60th Maintenance Group Web Application Development
Task Order Performance Work Statement (PWS)
20 May 2024

Name:	**Web Application Development**
Organization:	**60th Maintenance Group**
Address:	**501 Hangar Ave., Travis Air Force Base, CA**

Executive Summary

This contract provides for the administration of 60th Maintenance Group (MXG) Information Technology (IT) web assets on the Air Force Network (AFNet). The objective of the Web Application Developer (WAD) is to provide web services supporting the 60th MXG Commander at Travis Air Force Base directly, and indirectly supporting the 60th Air Mobility Wing. The contractor is expected to be a partner within the MXG community in continuously improving the quality of products and services offered to customers.

60th Maintenance Group Web Application Development

1. PURPOSE

The purpose of this Task Order is to acquire information technology (IT) services for the 60th Maintenance Group, Travis Air Force Base. The contractor shall provide on-site professional IT Web Application Development services for the 60th Maintenance Group Information Portal.

2. SCOPE

The 60th Maintenance Group is seeking the contracted support, sustainment, and future development of the existing 60th Maintenance Group Web Portal. The site supports the staff and 5 squadrons within the group. The scope of the services includes System Network Administration, Web Application management and Database Development. The support will be provided at Travis Air Force Base with web assets on the Air Force network (AFNet).

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

This is a non-personal services contract for the administration of 60th Maintenance Group (MXG) Information Technology (IT) web assets on the Air Force Network (AFNet). The mission of the Web Application Developer (WAD) is to provide web services supporting the 60th MXG Commander at Travis Air Force Base directly, and indirectly supporting the 60th Air Mobility Wing. This program gives the MXG Commander a method to combine all his/her resources together into an integrated network that supports all MXG users. The service contractor is expected to be a partner within the MXG community in continuously improving the quality of products and services offered to customers. This consolidated centralized programming effort provides IT infrastructure and sustainment for the 60 Maintenance Group's ever growing use of IT. The contractor shall perform/provide 60MXG customers with timely, proactive, high quality communications and web services. These services shall include, but not limited to, IT planning, local customer support of Information Hub (IH) resources, server management and administration, software installation, configuration and support, software management, information assurance, information protection operations, customer training and support and education. Contractor's proficiency level must keep pace with technological advances in the IT industry. The contractor will use DISA data feeds to populate portal content. In the event of data loss, the contractor must use DISA help desk sources to recover and sustain data feed.

Factor	**Data**
Code and data complexity	C#, .NET, Java, PL/SQL, TSQL, IIS, *.SLN, *.CSPROJ, *.CSS, *.XSD, *.RESX, *.WSDL, *.RDLC, *.P7B, *.CER, *.CRT, *KEY, *.PEM, ASP, XML, HTML5, VB. Use of stored procedures. Data pull thru DISA linked server Foreign Keys used in Travis ODS tables to ensure unique aircraft identifiers

Factor	Data
Stability	8-hours mean time to repair legacy code.
Number of concurrent users	30+
Application age	22+ years
Initial response time	2-hour average initial response time for online applications and/or web services.
Life expectancy	Contingent upon technical refresh and mission requirements
Operating system	SQL Server 2022, Windows Server or newer.
Platform	Standard server
Programming Languages	Code and data complexity C#, .NET, Java, PL/SQL, TSQL, IIS, *.SLN, *.CSPROJ, *.CSS, *.XSD, *.RESX, *.WSDL, *.RDLC, *.P7B, *.CER, *.CRT, *KEY, *.PEM, ASP, XML, HTML5, VB. Use of stored procedures. Data pull thru DISA linked server

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 system applications and resolve problems relating to software changes as they relate to existing system applications. The contractor shall maintain the current baseline of the system and provide software changes 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:

- Continually review developed applications to ensure sustained reliability and desired operation. Upgrades/updates as required. Responds to customer identification of discovered application “bugs” with appropriate fixes.

- 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 as written in Appendix A1.

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.

The contractor is responsible for developing new and updating existing applications in support of the 60th Maintenance Group. Contractor will be familiar with existing and emerging development technologies to ensure that the MXG is always developing on the latest industry standard. Contractor must have a high level of proficiency in full life cycle from analyzing business requirements, developing use cases, object modeling, developing, and testing software through production to deployment. Software being used/tested must be approved by the Air Force Evaluated Products List. Contractor must be able to analyze each programming project and apply the appropriate technology for the job.

- 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.

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 Web Services

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

3.3.2 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.

