of a product that is limited for that application/project.
Avg. transactions per day	This needs to be by type (i.e. updates, inquiries, web services, etc.).
Interfaces	Provide ICDs or equivalent information about the nature and design of the interace (i.e. frequency, data definitions, triggers, mechanism such as ftp or web service, etc.).
Upgrades	Planned as well as past history for both COTS and the applications.
Average help desk call volume	Provide by severity levels and the numbers that have passed from level 1 to 2 to 3.

### 3.3 Systems Support

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
- 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 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

### 3.4 Help Desk Support

The Contractor shall provide continuous Help Desk Tier 2 and Tier 3 support 7-days a week, 365-days a year. The Contractor shall provide patch management support for multiple software versions, providing technical assistance, training, warranty, and maintenance, for reporting deficiencies in software and hardware. The Contractor shall provide methods for responding to customer requests and order processing. The Contractor shall use deficiency reporting tools and establish methods for resolving and closing deficiency reports. The Contractor shall monitor discrepancy reports, provide performance improvement recommendations, identify environmental changes and changes in Government equipment or regulations and make the recommended performance improvement, environmental, or equipment changes as requested by the Government. Note, Tier 1 Help Desk is supported through the Field Assistance Service (FAS) at 334-416-5771 or DSN 596-5771.

Definitions:

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

### 3.5 [Next Requirement]

## 4. ENGINEERING REQUIREMENTS

### 4.1 Systems Engineering

***[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 Service Development and Delivery Process (SDDP)**

The contractor shall utilize and follow the SDDP as guidance 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**

***[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 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 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.

### **4.4.2 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.

#### **4.4.3 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.

#### **4.4.4 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 the 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 Defense Information Systems Agency (DISA) Application Security Development Security Technical Implementation Guide (STIG), which includes the need for source code scanning 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 by each individual 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 the 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 GFE and/or 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 the 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 for specific guidance.***

## **5.8 Performance Reporting**

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

- Provide quality products, incidentals, and customer support
- Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times
- Timely and accurate reports
- Responsive proposals
- Configuration assistance as identified in each delivery order

## **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 63-124, Performance Based Services Acquisition 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 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).

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 the Task/Delivery 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 the Task Order. This disclosure obligation shall apply to technical data and non-commercial computer software developed exclusively at Government expense by subcontractors under any 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 Performance of 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 the services being required of this Task Order. Make sure the services required have measurable outcomes.]**

Performance Requirements	Performance Threshold	Monitoring Method
<b>APPLICATION AVAILABILITY</b>		
Unscheduled application downtime	Customer meets application availability thresholds; Equal or fewer than 61.2 hours	QAE monthly review of system metrics
Unscheduled application downtime	Customer exceeds application availability thresholds; Equal or fewer than 26.2 hours	QAE monthly review of system metrics
Unscheduled application downtime	Customer exemplifies application availability thresholds; Equal or fewer than 4.4 hours	QAE monthly review of system metrics
Scheduled application downtime	Customer meets application availability thresholds; Equal or fewer than 200 hours	QAE monthly review of system metrics
Scheduled application downtime	Customer exceeds application availability thresholds; Equal or fewer than 50 hours	QAE monthly review of system metrics
Scheduled application downtime	Customer exemplifies application availability thresholds; Equal or fewer than 12 hours	QAE monthly review of system metrics
Mean Time To Restore (MTTR)	Time allowed for the system to be offline after application availability is interrupted. Mission-critical IT systems have a MTTR of two hours or fewer; non-mission-critical IT systems have a MTTR as short as five hours	QAE monthly review of system metrics



Performance Requirements	Performance Threshold	Monitoring Method
Recovery Time Objective (RTO)	The time it takes from the time of disaster to the time of service restoration and access by customers. Dependent on mission criticality	QAE monthly review of system metrics
Recovery Point Objective (RPO)	The amount of lost data that is acceptable after a disaster. Anywhere from zero to the point of the last backup of 24 hours	QAE monthly review of system metrics
User incidents	( X affected users / Y total users) * 100 = % Application Availability; Maximum % effected dependent on mission criticality	QAE monthly review of system metrics
<b>APPLICATION PERFORMANCE</b>		
Bandwidth utilization	Bandwidth utilization is kept to a minimum while not sacrificing application service performance; does not exceed X Mb, Gb	QAE monthly review of system metrics
Ports and protocols	Applications are using the port/protocol as specified by policy	QAE monthly review of system metrics
Computing requirements and resources (virtual environments)	Projected amount of computing resources and requirements is not exceeded; actual versus projected difference in computing resources (CPU, RAM, storage, etc.) acceptable	QAE monthly review of system metrics
User load/capacity	Services allow for the specified number of users required while not impacting system performance	QAE monthly review of system metrics
Data load	Job/process maximum load allowed; each job/process does not exceed X% utilization of CPU/RAM/IOP/etc	QAE monthly review of system metrics
Throughput	Amount of transactions per second permissible; applicable to service transactions or database transactions	QAE monthly review of system metrics
Response time	Average, maximum allowable response time for a user transaction; user transaction should not exceed X amount of seconds, minutes	QAE monthly review of system metrics
Degradation modes	Acceptable mode of operation when the system has been degraded in some manner	QAE monthly review of system metrics
Maximum bugs or defect rate	Expressed in terms of bugs/KLOC; categorized in terms of minor, significant, and critical; dependent on mission criticality	QAE monthly review of system metrics



