Application Services Task Order PWS Template

(NOTE: This is the broad based USAF Application Services Template. If you are in PEO BES and need the AF PEO BES System Sustainment template, please download it from the NETCENTS-2 website under Application Services Documents Templates. http://www.netcents.af.mil/contracts/netcents-2/appsrvs/documents/index.asp)

INSTRUCTIONS:

1. **You may use this format for your Application Services Performance Work Statement. Using a standard template helps offerors know where to look for requirements and can decrease the time required to solicit proposals for the Task Orders.**

2. **Save a copy of this template and modify it according to your requirements. Each time a PWS is accomplished, come back to the User's Guide and download the PWS template. The language, standards and references will be updated over time.**

3. **All bold italic text within brackets [ ] is instructional information specific to the section.**

4. **Text not within brackets is information that you are HIGHLY ENCOURAGED to keep in your PWS; only apply modifications, introduce additional information, or include updates in the event that standards or instructions change, or when deemed necessary by your specific program's or organization's policies.**

5. **All citations to policies, directives, instructions and reference material are included in Appendix A3, *Application Services Standards & References*.**

6. **Before submitting your completed PWS, REMEMBER TO DELETE all instructional text contained within brackets. It is shown here for instructional purposes only and must not remain in the final document.**

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

Name:	
Organization:	
Address:	***[physical mailing address]***

Executive Summary

[*Provide a <u>short</u> description of the work to be performed.*]

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

1. PURPOSE

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

2. SCOPE

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

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

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

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

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

Factor	**Data**
	Number of online screens. 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.). 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.
Stability	Provide the Mean Time to Repair on the legacy code. 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. The average (in FP or SLOC) number of modifications/improvements per period (quarterly, annually, etc.) per Baseline Change Request.
Number of concurrent users	
Application age	
Function Points Inputs External Inputs	
External Outputs	
Logical Internal Files	
External Interfaces	
External Inquiries	
Initial response time	Provide the current average response time for online applications and/or web services. Provide the expected/desired response time for online applications and/or web services. If there are throughput requirements on

Factor	Data
	batch/background updates or reports, provide the current average and the desired goal/objective.
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.
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 interface (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.

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

3.1 Systems Sustainment

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

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

- Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases and interfaces in compliance with applicable AF/DoD standards.

- Support system sustainment activities to include maintaining existing legacy systems and environments and to sustain applications, databases and interfaces.

- Provide application services to support, maintain and operate systems or services.

[NOTE: Remove entire section if not applicable or modify to meet your requirements.]

3.2 Systems Development, Migration and Integration

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

- Conduct software development, software security, web services development, web services testing, smart phone or other IT device applications and testing, security layer integration, database clean-up, data wrapping and data conversion.

- Develop, operate and maintain prototype applications, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. Develop schedules and implementation plans, including parallel operations, identification of technical approaches and a description of anticipated prototype results.

- Perform system performance tuning, system re-hosting and integration services.

- Migrate legacy systems to an Enterprise Resource Planning (ERP) system or an existing standard infrastructure such as the Global Combat Support System (GCSS) or DoD Enterprise Computing Center (DECC);

- Utilize Government-Off-The-Shelf (GOTS) or approved Commercial-Off-The-Shelf (COTS) tools for systems design and development.

- Ensure all mobile applications being developed receive their DIACAP (IA Certification) and they must be developed to be device agnostic. Ensure compliance with the DoD Mobile Development Strategy V2.0 dated May 2012.

- If applicable, ensure compliance with the USAF Implementation Baseline (IB). The IB is applicable to IT programs, new systems/applications, major increments and/or applications migrating to new infrastructure environments as identified in the baseline documentation.

  (For the latest Implementation Baseline version: IB version 2.1 documents are available on the RESTRICTED DTIC site (http://www.dtic.mil). Because the documents are marked 'Distribution D', it precludes them being made available on the public DTIC site. Once a publicly releasable version is accomplished, it will be available on the NETCENTS-2 web site. Anyone needing the IB documents must first register for an account on DTIC. Once account registration is completed and approved, the user must select the "DTIC Online Access Control (DOAC)" link on the right side of the DTIC homepage and then click, "Connect Now." Keep in mind that the public DTIC site is BLUE and the restricted side is GREEN. Searching "Technical Reports" using the title, 'Implementation Baseline V2.1', seems to be the most efficient method for returning the documents. There are 6 IB V2.1 documents in total; the main IB with 5 addenda (ERP, DEAMS Migration, .NET for STAX, ELS Use Cases, Enterprise Claims Service). For some reason, the documents are not all returned together; the user needs to scroll through the first 1 to 12 hits to locate all 6.

  [NOTE: Remove entire section if not applicable or modify to meet your requirements.]

3.3. Information Services

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

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

3.3.1 Development of New SOA Applications and Data Services

- Expose authoritative data, as defined, by re-engineering a business process, identifying the sources for the authoritative data and establishing user roles and permissions for information access as directed by COI.

- Support life-cycle management of new SOA-based applications that encapsulate business logic to provide new functional/operational mission capabilities.

[NOTE: Remove entire section if not applicable.]

3.3.2 Create Aggregation Services

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

[NOTE: Remove entire section if not applicable.]

3.3.3 Create Presentation Services

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

[NOTE: Remove entire section if not applicable.]

3.3.4 Specify Information Assets for Exposure

- Generate specification for exposing authoritative data as information asset payloads.
- Create semi-automated services that enable the specification of information assets by editing, sorting, filtering and translating.
- Utilize applicable data definitions and standards for information assets to be exposed
- Create schema/documentation for organizations to register for use throughout the DoD enterprise.