Performance Requirements	Performance Threshold	Monitoring Method
Accuracy	Specify precision (resolution) and accuracy (known standard) that is required in the systems output	QAE monthly review of system metrics
<b>SYSTEM OPERATIONS &amp; MAINTENANCE</b>		
Sustainment activities	Systems are sustained without periods of prolonged degradation	QAE monthly review of system metrics
Sustainment activities	Complex software problems are isolated and resolved	QAE monthly review of system metrics
Database administration	Maintain development and test environments and databases; operating system and software upgrades, patches, and hot fixes are applied	Random sampling, 100% inspection, periodic sampling
Performance tuning and development	Margin of improvement for application services; Y=after; X=before; $(Y-X)/X$ =system improvement or degradation	QAE monthly review of system metrics
Establish individual User Accounts (including email)	# of business hours until completion from time of notification by Service Recipient; 8 hours, 80% of the time	Measure weekly and report monthly
Password Reset	# of minutes until completion from time of notification by Service Recipient; 30 minutes, 95% of the time	Measure weekly and report monthly
Delete User Accounts (including email)	# of business hours until completion from time of notification by Service Recipient; 1 day	Measure weekly and report monthly
Backup and Restore Requirements	Provider shall implement and maintain backup and restoration capabilities for all data, applications and component configurations; backup frequency – daily, weekly, monthly; retention period – dependent on mission criticality and policy	Measure weekly and report monthly
<b>SOFTWARE DESIGN, DEVELOPMENT &amp; TESTING</b>		
Software procurement analysis	Feasibility analysis, detailed analysis	100% inspection
Software design	Output may be tailored for efficiency: revised modification list, updated design baseline, updated test plans, revised detailed analysis, verified requirements, revised implementation plan, and a list of documented constraints and risks	100% inspection



Performance Requirements	Performance Threshold	Monitoring Method
Software coding design	Each modified software unit and database ('packing list'); test procedures and data for testing each software unit and database	100% inspection
Software implementation	Output may be tailored for efficiency; Updated software and design documents, Updated test documents, recommended updates to impacted portions of the training materials, test readiness review report	100% inspection
Software testing	Output may be tailored for efficiency; tested and fully integrated system, system test report, acceptance test readiness review report	100% inspection
Software acceptance support	The output of this activity may be tailored and shall be at least one of the following; new system baseline, functional configuration audit report, acceptance test report	100% inspection
Software delivery	Delivery plan (when directed), participation and documentation of installation event (mandatory)	100% inspection
<b>QUALITY ASSURANCE</b>		
Configuration management database updates and accuracy	Configuration management database updated with new systems or software with 2 duty days	QAE random checks
Configuration management database updates and accuracy	Configuration management database includes all systems and software and a 98% accuracy rate is maintained at all times	QAE random checks
IT systems inventory updates and accuracy	IT system inventories include all systems and software and a 98% accuracy rate is maintained	QAE random checks
Accuracy of software architecture drawings	More than 95% of all changes to architecture drawings updated within one week	QAE random checks
Change request rate	Change requests are increasing on a month-to-month basis	QAE random checks
Change management resolution time	The time it takes to initiate a request, address/resolve the request, and close out the request are kept to a minimum; dependent on mission criticality	QAE random checks
Configuration management	Configuration management practices are followed as prescribed by AF procedures to include version control, etc	QAE random checks



Performance Requirements	Performance Threshold	Monitoring Method
Change management	Change management practices are followed as prescribed by AF procedures	QAE random checks
Incident/Problem resolution	The number of identified problems should continue to decrease or not exceed a certain monthly threshold	QAE random checks
Software management	Between 95-98% of scheduled upgrades and/or maintenance are executed according to schedule	Event-driven and call-handling activity reports
Software management	For non-mission critical applications, between 80-90% of requests for unscheduled software maintenance are responded to within 48 hours	Event-driven and call-handling activity reports
Software management	For mission critical applications, 95-100% of requests are responded to within 2 hours	Event-driven and call-handling activity reports
Use of energy efficient equipment	95% of new electronic equipment must meet agency environmental requirements as described by Energy Star, FEMP, or EPEAT guidelines	QAE monthly review of contractor metrics
Minimize energy consumption	Meet the energy reduction goal of 3% annually through FY 2015 or a 30% reduction by the end of FY 2015	QAE monthly review of contractor metrics
Employees security clearances; control access badges; control limited access areas; maintain security of government facilities, classified data and material	Available 24/7/365 to respond within two hours to security incidents 100% of the time	QAE random checks and review of security incident information
<b>INFORMATION ASSURANCE</b>		
System security compliance	Maintain C&A compliance IAW applicable DoD and AF policy and instruction, particularly DoD Instruction 8500.2 – Information Assurance	Random sampling, 100% inspection, periodic sampling
Application security compliance	Maintain application security compliance IAW applicable DoD and AF policy and instruction, particularly the Security Technical Implementation Guide (STIG)	Random sampling, 100% inspection, periodic sampling