[NOTE: Remove entire section if not applicable.]

3.3.5 Registering Services

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

[NOTE: Remove entire section if not applicable.]

3.3.6 Web Services

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

[NOTE: Remove entire section if not applicable.]

3.3.7 Service Lifecycle Management

Generate necessary design and implementation artifacts that will support life-cycle management, defined as service development, testing, certification, registration, sustainment and evolution aligned with defined requirements. These artifacts will include the metadata needed for service life-cycle management IAW the current version of the DoD Discovery Metadata Specification (DDMS). The design and implementation artifacts for Top Secret network systems and applications, as well as ISR mission systems, are owned by the Government and provided to the Government representative prior to the end of the task order at no additional cost to the Government unless otherwise stated in the task order.

[NOTE: Remove entire section if not applicable.]

3.3.8 Vocabulary Management

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

[NOTE: Remove entire section if not applicable.]

3.3.9 Register Vocabularies

Support the alignment, articulation and registration of vocabulary artifacts.

[NOTE: Remove entire section if not applicable.]

3.3.10 Data Stores

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

[NOTE: Remove entire section if not applicable.]

3.3.11 Information Exposure Services

- Provide application services.
- Prepare and standardize data retrieved from legacy information sources
- Modify the information source’s interface, data and/or behavior for standardized accessibility.
- Transform communication interfaces, data structures and program semantic alignment.
    - Provide standardized communication/program wrapping services, data language translation, etc.

- Employ configuration management plan of existing legacy baseline code and data exposure code.

[NOTE: Remove entire section if not applicable.]

3.4 Systems Operations

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

The contractor shall provide operational support services including, but not limited to, database administration, systems administration, customer training and help desk support of both legacy and new applications and systems in accordance with AFI 33-115 Network Operations and DoD 8570.01M Information Assurance Workforce Improvement Program.

3.4.1 Database Administration

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

[NOTE: Remove entire section if not applicable.]

3.4.2 Systems Administration

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

[NOTE: Remove entire section if not applicable.]

3.4.3 Customer Training

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

[NOTE: Remove entire section if not applicable.]

3.4.4 Help Desk Support

Provide Help Desk Tier 1, Tier 2 and/or Tier 3 support for technical assistance, order processing, support of multiple software versions, training, warrant, and maintenance, 24-hours a day, 7-days a week, 365 days a year.

- Tier 1 – Basic application software and/or hardware support.

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

[NOTE: Remove entire section if not applicable.]

3.5 Agent of the Certifying Authority (ACA) Support Services

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

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

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

[NOTE: Remove entire section if not applicable.]

3.6 [Next Requirement]

4. ENGINEERING REQUIREMENTS

4.1 Systems Engineering

[If applicable, insert additional MAJCOM or organization Business and Enterprise Systems (BES) Process Directory policy, requirements or guidelines. Include any special 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

[Keep this section unless organizational specific language is inserted.]

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 Business and Enterprise Systems (BES) Process Directory

If applicable, the contractor shall follow and refer to the Air Force Program Executive Office (AFPEO) Business Enterprise Systems (BES) Process Directory website https://acc.dau.mil/bes 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.

4.2 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 http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf.

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

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

4.2.3 Capabilities Integration Environment (CIE)

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

4.2.4 DoD Mobility Strategy

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

4.2.5 Federal Desktop Core Configuration (FDCC)

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

4.3 Configuration Management

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

4.4 Testing

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

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

4.4.1 Test Lab

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

4.4.2 Regression Testing

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

4.4.3 Product/System Integration Testing

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

4.4.4 Simulated Operational Testing

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

4.4.5 Acceptance Testing

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

4.4.6 System Performance Testing

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

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

4.5 Information Assurance

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

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

4.5.1 System IA

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

4.5.2 Application IA

For those solutions that will be deployed to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inherit existing network security controls, application security assurance is required at the Application layer of the TCP/IP DoD Model. The contractor shall ensure that all application deliverables adhere to Public Law 111-383, which states the general need for software assurance. Specifically, the contractor shall ensure that all application deliverables comply with the Defense Information Systems Agency (DISA) Application Security & Development Security Technical Implementation Guide (STIG), which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.5.3 Personnel IA

Personnel performing Information Assurance (IA) activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005 (with all current changes).

5. CONTRACTUAL REQUIREMENTS

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

5.1 Contractors Use of NETCENTS-2 Products Contract

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

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

5.4 Government Furnished Property

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

need to provide to contractor personnel for project performance. Sample language is provided below.]

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

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

Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the Task Order will be provided to the contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the responsible Government QAP upon request or at the end of the Task Order period of performance.

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

5.5 Billable Hours

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

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

5.6 Non-Personal Services

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

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

5.7 Contractor Identification

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

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

5.8 Performance Reporting

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

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

5.9 Program Management/Project Management

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

5.9.1 Services Delivery Summary

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

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

5.9.2 Task Order Management

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

5.9.3 Documentation and Data Management

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

5.9.4 Records, Files, and Documents

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

5.9.5 Personnel Security

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

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

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

5.9.5.1 Transmission of Classified Material

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

5.9.5.2 Protection of System Data

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

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

5.9.5.3 System and Network Authorization Access Requests

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

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

5.9.6 Travel

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

If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use 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:

- The contractor employees' participation is on a space-available basis,
- The contractor employees' participation does not negatively impact performance of this task order,
- The Government incurs no additional cost in providing the training due to the contractor employees' participation, and
- Man-hours spent due to the contractor employees' participation in such training are not invoiced to the task order.

5.11 Data Rights and Non-Commercial Computer Software

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

5.12 Software Support and Data Rights

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

5.13 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.

5.14 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.