Performance Requirements	Performance Threshold	Monitoring Method
Use Enterprise Information Technology Data Repository (EITDR) or Enterprise Mission Assurance Support Service (eMASS) to conduct virtual evaluation of systems security	Used to conduct virtual evaluations of a programs Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information, input is required into the EITDR or eMASS system 100% of the time	Random sampling, 100% inspection, periodic sampling
<b>TRAINING</b>		
Training	Specify the required training time for normal users and power users to become productive at particular operations; dependent on mission	Random sampling, 100% inspection, periodic sampling
Training materials	Timely training materials are provided on time as required by a CDRL or contract requirement	Random sampling, 100% inspection, periodic sampling
Training materials	Quality training materials are provided to the customer that accurately reflect and correspond to processes and services	Random sampling, 100% inspection, periodic sampling
<b>HELP DESK SUPPORT</b>		
Help desk support	Provide problem resolution for assigned calls; 100% of assigned calls have a problem resolution	Random sampling, 100% inspection
Customer assistance performance	Contractor propose industry best practices for speed to answer rate, true call abandonment rate, level 1 resolution rate, and call resolution rate, etc	QAE monthly review of contractor metrics and customer feedback
Customer Satisfaction	Contractor propose industry best practices for customer satisfaction surveys	QAE random review of customer surveys
Admin Changes (Access user ID, password reset)	98% completed $\leq$ 1 business days (Changes done electronically)	QAE monthly review of contractor metrics
Average speed to answer calls	80% answered <30 sec	QAE monthly review of call handling activity reports
Help desk Agent Utilization Rate	Rate should remain between 65% - 75% (Talk time + after call work time)	Totals and averages are usually reported monthly; both numerically (tabular data) and graphically



Performance Requirements	Performance Threshold	Monitoring Method
Abandoned Call Rate	<5% of calls abandoned	Totals and averages are usually reported monthly; both numerically (tabular data) and graphically
First Call Resolution	65 % of problems resolved during initial call	Automated extraction from enterprise-class service desk toolset with focus on monthly average trending
Follow-on calls due to problem repeated after initial fix failed	10% for the first two months with a 1% reduction per month until 5% is achieved	Service Provider provided system has capability to track and report out of compliance activities
Call Center Availability	99.5% Availability	Service Provider provided system has capability to track and report out of compliance activities

## 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. 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.]***

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 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.

Sequence Number	Data Item Description	Title	Corresponding SEP Artifact
A001	DI-ADMN-81306	Program Protection Implementation Plan (PIIP)	



Sequence Number	Data Item Description	Title	Corresponding SEP Artifact
A002	DI-CMAN-80463C	Engineering Release Record (ERR)	
A003	DI-CMAN-80639C	Engineering Change Proposal (ECP)	
A004	DI-CMAN-80640C	Request for Deviation (RFD)	
A005	DI-CMAN-80642C	Notice of Revision (NOR)	
A006	DI-CMAN-80643C	Specification Change Notice (SCN)	
A007	DI-CMAN-80792A	Validation Report	
A008	DI-CMAN-80858B	Contractor's Configuration Management Plan	
A009	DI-CMAN-80874	Configuration Data Lists (CDLS)	
A010	DI-CMAN-81022C	Configuration Audit Summary Report	<a href="#">Functional Configuration Audit Checklist</a> and <a href="#">Physical Configuration Audit Checklist</a>
A011	DI-CMAN-81121	Baseline Description Document	
A012	DI-EDRS-80410	Engineering Documentation Information	
A013	DI-ILSS-80481A	Source, Maintenance and Recoverability (SMR) Code Change Request	
A014	DI-ILSS-80812	Logistic Technical Data User Profile	
A015	DI-ILSS-80813	List of Logistic Technical Data Users	
A016	DI-ILSS-80872	Training Materials	
A017	DI-ILSS-81070	Training Program Development and Management Plan	<a href="#">Project-Specific Training Template</a>
A018	DI-ILSS-81495	Failure Mode Effects, and Criticality Analysis Report	
A019	DI-IPSC-80590B	Computer Program End Item Documentation	
A020	DI-IPSC-80942	Computer Software System Document	<a href="#">Design Document Template</a>
A021	DI-IPSC-81427A	Software Development Plan (SDP)	<a href="#">Software Development Plan Template</a>
A022	DI-IPSC-81428A	Software Installation Plan (SIP)	<a href="#">Implementation Plan Template</a>
A023	DI-IPSC-81429A	Software Transition Plan (STRP)	
A024	DI-IPSC-81430A	Operational Concept Description (OCD)	<a href="#">Concept of Operations Template</a> or <a href="#">General Requirements Specification Template</a>
A025	DI-IPSC-81431A	System/Subsystem Specification (SSS)	<a href="#">System Subsystem Specification Template</a> , or <a href="#">General Requirements Specification Template</a> , <a href="#">Supplementary Specification Template</a> , and <a href="#">Use Case Specification Template</a>



Sequence Number	Data Item Description	Title	Corresponding SEP Artifact
A026	DI-IPSC-81432A	System/Subsystem Design Description (SSDD)	<a href="#">Design Document Template</a> and <a href="#">Supplementary Specification Template</a>
A027	DI-IPSC-81433A	Software Requirements Specification (SRS)	<a href="#">Software Requirements Specification Template</a> , or <a href="#">General Requirements Specification Template</a> , <a href="#">Supplementary Specification Template</a> , and <a href="#">Use Case Specification Template</a>
A028	DI-IPSC-81434A	Interface Requirements Specification (IRS)	<a href="#">Interface Requirements Agreement Template</a> , plus either the <a href="#">General Requirements Specification Template</a> , or the <a href="#">System Subsystem Specification Template</a> and the <a href="#">Software Requirements Specification Template</a>
A029	DI-IPSC-81435A	Software Design Description (SDD)	<a href="#">Design Document Template</a> and <a href="#">Supplementary Specification Template</a>
A030	DI-IPSC-81436A	Interface Design Description (IDD)	<a href="#">Design Document Template</a>
A031	DI-IPSC-81437A	Database Design Description (DBDD)	<a href="#">Database Specification Template</a>
A032	DI-IPSC-81438A	Software Test Plan (STP)	<a href="#">Integrated Test Plan Template</a>
A033	DI-IPSC-81439A	Software Test Description (STD)	<a href="#">Integrated Test Description Template</a> and <a href="#">Test Script Template</a>
A034	DI-IPSC-81440A	Software Test Report (STR)	<a href="#">Integrated Test Report Template</a>
A035	DI-IPSC-81441A	Software Product Specification (SPS)	
A036	DI-IPSC-81442A	Software Version Description (SVD)	<a href="#">Version Description Form</a>
A037	DI-IPSC-81443A	Software User Manual (SUM)	<a href="#">User Manual Template</a>
A038	DI-IPSC-81444A	Software Center Operator Manual (SCOM)	<a href="#">Operator Manual Template</a>
A039	DI-IPSC-81445A	Software Input / Output Manual (SIOM)	<a href="#">User Manual Template</a>
A040	DI-IPSC-81488	Computer Software Product	
A041	DI-IPSC-81633	Software Programmer's Guide	
A042	DI-IPSC-81756	Software Documentation	
A043	DI-MCCR-80459	Software Developmental Status Report (SDSR)	
A044	DI-MCCR-80491A	Computer Software Flowchart	
A045	DI-MCCR-80700	Computer Software Product End Items	
A046	DI-MCCR-80902	Software Development Summary Report	
A047	DI-MCCR-81344	Design Specification	<a href="#">Design Document Template</a> and <a href="#">Supplementary Specification Template</a>



Sequence Number	Data Item Description	Title	Corresponding SEP Artifact
A048	DI-MGMT-80227	Contractor's Progress, Status and Management Report	
A049	DI-MGMT-80269	Status of Government Furnished Equipment (GFE) Report	
A050	DI-MGMT-80277	Government Furnished Inspection Equipment Maintenance Report	
A051	DI-MGMT-80368A	Status Report	
A052	DI-MGMT-80389B	Receipt of Government Material Report	
A053	DI-MGMT-80408B	Request for Government Furnished Materiel	
A054	DI-MGMT-80469A	System Assessment Report (SAR)	
A055	DI-MGMT-80501	Contractor's Corrective Action Plan	
A056	DI-MGMT-80507C	Project Planning Chart	
A057	DI-MGMT-80555A	Program Progress Report	
A058	DI-MGMT-80920	List of Items Delivered During the Term of a Contract	
A059	DI-MGMT-81466A	Contract Performance Report (CPR)	
A060	DI-MGMT-81580	Contractor's Standard Operating Procedures	
A061	DI-MGMT-81642	Small Business Subcontractor Report	
A062	DI-MGMT-81739B	Software Resources Data Reporting: Initial Developer Report and Data Dictionary	
A063	DI-MGMT-81740A	Software Resources Data Reporting: Final Developer Report and Data Dictionary	
A064	DI-MGMT-81797	Program Management Plan	
A065	DI-MGMT-81808	Contractor's Risk Management Plan	
A066	DI-MGMT-81809	Risk Management Status Report	
A067	DI-MGMT-81834	Contractor's Personnel Roster	
A068	DI-MGMT-81842	Vulnerability Scan Compliance (VSC) Report	
A069	DI-MGMT-81843	Information Assurance (IA) Test Report	<a href="#">Integrated Test Report Template</a>
A070	DI-MGMT-81844	Information Assurance (IA) Test Plan	<a href="#">Integrated Test Plan Template</a>
A071	DI-MGMT-81845	Information Assurance (IA) Design Review Information Package (DRIP)	
A072	DI-MISC-80392	Operating Instructions	
A073	DI-MISC-80564	Vulnerability Analysis Report	
A074	DI-MISC-81418	Operating Procedures Manual	
A075	DI-MISC-81627	System Deficiency Report (SDR) Data	
A076	DI-MISC-81807	Software/Firmware Change Request	