5.15 Software License Management

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

5.16 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.

5.17 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.

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

The performance of these services may be considered mission-essential functions during time of crisis. Should a crisis be declared by the Secretary of Defense, the CO or representative will verbally advise the contractor of the revised requirements, followed by written direction. When a crisis is declared, all services identified in this PWS are considered mission-essential functions during a crisis. The contractor shall continue providing service to the requesting organization 24-hours a day until the crisis is over. The contractor shall ensure enough skilled personnel are available during a crisis for any operational emergency. A crisis management plan shall be submitted IAW A-TE-3, A04, which states that the contractor shall "Submit an essential personnel list within 10 days after the contract start date." The list shall contain the employee's name, address, home phone number, beeper number (or cell phone number), social security number, security clearance and duty title. This list shall be updated annually or as changes occur. It must include the language spelled out in DFARS 237.76 – Continuation of Essential Contractor Services to identify services determined mission-essential functions during a crisis situation IAW DODI 3020.37. **Note: It is the responsibility of the Combatant Commander to determine mission-essential functions and to establish procedures to ensure that these standard support requirements and any additional requirements are met.**

5.19 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."

5.20 Incentives

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

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

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

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

6. SERVICES DELIVERY SUMMARY

[Modify to fit task order requirements. Make sure the services required have measurable outcomes. Refer to Appendix A1, "**Application Services Sample Performance Parameters*****," for sample performance parameters.]***

7. SECURITY REQUIREMENTS

[NOTE: Contact your local Security Office to determine which requirements may not be applicable to your task order, or which additional security requirements may need to be included. For the sake of readability of your PWS, it may be preferable to move this language to a separate document and include that document as an attachment to your RFP. It is recommended to include this language, as modified to meet Task Order requirements, in that attachment if your unit prefers to remove this section from the PWS itself.]

7.1 Security Facility Clearance Requirements

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

The contractor must possess or obtain an appropriate facility security clearance as identified below prior to performing work on a classified government contract: **(SELECT ONE)**

(   )   Top Secret

(   )   Secret

If the contractor does not possess a facility clearance the government will request one. The contractor shall notify the 42d Security Forces Squadron, Plans and Programs Flight, Information Protection (42 SFS/S5X/IP) before on-base performance of the service. The notification shall include:

- Name, address and telephone number of company representatives.
- The contract number and contracting agency.
- The highest level of classified information which contractor employees require access to.
- The location(s) of service performance and future performance, if known.

- The date service performance begins.
- Any change to information previously provided under this paragraph.

*** See Section 7.4 on how to complete this action***

7.2 Personnel Security Clearance Requirements

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

Some or all of the personnel performing work on this contract will require a security clearance as identified below: **(SELECT ONE)**

(   )   Top Secret

(   )   Secret

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

7.2.1 Additional Investigation Requirements

Anyone working on the contract that does not require a security clearance must have at a minimum a favorably adjudicated National Agency Check with Written Inquiries (NACI) investigation to access a government furnished information system or environment. This investigation must be submitted by the contract company.   Note: AFI 31-501, and AFI 31-601 for unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/or sensitive equipment.

7.3 Security Manager Appointment

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

The contractor shall appoint a security manager for the on base long-term visitor group. The security manager may be a full-time position or an additional duty position. The security manager shall provide contractor employees with training required by DoDM 5200.01, Volume 3, Enclosure 5, *DoD Information Security Program*, AFPD 31-4, *Information Security* and AFI 31-401, *Information Security Program Management*. The contractor security manager shall provide initial and follow-on training to contractor personnel who work in Air Force controlled or restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101, *Air Force Integrated Defense Plan*.

7.4 Visit Requests

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

7.5 Obtaining and Retrieving Identification Media

As prescribed by the AFFAR 5352.242-9000 Contractor Access to Air Force Installations, AFFAR 5352.242-9001, Common Access Cards (CAC) for Contractor Personnel and FAR 52.204-9, Personal Identity Verification of Contractor Personnel, the contractor must comply with the requirements set forth in these guidance. Contractors requesting a CAC for personnel on the contract will submit on company letterhead the names and all other personnel information as prescribed by the contracting officer to begin the identification processing effort. Contracting officers will follow installation specific guidance regarding the issuance and recovery of all identification media issued to the contractors by the government. Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

7.6 Pass and Identification Items

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

NOTE: Contact your local Security Office to determine the appropriate identification for this task order.]

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

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

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

7.7 Visitor Group Security Agreement (VGSA)

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

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

- Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, *Industrial Security Regulation,* Air Force Policy Directive 31-6, *Industrial Security,* Air Force Instruction 31-601, *Industrial Security Program Management,* DoDM 5200.01, Volumes 1-4, *DoD Information Security Program,* and AFI 31-401, *Information Security Program Management.*

- Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.
- On base, the long-term visitor group security agreement may take the place of a *Standard Practice Procedure* (SPP).

7.8 Information Security

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

7.9 Unescorted Entry to Secure Rooms

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

Contractor personnel requiring unescorted entry to secure rooms designated by the installation commander shall comply with base access requirements and these additional security instructions; DoD 5200.2-R, *DoD Personnel Security Program,* AFI 31-101, *Air Force Integrated Defense Plan* and AFI 31-501, *Personnel Security Program Management* as applicable. Contractor personnel shall be the subject of a favorably adjudicated National Agency Check with Local Agency Check (NACLC) investigation to qualify for unescorted entry to a secure room. Contractor personnel must contact their Contracting Officer Representative (COR) and the appropriate secure room monitor for permission.

7.10 Computer and Network Access Requirements

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

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

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

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

( ) **AIS-III Position - Nonsensitive Positions.** No security clearance required but is a **Trusted Position** based on a favorable NACI background investigation. All other positions involved in U.S. Government computer activities.

7.11 Reporting Requirements

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

7.12 Physical Security

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

7.13 Wireless Electronic Devices

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

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

7.14 Operating Instructions

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

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

7.15 Government Authorization

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

7.16 Access Lock Combinations

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

7.17 Security Combinations

Combinations to security containers, secure rooms or vaults are classified information and must be properly safeguarded. Only contractor employees, who have the proper security clearance and the need-to-know, will be given combinations to security containers, secure rooms or vaults. Contractor employees are responsible for properly safeguarding combinations. Contractor employees will not record security containers, secure rooms or vaults combinations without written approval by the government functional director. Contractors will not change combinations to security containers, secure rooms or vaults without written approval by the security officer and the government functional director.

7.18 Security Alarm Access Codes

Security alarm access codes are "*For Official Use Only*" and will be protected from unauthorized personnel. Security alarm access codes will be given to contractors employees who require entry into areas with security alarms. Contractor employees will adhere to the Air Force activity operating instructions and will properly safeguard alarm access codes to prevent unauthorized disclosure. Contractors will not record alarm access codes without written approval by the government functional director.

7.19 Freedom of Information Act Program (FOIA*)*

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

7.20 Traffic Laws:

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

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

7.21 Cellular Phone Operation Policy

The contractor shall comply with local base policies regarding cellular phone operation.

7.22 Security Education and Training

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

The contractors are required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system. Annually, all contractors will complete all required security training. Required annual training includes Force Protection (FP), Information Protection (IP), Cybersecurity and OPSEC. If contract team members will be using the SIPRNet, users will also have to comply with the organizational Derivative Classification Training as a condition of access.

8. DATA DELIVERABLES

[Define deliverables required for individual task orders. This section contains information on data requirements, such as reports or any of those items contained within a Contract Data Reports List (CDRL). Strive to minimize data requirements that require government approval and delivery. Only acquire data that are absolutely necessary. The usual rule of thumb is to limit data to those needed by the government to make a decision or to comply with a higher level requirement. Refer to Appendix A4, **"Application Services Task Order Data Item Description Deliverables,"** ***for sample data item deliverables. Deliverables should relate directly to the Services Delivery Summary in Section 6. Detailed CDRL requirements and formats should be provided IAW DFAR 204.7105 on DD Form 1423-1, FEB 2001. Note, the number and complexity of required Deliverables need to correlate to the size and complexity of requirements contained in the Task Order.]***

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

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

9. APPLICABLE STANDARDS AND REFERENCES

[Insert applicable standards and compliance references for Appendix A5 in this section. Refer to Appendix A3, **"Application Services Standards & References,"** ***for applicable certifications, specifications, standards, policies and procedures that are required for compliance on individual Task Orders.   Tailor the list as needed for individual Task Orders may impose additional standards to those required at the contract level. The list is not all-inclusive and the most current version of the document at the time of task order issuance will take precedence. Web links are provided wherever possible.]***

10. PRODUCTS STANDARDS AND COMPLIANCE REQUIREMENTS

[If your effort will be requiring the vendor to provide IT Products to meet your requirements then ensure you have selected the applicable IT Product standards and compliance areas from section 10.1-10.18 below.   If your effort will not require IT Products then delete section 10.]

10.1 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 Committee on National Systems Security Policy Number 11 (CNSSP-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.

10.2 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/disr_ipv6_50.pdf). Some example IPV6 mandated products from the DoD IPV6 Standards Profile are listed below:

- Host/Workstations - a desktop or other end-user computer or workstations running a general purpose operating system such as UNIX, Linux, Windows or a proprietary operations system that is capable of supporting multiple applications.

- Network Appliance or Simple Server - Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A Simple Server supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)11 servers, a "web camera" appliance that serves pictures via an embedded web server and a network time server appliance that solely functions to serve NTP requests. Advanced Server - End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network.

- Intermediate Nodes – routers, switches, IA or IA enabled devices.

- IPV6 Capable Software - a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform.

10.3 Energy Star

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

ENERGY EFFICIENCY IN ENERGY-CONSUMING PRODUCTS (DEC 2007)

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

(1) Means a product that—

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

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

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

(1) Delivered;
(2) Acquired by the Contractor for use in performing services at a Federally-controlled facility;
(3) Furnished by the Contractor for use by the Government; or

(4) Specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance.

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

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

(d) Information about these products is available for—

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

NOTE: Remove if not applicable. The following are some example products that are required to be energy star compliant: computers, displays and monitors, enterprise servers, copiers, digital duplicators, fax/printer machines, printers, scanners, televisions, cordless phones, battery chargers, set-top and cable boxes, and audio and video equipment. For further guidance please see the below url: http://www1.eere.energy.gov/femp/technologies/eep_purchasingspecs.html

10.4 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).

10.5 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.

10.6 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/.

10.7 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 PWS. 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.

10.8 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/.

10.9 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.

10.10 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.

10.11 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.

10.12 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.

10.13 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.

10.14 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.

10.15 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.

10.16 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.

10.17 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.