Sequence Number	Data Item Description	Title	Corresponding SEP Artifact
A077	DI-NUOR-81412	Software Certification Plan (SCP)	
A078	DI-QCIC-80736	Quality Deficiency Report	
A079	DI-QCIC-81187	Quality Assessment Report	
A080	DI-QCIC-81200	Quality Inspection Test, Demonstration, and Evaluation Report	
A081	DI-QCIC-81379	Quality System Plan	
A082	DI-QCIC-81794	Quality Assurance Program Plan	
A083	DI-QCIC-81795	Software Quality Assurance Report	
A084	DI-RELI-80254	Corrective Action Plan	
A085	DI-RELI-80255	Failure Summary and Analysis Report	
A086	DI-RELI-80807	Failure Data and Traceability Record	
A087	DI-SESS-81001D	Conceptual Design Drawings/Models	
A088	DI-SESS-81002E	Developmental Design Drawings/Models and Associated Lists	
A089	DI-SESS-81785	Systems Engineering Management Plan (SEMP)	
A090	DI-TMSS-80007	Test Program Manual	
A091	DI-TMSS-80527C	Commercial Off-The-Shelf (COTS) Manuals and Associated Supplemental Data	
A092	DI-TMSS-81815	Commercial Off-The-Shelf (COTS) Manuals	
A093	DI-TMSS-81816	Commercial Off-The-Shelf (COTS) Manual Supplemental Data	
A094	DI-TMSS-81817	Technical Manual Quality Assurance (TMQA) Program Plan	
A095	DI-TMSS-81818	Technical Manual Validation Plan	
A096	DI-TMSS-81819A	Technical Manual Validation Certificate	
A097	DI-TMSS-81820	Technical Manual Verification Discrepancy/Disposition Record	
A098	DI-TMSS-81821	Technical Manual Verification Incorporation Certificate	

## 8. APPLICABLE STANDARDS AND REFERENCES

*[Tailor the list as needed for individual Task Orders requirements. 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.]*



Documentation	URL	Description
<b>ENTERPRISE STRATEGY</b>		
DoD CIO Net-Centric Data Strategy	<a href="http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf">http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf</a>	<p>This document describes the Net-Centric Data Strategy for the Department of Defense (DoD), including DoD intelligence agencies and functions. It describes a vision for a net-centric environment and the data goals for achieving that vision. It defines approaches and actions that DoD personnel will have to take as users—whether in a role as consumers and producers of data or as system and application developers.</p>
DoD CIO Net-Centric Services Strategy	<a href="http://cio-nii.defense.gov/docs/Services_Strategy.pdf">http://cio-nii.defense.gov/docs/Services_Strategy.pdf</a>	<p>The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.</p>
DODD 8320.02, Data Sharing in a Net-Centric Department of Defense	<a href="http://www.dtic.mil/whs/directive/s/corres/pdf/832002p.pdf">http://www.dtic.mil/whs/directive/s/corres/pdf/832002p.pdf</a>	<p>Establishes policies and responsibilities to implement data sharing, in accordance with DoD Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002.</p>
DoD Discovery Metadata Specification (DDMS)	<a href="http://metadata.dod.mil/mdr/irs/DDMS/">http://metadata.dod.mil/mdr/irs/DDMS/</a>	<p>Visibility, accessibility, and understandability are the high priority goals of the DoD Net-Centric Data Strategy. Of these goals, visibility and discovery are intimately linked. Visibility of a resource is, in a practical sense, useless, if the resource is not easily discoverable. With the express purpose of supporting the visibility goal of the DoD Net-Centric Data Strategy, the DDMS specifies a set of information fields that are to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services.</p>
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	<a href="http://www.dtic.mil/cics_directive/s/cdata/unlimit/6211_02.pdf">http://www.dtic.mil/cics_directive/s/cdata/unlimit/6211_02.pdf</a>	<p>This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain).</p>
CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems	<a href="http://www.dtic.mil/cics_directive/s/cdata/unlimit/6212_01.pdf">http://www.dtic.mil/cics_directive/s/cdata/unlimit/6212_01.pdf</a>	<p>Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&amp;S) needs. Establishes procedures to perform I&amp;S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs and systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment.</p>