10.18 Product Maintenance

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

Appendix A1 – Application Services Sample Performance Parameters

<u>Instruction</u>: The sample metrics provided in this appendix can be used to measure a contractor's performance and ability to meet defined performance parameters. Utilization of predictive metrics can provide early indication of potential trouble areas through use of trend analysis and provide enough lead time to take preventative maintenance measures to prevent outages and loss of service. Finally, create a set of robust customer service-focused metrics that lead to real improvements in operational performance and customer satisfaction. Include selected performance parameters in Section 6 of the Performance Work Statement, Services Delivery Summary. You are encouraged to include any other performance parameters not mentioned in this document that will assist in measuring a contractor's performance. **Note, the number and complexity of Performance Parameters must correlate to the size and complexity of requirements contained in the Task Order.**

Performance Requirements	Performance Threshold	Monitoring Method
APPLICATION AVAILABILITY		
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
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

Performance Requirements	Performance Threshold	Monitoring Method
User incidents	(X affected users / Y total users) * 100 = % Application Availability; Maximum % effected dependent on mission criticality	QAE monthly review of system metrics
APPLICATION PERFORMANCE		
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
Accuracy	Specify precision (resolution) and accuracy (known standard) that is required in the systems output	QAE monthly review of system metrics
SYSTEM OPERATIONS & MAINTENANCE		
Sustainment activities	Legacy systems are sustained without periods of prolonged degradation	QAE monthly review of system metrics

Performance Requirements	Performance Threshold	Monitoring Method
Sustainment activities	Complex software problems are isolated and resolved	QAE monthly review of system metrics
Sustainment activities	Backlog of deficiencies do not exceed an average of XX (for example pick an appropriate number such as 50 for that particular project) between releases.	Monthly metrics review in the PMR
Sustainment activities	Mean time to assess (MTTA) and mean time to repair (MTTR) for deficiency reports. Choose an appropriate number for each for the project such as 24 hours for category 1, 48 for category 2, etc. and something like 3 business days MTTR for category 1, 15 business days for category 2, and so on.).	Monthly metrics review in the PMR
Sustainment activities	Defect density of repaired code delivered for deficiency repairs and enhancements from BCRs. This should be expressed in average defects per FP or KSLOC.	Monthly metrics review in the PMR
Sustainment activities	Improvement and technology refresh of the application. This should be expressed in percentage of defect density improvement for code and reduction in maintainable code for using new technologies such as code generators.	Monthly metrics review in the PMR
Sustainment activities	Application enhancement performance. This should be expressed in new Function points delivered and function points touched for BCR improvements.	Monthly metrics review in the PMR
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

Performance Requirements	Performance Threshold	Monitoring Method
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
SOFTWARE DESIGN, DEVELOPMENT & TESTING		
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
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
Source Code Scanning	Source code scanning for applications is performed with software that can certify quality application source code, i.e. Sonar.	Random sampling, 100% inspection, periodic sampling

Performance Requirements	Performance Threshold	Monitoring Method
Source Code Scanning	Source code scanning for applications is performed with software that can certify secure application source code, i.e. Fortify.	Random sampling, 100% inspection, periodic sampling
Database Scanning	Database scans will be performed to identify, mitigate, and/or resolve any issues using the DoD Database STIG.	Random sampling, 100% inspection, periodic sampling
QUALITY ASSURANCE		
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
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

Performance Requirements	Performance Threshold	Monitoring Method
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
Equipment disposal	Always follow environmental guidelines when disposing of hardware or electrical equipment	QAE monthly review of contractor metrics
Project design	Always coordinate with applicable engineering functions during the initial project design	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 relative to the agency's 2003 energy use baseline	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
INFORMATION ASSURANCE		
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
Source Code Scanning	Source code scanning for applications is performed with software that can certify quality application source code, i.e. Sonar.	Random sampling, 100% inspection, periodic sampling
Source Code Scanning	Source code scanning for applications is performed with software that can certify secure application source code, i.e. Fortify.	Random sampling, 100% inspection, periodic sampling
Database Scanning	Database scans will be performed to identify, mitigate, and/or resolve any issues using the DoD Database STIG.	Random sampling, 100% inspection, periodic sampling

Performance Requirements	Performance Threshold	Monitoring Method
System C&A compliance	Maintain C&A compliance IAW applicable DoD and AF policy and instruction, particularly DoD Instruction 8510.01 – DIACAP	Random sampling, 100% inspection, periodic sampling
System C&A compliance	Maintain C&A compliance IAW applicable DoD and AF policy and instruction, particularly AFI 33-210 – AFCAP	Random sampling, 100% inspection, periodic sampling
Common usability standards	Requirements to conform to common usability standards, i.e., IBM's CUA or Microsoft's GUI	Random sampling, 100% inspection, periodic sampling
Use Enterprise Information Technology Data Repository (EITDR) to conduct virtual evaluation of systems security and maintain program portfolio data	Used to conduct virtual evaluations of a programs Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information, input is required into the EITDR 100% of the time	Random sampling, 100% inspection, periodic sampling
Use Enterprise Mission Assurance Support Service (eMASS) to conduct virtual evaluation of systems security	Used to conduct virtual evaluations of a programs Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information, input is required into eMASS 100% of the time	Random sampling, 100% inspection, periodic sampling
Communities of Interest (COI) Compliance	Exposed data and information assets in the Metadata Environment (MDE) comply with COI ontology and requirements	Random sampling, periodic sampling
TRAINING		
Training	Specify the required training time for normal users and power users to become productive at particular operations; dependent on mission	Random sampling, 100% inspection, periodic sampling
Training materials	Timely training materials are provided on 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
HELP DESK SUPPORT		
Help desk support	Provide problem resolution for assigned calls; 100% of assigned calls have a problem resolution	Random sampling, 100% inspection

Performance Requirements	Performance Threshold	Monitoring Method
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 ≤ 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
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

Appendix A2 - Application Services Task Order Data Item Description Deliverables

Instruction: The following list provides Data Item Description (DID) deliverables applicable to the Application Services task orders. This list is not meant to be exhaustive or inclusive of all that may be required, referenced or otherwise identified within a given Task Order. The government Task Order Manager, if desired, may require that a CDRL comply with a specific DID or Military Standard, even if it has been rescinded, cancelled or exists only in a draft form. The government Task Order Manager may likewise require the contractor to comply with an identified industry or commercial standard or request the contractor format or utilize existing contractor data. Include all data deliverables in Section 7 of the Performance Work Statement, Data Deliverables. Further guidelines are provided below for compiling your deliverables list. **Note, the number and complexity of required Deliverables must correlate to the size and complexity of requirements contained in the Task Order.**

Adhere to the following guideline when compiling your deliverables list:

- CDRLs that **are separately priced** must use the same sequence number, except the sequence number must start with a "**B**."
- CDRLs with a sequence number starting with an "A" (A001, A002,…) are not separately priced.
- CDRLs with a sequence number starting with a "B" (B001, B002,…) are separately priced.

For detailed CDRL instructions see DoD 5010.12-M, *Procedure for Acquisition and Management of Technical Data*.

http://www.dtic.mil/whs/directives/corres/pdf/501012m.pdf

For detailed information on the DIDs listed below or to obtain DIDs documentation, visit the ASSIST website to search for specific DIDs.

http://www.assistdocs.com/search/search_basic.cfm

For all CDRLs use the following information when completing DD Form 1423-1, FEB 2001

Sequence Number	Data Item Description	Title
A001	DI-ADMN-81306	Program Protection Implementation Plan (PPIP)
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

Sequence Number	Data Item Description	Title
A009	DI-CMAN-80874	Configuration Data Lists (CDLS)
A010	DI-CMAN-81022C	Configuration Audit Summary Report
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
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
A021	DI-IPSC-81427A	Software Development Plan (SDP)
A022	DI-IPSC-81428A	Software Installation Plan (SIP)
A023	DI-IPSC-81429A	Software Transition Plan (STRP)
A024	DI-IPSC-81430A	Operational Concept Description (OCD)
A025	DI-IPSC-81431A	System/Subsystem Specification (SSS)
A026	DI-IPSC-81432A	System/Subsystem Design Description (SSDD)
A027	DI-IPSC-81433A	Software Requirements Specification (SRS)
A028	DI-IPSC-81434A	Interface Requirements Specification (IRS)
A029	DI-IPSC-81435A	Software Design Description (SDD)
A030	DI-IPSC-81436A	Interface Design Description (IDD)
A031	DI-IPSC-81437A	Database Design Description (DBDD)
A032	DI-IPSC-81438A	Software Test Plan (STP)
A033	DI-IPSC-81439A	Software Test Description (STD)
A034	DI-IPSC-81440A	Software Test Report (STR)
A035	DI-IPSC-81441A	Software Product Specification (SPS)
A036	DI-IPSC-81442A	Software Version Description (SVD)
A037	DI-IPSC-81443A	Software User Manual (SUM)
A038	DI-IPSC-81444A	Software Center Operator Manual (SCOM)
A039	DI-IPSC-81445A	Software Input / Output Manual (SIOM)
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

Sequence Number	Data Item Description	Title
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
A070	DI-MGMT-81844	Information Assurance (IA) Test Plan
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
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

Sequence Number	Data Item Description	Title
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

Appendix A3 – Application Services Standards & References

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

Documentation	URL	Description
ENTERPRISE STRATEGY		
DoD CIO Net-Centric Data Strategy	http://dodcio.defense.gov/Portals/0/documents/Net-Centric-Data-Strategy-2003-05-092.pdf	This document describes the Net-Centric Data Strategy for the Department of Defense (DoD), including DoD intelligence agencies and functions. It describes a vision for a net-centric environment and the data goals for achieving that vision. It defines approaches and actions that DoD personnel will have to take as users—whether in a role as consumers and producers of data or as system and application developers.
DoD CIO Net-Centric Services Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf	The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.
DODI 8320.02, Data Sharing in a Net-Centric Department of Defense	http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf	Establishes policies and responsibilities to implement data sharing, in accordance with DoD Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy,” September 19, 2002.
DoD Discovery Metadata Specification (DDMS)	http://metadata.ces.mil/dse/irs/DDMS/	Visibility, accessibility, and understandability are the high priority goals of the DoD Net-Centric Data Strategy. Of these goals, visibility and discovery are intimately linked. Visibility of a resource is, in a practical sense, useless, if the resource is not easily discoverable. With the express purpose of supporting the visibility goal of the DoD Net-Centric Data Strategy, the DDMS specifies a set of information fields that are to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services.
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf	This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain).

Documentation	URL	Description
CJCSI 6212.01F, Interoperability and Supportability of Information Technology and National Security Systems	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf	Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs. Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs and systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment.
Netcentric Enterprise Solutions for Interoperability (NESI)	https://nesix.spawar.navy.mil/home.html	NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application.
DoDI 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS)	http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf	Establishes policy, assigns responsibilities, and provides direction for certifying the interoperability of IT and NSS pursuant to sections 2222, 2223, and 2224 of Title 10, United States Code (Reference (c)). Establishes a capability-focused, architecture-based approach for interoperability analysis. Establishes the governing policy and responsibilities for interoperability requirements development, test, certification and prerequisite for connection of IT, including NSS (referred to in this instruction as "IT"). Defines a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) approach to enhance life-cycle interoperability of IT. Establishes the requirement for enterprise services to be certified for interoperability. Incorporates and cancels DoDD 4630.05, DoDI 4630.8, and DoD Chief Information Officer (CIO) memorandum (References (d), (e), and (f)).
Joint Vision 2020	http://www.fraw.org.uk/files/peace/us_dod_2000.pdf	Strategic Guidance: Joint Vision 2020 builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing transformation of America's Armed Forces.
ENTERPRISE ARCHITECTURE		
DoD Global Information Grid Architectural Vision	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&Location=U2&doc=GetTRDoc	The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information – the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.
Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework.aspx	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.