Documentation	URL	Description
DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	<a href="http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf</a>	Implements a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability throughout the Department of Defense (DoD). This approach incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership and education, personnel, and facilities) aspects to ensure life-cycle interoperability and supportability of IT and NSS throughout the DoD. Implements the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability.
Netcentric Enterprise Solutions for Interoperability (NESI)	<a href="http://nesipublic.spawar.navy.mil/">http://nesipublic.spawar.navy.mil/</a>	NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application.
<b>ENTERPRISE ARCHITECTURE</b>		
DoDD 8100.1, Global Information Grid (GIG) Overarching Policy	<a href="http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf">http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf</a>	Establishes policy and assigns responsibilities for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.
DoD Global Information Grid Architectural Vision	<a href="http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&amp;Location=U2&amp;doc=GetTRDoc">http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&amp;Location=U2&amp;doc=GetTRDoc</a>	The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information – the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.
Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	<a href="http://cio-nii.defense.gov/sites/dodaf20/index.html">http://cio-nii.defense.gov/sites/dodaf20/index.html</a>	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCA), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.



Documentation	URL	Description
Air Force Policy Directive (AFPD) 33-4, Information Technology Governance	<a href="#">IN DRAFT – SUPERSEDES 33-4, JUNE 2006</a>	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.
AFI33-401, Implementing Air Force Architectures	<a href="http://www.af.mil/shared/media/epubs/AFI33-401.pdf">http://www.af.mil/shared/media/epubs/AFI33-401.pdf</a>	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.
<b>SYSTEMS ENGINEERING</b>		
Air Force Program Executive Office (AFPEO) Business Enterprise Systems (BES) Systems Engineering Process	<a href="https://org.eis.afmc.af.mil/sites/754elsg/ES/HIJG/SEP/default.aspx">https://org.eis.afmc.af.mil/sites/754elsg/ES/HIJG/SEP/default.aspx</a>	The Systems Engineering Process is a life cycle management and systems engineering process based on the Defense Acquisition, Technology, and Logistics Life Cycle Management System as tailored for Information Technology Systems and the Capability Maturity Model Integrated. It provides common plans, procedures, checklists, forms, and templates that support system life cycle management and systems engineering processes.
AFI 10-601, Capabilities-Based Requirements Development	<a href="http://www.e-publishing.af.mil/shared/media/epubs/afi10-601.pdf">http://www.e-publishing.af.mil/shared/media/epubs/afi10-601.pdf</a>	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.
AFI 63-101, Acquisition and Sustainment Life Cycle Management	<a href="http://www.af.mil/shared/media/epubs/AFI63-101.pdf">http://www.af.mil/shared/media/epubs/AFI63-101.pdf</a>	The purpose of this instruction is to implement direction from the Secretary of the Air Force as outlined in Air Force Policy Directive (AFPD) 63-1/20-1, Acquisition and Sustainment Life Cycle Management. The primary mission of the Integrated Life Cycle Management (ILCM) Enterprise is to provide seamless governance, transparency and integration of all aspects of weapons systems acquisition and sustainment management.
AFI 63-1201, Life Cycle Systems Engineering	<a href="http://www.e-publishing.af.mil/shared/media/epubs/afi63-1201.pdf">http://www.e-publishing.af.mil/shared/media/epubs/afi63-1201.pdf</a>	It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost-effective products and systems that are operationally safe, suitable, and effective.



Documentation	URL	Description
AFI 99-103, Capabilities-Based Test and Evaluation	<a href="http://www.e-publishing.af.mil/shared/media/epubs/AFI99-103.pdf">http://www.e-publishing.af.mil/shared/media/epubs/AFI99-103.pdf</a>	<p>It describes the planning, conduct, and reporting of cost effective test and evaluation (T&amp;E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&amp;E are to mature system designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&amp;E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.</p>
DoD Open Technology Development Guidebook	<a href="http://www.acq.osd.mil/ictd/articles/OTDRoadmapFinal.pdf">http://www.acq.osd.mil/ictd/articles/OTDRoadmapFinal.pdf</a>	<p>This roadmap outlines a plan to implement Open Technology Development practices, policies and procedures within the DoD.</p>
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	<a href="http://www.sei.cmu.edu/library/assets/soabest.pdf">http://www.sei.cmu.edu/library/assets/soabest.pdf</a>	<p>This document was developed under the Net-Centric Operations Industry Forum charter to provide industry advisory services to the Department of Defense (DoD), Chief Information Officer (CIO). It presents a list of industry best practices in achieving Service Oriented Architecture (SOA).</p>
Readiness Improvement through Systems Engineering (RISE) Handbook	<p>[NO PUBLIC LINK AVAILABLE]</p> <p><a href="#">Contact AFLCMC Office for copy.</a></p>	<p>The RISE Handbook is a reference and guide to be used by engineers and the program management to address RAM on 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 &amp; Manufacturing Development Phase, and Production &amp; 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.</p>
Community of Interest (COI) Engagement Process Plan	<a href="http://www.jpdo.gov/library/20120202_COI_Engagement_Plan_FINAL.pdf">http://www.jpdo.gov/library/20120202_COI_Engagement_Plan_FINAL.pdf</a>	<p>This document describes the approach used by the Joint Planning and Development Office (JPDO) Net-Centric Operations Division (NCOD) in sponsoring the development of ontologies and encouraging ontology implementation in support of Net-Centric information exchanges. This approach uses small, agile development teams, called Community of Interest<sup>1</sup> (COI) Engagement Teams, to create an inter-organizational environment that is efficient, sustainable, and extensible. This document outlines a typical NCOD engagement with a COI or Working Group (WG) and defines a set of products that result from a typical engagement.</p>
Federal Desktop Core Configuration (FDCC)	<a href="http://nvd.nist.gov/fdcc/index.cfm">http://nvd.nist.gov/fdcc/index.cfm</a>	<p>The United States Government Configuration Baseline (USGCB) is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate.</p>
<b>INFORMATION ASSURANCE</b>		



Documentation	URL	Description
ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	<a href="http://www.dni.gov/electronic_reading_room/ICD_503.pdf">http://www.dni.gov/electronic_reading_room/ICD_503.pdf</a>	This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.
DoDD 8500.01E Information Assurance (IA)	<a href="http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf</a>	Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) Information Assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
DoDI 8500.2, Information Assurance (IA) Implementation	<a href="http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf</a>	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.01E, "Information Assurance."
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management	<a href="http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf</a>	Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.
DoD 8570.01-M, Information Assurance Workforce Improvement Program	<a href="http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf">http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf</a>	Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual.
DoDI 8510.01, Information Assurance Certification and Accreditation Process (DIACAP)	<a href="http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf</a>	Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.
AFI 33-200, Information Assurance	<a href="http://www.e-publishing.af.mil/shared/media/epubs/AFI33-200.pdf">http://www.e-publishing.af.mil/shared/media/epubs/AFI33-200.pdf</a>	This AFI provides general direction for implementation of IA and management of IA programs according to AFD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process.
AFI 33-210, AF Certification and Accreditation Program (AFCAP)	<a href="http://www.e-publishing.af.mil/shared/media/epubs/AFI33-210.pdf">http://www.e-publishing.af.mil/shared/media/epubs/AFI33-210.pdf</a>	This AFI implements DIACAP for authorizing the operation of Air Force ISs consistent with federal, DoD, and Air Force policies. It is used to ensure IA for all Air Force procured Information Systems, and Guest systems operating on or accessed from the AF-GIG.
Security Technical Implementation Guides (STIGs)	<a href="http://iase.disa.mil/stigs/stig/index.html">http://iase.disa.mil/stigs/stig/index.html</a>	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	<a href="http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf</a>	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.



Documentation	URL	Description
Public Law 111-383	<a href="http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf">http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf</a>	An Act to authorize appropriations for fiscal year 2011 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.
<b>INFORMATION TECHNOLOGY STANDARDS</b>		
Federal Information Processing Standards (FIPS)	<a href="http://www.itl.nist.gov/fipspubs/">http://www.itl.nist.gov/fipspubs/</a>	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
Info-structure Technology Reference Model (i-TRM)	<a href="https://cs.eis.af.mil/a6/itrm/default.aspx">https://cs.eis.af.mil/a6/itrm/default.aspx</a>	i-TRM is the Air Force’s authoritative source for Communications and Information (C&I) products, computer configurations, platform and service profiles, technical solutions, and standards (presented as standards profiles).
National Institute for Standards and Technology (NIST)	<a href="http://www.nist.gov/information-technology-portal.cfm">http://www.nist.gov/information-technology-portal.cfm</a>	Advancing the state-of-the-art in IT in such applications as cyber security and biometrics, the National Institute of Standards and Technology accelerates the development and deployment of systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.
International Standards Organization (ISO)	<a href="http://www.iso.org/iso/home.html">http://www.iso.org/iso/home.html</a>	ISO is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 162 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.
American National Standards Institute (ANSI)	<a href="http://www.ansi.org/">http://www.ansi.org/</a>	The Institute oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector. ANSI is actively engaged in accrediting programs that assess conformance to standards – including globally-recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.
International Committee for Information Technology Standards	<a href="http://www.incits.org/">http://www.incits.org/</a>	INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1. JTC 1 is responsible for International standardization in the field of Information Technology.