Documentation	URL	Description
AFPD 33-4, Information Technology Governance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-4/afpd33-4.pdf	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.
AFI 33-401, AIR FORCE ARCHITECTING	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 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.
GiG Technical Guidance Federation GIG-F	https://gtg.csd.disa.mil/uam/registration/register	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.
SYSTEMS ENGINEERING		
Business and Enterprise Systems (BES) Process Directory	https://acc.dau.mil/bes	The BES Process Directory (BPD) is a life cycle management and systems engineering process based on the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System; as tailored for Information Technology (IT) systems via the Defense Acquisition Process Model for Incrementally Fielded Software Intensive Programs
AFI 10-601, Capabilities-Based Requirements Development	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.

Documentation	URL	Description
AFI 63-101, Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	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 99-103, Capabilities-Based Test and Evaluation	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature sys-tem designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.
DoD Open Technology Development Guidebook		This roadmap outlines a plan to implement Open Technology Development practices, policies and procedures within the DoD.
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	http://www.sei.cmu.edu/library/assets/soabest.pdf	This document was developed under the Net-Centric Operations Industry Forum charter to provide industry advisory services to the Department of Defense (DoD), Chief Information Officer (CIO). It presents a list of industry best practices in achieving Service Oriented Architecture (SOA).
INFORMATION ASSURANCE		
ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.dni.gov/files/documents/ICD/ICD_503.pdf	This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.
DoDI 8500.01 Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) 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.
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf	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	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf	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,Risk Management Framework (RMF) for DoD Information Technology (IT)	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf	Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

Documentation	URL	Description
AFI 33-200, Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 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)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf	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)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.
Air Force Guidance Memorandum (AFGM), End-of-Support Software Risk Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2015-33-01/afgm2015-33-01.pdf	This Guidance Memorandum supersedes AFGM 2014-33-03, Microsoft Windows XP End-of-Life, and highlights current policies and SAF/CIO A6 authorities to mitigate cybersecurity vulnerabilities introduced by unsupported software. Compliance with this Memorandum is mandatory.
AFMAN 33-282, COMPUTER SECURITY (COMPUSEC)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-282/afman33-282.pdf	This AFMAN implements Computer Security in support of AFPD 33-2, Information Assurance Program and AFI 33-200, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 33-200.
AFMAN 33-285, Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-285/afman33-285.pdf	This rewrite identifies cybersecurity baseline certification requirements for the AF cybersecurity workforce; stipulates minimum certification requirements for various cyber roles and risk management positions; sets qualifications criteria; clarifies the cybersecurity-coding position process; and codifies the waiver policy for baseline certification requirements.
DoDI 8540.01, Cross Domain (CD) Policy	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf	Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) in accordance with the authority in DoD Directive (DoDD) 5144.02
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.
INFORMATION TECHNOLOGY STANDARDS		
Federal Information Processing Standards (FIPS)	http://www.nist.gov/itl/fipscurrent.cfm	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

Documentation	URL	Description
IEEE/EIA 12207.0, "Standard for Information Technology	http://www.ieee.org/	IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes", is a standard that establishes a common framework for software life cycle process. This standard officially replaced MIL-STD-498 for the development of DoD software systems in May 1998.[1] Other NATO nations may have adopted the standard informally or in parallel with MIL-STD-498.This standard defines a comprehensive set of processes that cover the entire life-cycle of a software system—from the time a concept is made to the retirement of the software. The standard defines a set of processes, which are in turn defined in terms of activities. The activities are broken down into a set of tasks. The processes are defined in three broad categories: Primary Life Cycle Processes, Supporting Life Cycle Processes, and Organizational Life Cycle Processes.
DoDD 8000.01 Management of the Department of Defense Information Enterprise	http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf	Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense
AFI 10-208 Air Force Continuity of Operations (COOP) Program	http://www.fas.org/irp/doddir/usaf/afi10-208.pdf	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs); and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).
US Government Configuration Baseline (USGCB)	http://usgcb.nist.gov/	The United States Government Configuration Baseline (USGCB) is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. USGCB continues to be one of the most successful government IT programs aimed at helping to increase security, reduce costs, and accelerate the adoption of new government technologies, while creating a more managed desktop environment.
DoD Mobile Application Strategy	http://www.defense.gov/news/dodmobilitystrategy.pdf	It is intended to align the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from such activities and aligns with efforts composing the Joint Information Environment.
ISO/IEC 20000	http://www.iso.org/iso/home.html	ISO/IEC 20000 is an international standard for IT Service Management (ITSM). It allows IT organizations to ensure the alignment between ITSM processes and their overall organization strategy. It requires the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system (SMS). ISO/IEC 20000 consist of 5 separate documents, ISO/IEC 20000-1 through 20000-5
QUALITY ASSURANCE		
AFPD 33-3, Information Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-3/afpd33-3.pdf	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.

Documentation	URL	Description
AFMAN 33-363, Management of Records	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf	This manual implements DoDD 5015.2, *DoD Records Management Program*, and Air Force Policy Directive (AFPD) 33-3, *Information Management*. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.
DoD Instruction 5015.02, DoD Records Management Program	http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic
AFI 33-364, Records Disposition – Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management,* by listing program objectives and responsibilities, guiding personnel in disposing of special types of records, retiring or transferring records using staging areas, and retrieving information from inactive records.
DoDI 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoDD_523024.pdf	This Directive updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
AFI 61-204, Disseminating Scientific and Technical Information	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-204/afi61-204.pdf	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.
AFMAN 33-152 Communications and Information	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-152/afman33-152.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*, AFPD 33-2, *Information Assurance (IA) Program*, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities.
AFMAN 33-402 - Service Development and Delivery Process (SDDP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-402/afman33-402.pdf	This Air Force Manual (AFMAN) provides guidance for the definition, design, acquisition, implementation and delivery of Business Mission Area (BMA) capabilities using the Service Development and Delivery Process (SDDP). The SDDP is end user-centric to better align the assistance required by an end user to address a process-based problem across a holistic set of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) solutions. The SDDP details the processes and procedures by which Information Technology (IT) capabilities supporting Air Force (AF) processes are identified, defined, developed and delivered in a way that ensures IT capabilities are necessary, and maximize the potential for successful implementation of IT investments. The SDDP is applicable to large and small scale problems and can be used to implement IT capabilities of all sizes and types.

Documentation	URL	Description
AFMAN 33-153 Information Technology (IT) Asset Management (ITAM)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-153/afman33-153.pdf	This is a total revision to replace and incorporate Air Force Instruction (AFI) 33-112, Information Technology Hardware Asset Management, and AFI 33-114, Software Management, into a single IT asset management manual. This revision incorporates the PWCS asset management portions of AFI 33-106, Managing High Frequency Radios, Personal Wireless Communications Systems, and the Military Affiliate Radio System, to remove that guidance; and identifies Tiered waiver authorities for unit level compliance items.
DoDD 5205.02E, Operations Security (OPSEC) Program	http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf	Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations.
AFI 10-701, Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf	This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.
DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).
DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf	This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
Section 508 of the Rehabilitation Act of 1973	http://www.opm.gov/html/508-textOfLaw.asp	On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.

Documentation	URL	Description
DoDI 1100.22 Policy and Procedures For Determining Workforce Mix	http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf	In accordance with the authority in DoD Directive 5124.02, this Instruction establishes policy, assigns responsibilities, and prescribes procedures for determining the appropriate mix of manpower and private sector support. It implements policy established in DoDD 1100.4 and incorporates and cancels DoDI 3020.37. This Instruction provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently governmental (IG); commercial (exempt from private sector performance); and commercial (subject to private sector performance). It reconciles and consolidates the definitions and examples of IG from section 306 of title 5, U.S.C.; sections 501 (note), 1115, and 1116 of title 31, U.S.C., Attachment A of OMB Circular A-76; and Subparts 2 and 7.503(c) of the FAR into a set of criteria for Defense-wide use. This Instruction also implements aspects of sections 113, 188(b), 129a, and 2463 of title 10, U.S.C., and reissues and cancels DoDI 1100.22.
DoDD 8320.1 Data Administration	https://acc.dau.mil/adl/en-US/33650/file/6823/DoDD83201%20Data%20Admin.pdf	This Instruction applies to the administration and standardization of DoD standard data elements generated within the functional areas of audit and criminal investigations for DoD. It also applies to the administration of DoD standard and non-standard data elements generated, stored, or used by the DoD. Data elements will be administered in ways that provide accurate, reliable, and easily accessible data throughout the DoD, while minimizing cost and redundancy. Data elements will be standardized to meet the requirements for data sharing and interoperability throughout the DoD. Data administration will be encouraged and promoted within the DoD.
AFI 33-332, Air Force Privacy and Civil Liberties Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf	Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
AFI 31-501, Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi31-501/afi31-501.pdf	Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5 to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013.
AFI 16-1404, Air Force Information Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf	This publication implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance; Department of Defense (DoD) Directive 5210.50, Management of Serious Security Incidents Involving Classfied Information, DoD Instruction (DoDI) 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual (DoDM) 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDm 5200.45, Instructions for Developing Security Classification Guides.

Documentation	URL	Description
Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	FISMA was enacted as part of the E-Government Act of 2002 to “provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets,” and also to “provide for development and maintenance of minimum controls required to protect Federal information and information systems.” FISMA requires Federal agencies to: •designate a Chief Information Officer (CIO), •delegate to the CIO authority to ensure compliance with the requirements imposed by FISMA, •implement an information security program, •report on the adequacy and effectiveness of its information security policies, procedures, and practices, •participate in annual independent evaluations of the information security program and practices, and •develop and maintain an inventory of the agency’s major information systems. FISMA requires the Director of the Office of Management and Budget (OMB) to ensure the operation of a central Federal information security incident center. FISMA makes the National Institute of Standards and Technology (NIST) responsible for “developing standards, guidelines, and associated methods and techniques” for information systems used or operated by an agency or contractor, excluding national security systems.
ISO/IEC 19770-2, Software Tagging	http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670	ISO/IEC 19770-2:2009 establishes specifications for tagging software to optimize its identification and management. (http://en.wikipedia.org/wiki/ISO/IEC_19770)
FAR CLAUSES		
DFARS 252.227-7015 Technical Data Commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1079_80393	Provides the Government specific license rights in technical data pertaining to commercial items or processes. DoD may use, modify, reproduce, release, perform, display, or disclose data only within the Government. The data may not be used to manufacture additional quantities of the commercial items and, except for emergency repair or overhaul and for covered Government support contractors, may not be released or disclosed to, or used by, third parties without the contractor's written permission.
DFARS 252.227-7014 Rights in Noncommercial Computer Software	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P683_47378	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.
DFARS 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1182_92447	Provides requirements for the identification and assertion of technical data.
DFARS 252.227-7013 Rights in Technical Data---Non-commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P295_15657	Provides guidelines for rights in technical data on non-commercial items