Documentation	URL	Description
Institute of Electrical and Electronics Engineers (IEEE)	<a href="http://www.ieee.org/">http://www.ieee.org/</a>	IEEE is the world’s largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE’s highly cited publications, conferences, technology standards, and professional and educational activities.
National Security Agency/The Common Criteria Evaluation/NIST and Validation Scheme	<a href="http://www.niap-ccevs.org/">http://www.niap-ccevs.org/</a>	The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors. This program is being implemented to help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.
<b>QUALITY ASSURANCE</b>		
AFPD 33-3, Information Management	<a href="http://www.e-publishing.af.mil/shared/media/epubs/AFPD33-3.pdf">http://www.e-publishing.af.mil/shared/media/epubs/AFPD33-3.pdf</a>	This policy directive establishes Air Force policy for the management of information assets (all forms of data and content), across all AF information sources, as both a strategic resource and corporate asset supporting the warfighter during mission and support operations.
AFMAN 33-363, Management of Records	<a href="http://www.e-publishing.af.mil/shared/media/epubs/AFMAN33-363.pdf">http://www.e-publishing.af.mil/shared/media/epubs/AFMAN33-363.pdf</a>	This manual implements DoDD 5015.2, <i>DoD Records Management Program</i> , and Air Force Policy Directive (AFPD) 33-3, <i>Information Management</i> . It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.
AFI 33-364, Records Disposition – Procedures and Responsibilities	<a href="http://www.e-publishing.af.mil/shared/media/epubs/AFI33-364.pdf">http://www.e-publishing.af.mil/shared/media/epubs/AFI33-364.pdf</a>	This instruction implements Air Force Policy Directive (AFPD) 33-3, <i>Information Management</i> , by listing program objectives and responsibilities, guiding personnel in disposing of special types of records, retiring or transferring records using staging areas, and retrieving information from inactive records.
T.O. 00-33A-1001, General Communications Activities Management Procedures and Practice Requirements	No link available	The control of production within an organization is accomplished at various levels to varying degrees. Control of production includes planning and scheduling production, ordering and managing materials, and maintaining Automated Information Systems (AIS). The fundamental concepts, responsibilities, and procedures are detailed in the following paragraphs.
DoDD 5230.24, Distribution Statements on Technical Documents	<a href="http://www.dtic.mil/whs/directive/s/corres/pdf/523024p.pdf">http://www.dtic.mil/whs/directive/s/corres/pdf/523024p.pdf</a>	This Directive updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
AFI 61-204, Disseminating Scientific and Technical Information	<a href="http://www.e-publishing.af.mil/shared/media/epubs/afi61-204.pdf">http://www.e-publishing.af.mil/shared/media/epubs/afi61-204.pdf</a>	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.



Documentation	URL	Description
AFI 33-114, Software Management	<a href="http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA404975">http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA404975</a>	It identifies responsibilities for management of commercial off-the-shelf (COTS) and Air Force-unique software acquired by the Air Force. It includes policy and management structure for establishing and managing Air Force COTS software licenses and ensuring compliance with The Copyright Act and E.O. 13103.
DoDD 5205.02, Operations Security (OPSEC) Program	<a href="http://www.fas.org/irp/doddir/dod/d5205_02.pdf">http://www.fas.org/irp/doddir/dod/d5205_02.pdf</a>	Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations.
AFI 10-701, Operations Security (OPSEC)	<a href="http://www.fas.org/irp/doddir/usaf/afi10-701.pdf">http://www.fas.org/irp/doddir/usaf/afi10-701.pdf</a>	This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.
Air Force Anthrax Vaccine Immunization Program (AVIP)	<a href="http://www.vaccines.mil/documents/1012AirForceImplementation.pdf">http://www.vaccines.mil/documents/1012AirForceImplementation.pdf</a>	
DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	<a href="http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf">http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf</a>	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).
DoD 5220.22-M, National Industrial Security Program Operating Manual	<a href="http://www.dss.mil/documents/00aa/nispom2006-5220.pdf">http://www.dss.mil/documents/00aa/nispom2006-5220.pdf</a>	This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
DoDI 2000.16, Antiterrorism Standards	<a href="http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf">http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf</a>	Updates policy implementation, responsibilities, and the antiterrorism (AT) standards. This update reorganizes AT standards according to the minimum required elements for an AT program: risk management, planning, training and exercises, resource application, and comprehensive program review.
DoD 5400.7-R, Freedom of Information Act Program	<a href="http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf">http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf</a>	This Regulation provides policies and procedures for the DoD implementation of the Freedom of Information Act (5 U.S.C. 552, as amended) and DoD Directive 5400.7, and promotes uniformity in the DoD Freedom of Information Act (FOIA) Program.



Documentation	URL	Description
Section 508 of the Rehabilitation Act of 1973	<a href="http://www.access-board.gov/sec508/guide/act.htm">http://www.access-board.gov/sec508/guide/act.htm</a>	<p>On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.</p>
DoDI 3020.37, Continuation of Essential DoD Contractor Services During Crises	<a href="http://www.afsc.army.mil/gc/files/i302037.pdf">http://www.afsc.army.mil/gc/files/i302037.pdf</a>	<p>This Instruction implements DoD policy, assigns responsibilities, and prescribes procedures, in accordance with references (a) and (b), to provide reasonable assurance of the continuation of essential services provided by DoD contractors, including services provided to Foreign Military Sales (FMS) customers, during crisis situations.</p>

## 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://jitc.fhu.disa.mil/apl/ipv6/pdf/dsr\\_ipv6\\_50.pdf](http://jitc.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)<sup>11</sup> 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](http://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](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.