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 17-100 Air Force Technology (IT) Service Management, DoD 8570.01M Information Assurance Workforce Improvement Program and transitory publication DoDM 8140.03.

3.4.1 Database Administration

Contractor will have a plan for data backup and recovery and for short-term loss of system hardware and software. Develop and maintain a system backup and recovery procedures. Executes backups on all assigned systems by extracting the backup information and moving it to a primary designated backup system and clearly labeling it by backup object and date. Backup the data and rotate the data at specified times, in accordance with established procedures to prevent potential data loss from malfunctions and preserve database integrity. Maintain a current digital backup library, locating digital backup in government provided secure site storage. Restore files and databases when requested. Ensure all digital data are labeled properly, sufficient, and legible. This information shall be verified every time the digital data backup is used.

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

3.4.2 Systems Administration

The contractor responsibilities include management of 60th Maintenance Group Information Hub core servers/services. Server administration functions including applications services and application development functions. Contractor will be responsible for the configuration, administration, backup, and routine tasks associated with all core servers and their operation IAW applicable directives and regulations.

The contractor is responsible for technical administration, maintenance, deployment and administrative upgrade of government furnished; contractor deployed application servers. This includes hardware and software configurations, maintenance, upgrades and any security updates or patches required.

- Integrate and perform analysis of existing systems to maximize continuity between applications and the performance of system hardware.
- Install, support and maintain computer systems.
- Maintain hardware and software lifecycle End of Life (EOL) dates and request government replacement/refresh 18-months prior to the End of Support date.
- Plan and respond to service outages.
- Diagnose software and hardware failures to resolution.
- Implement and ensure security preventive measures are fully functioning.
- Monitor and enhance system performance.

3.4.3 Customer Training

Contractor shall provide application training support on developed software applications. Provide technical services, to include basic, intermediate, and advanced training on the use of the standard automation tools provided to the members. Training will be conducted in a classroom environment. Contractor shall provide a visual presentation in conjunction with a lecture on the use of the contractor developed software applications and standard automation tools provided to the Maintenance Group members. Contractor will provide all necessary training for developed applications to task key personnel within five duty days upon completion of all contractor developed software applications. The contractor is responsible for the following:

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

3.4.3.1 Customer Support

- Assist users with application interface and operability issues.
- Conducts customer assistance for developed applications as needed.
- Routinely works with resident LOGNET IT contractors to sustain and develop new applications using shared data.

4. ENGINEERING REQUIREMENTS

4.1 Systems Engineering

The contractor is responsible to design, develop and perform Web Application and Development services for the 60 MXG website. Contractor will work independently in support of database development and management. The contractor analyzes requirements, creates, designs, and implements requirements in required media, and provides program support, tests, debugs and writes documentation as required.

4.1.1 Life-Cycle Systems Engineering

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

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 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

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.

Develops and programs using C#, .NET, Java, PL/SQL, TSQL, IIS, *.SLN, *.CSPROJ, *.CSS, *.XSD, *.RESX, *.WSDL, *.RDLC, *.P7B, *.CER, *.CRT, *KEY, *.PEM, ASP, XML, HTML5, VB, and other modern languages to facilitate implementation of desired system improvements and capabilities. Designs, implements, manages, and upgrades all required database back ends for developed applications. Acts as the technical advisor for all contractor developed programs, infrastructure, and applications.

Contractor shall document all programming language and architecture for each web based application/database. This documentation shall be logged daily and presented to the IT Manager upon request. Documentation medium will be contained in the form of an operating manual detailing the logic of the code utilized to design each web-based application/database.

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 DODAF - DOD Architecture Framework Version 2.02 - DOD Deputy Chief Information Officer (defense.gov).

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

The contractor shall conduct testing and deployment of web application services using distributed testing environments. The contractor shall develop dynamic testing environments to support C&A and functional testing.

4.4.1 Test Lab

The contractor shall establish and maintain an integrated test source 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 DAFI 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.

4.5 Information Assurance

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.

The contractor will ensure that servers are configured using the latest Directory Service Control Center and security policies of AFNet. Contractor will also ensure server is configured with System Center Configuration Manager client and is responsible for testing/applying security

patches. If a patch is found not to be compatible, contractor must provide Network Operations (60 CS/SCOO) Plan of Action & Milestones (POA&M) for specific security patch/TCNO.

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 AFMAN 17-301, Computer Security (COMPUSEC)and AFI 17-130, Air Force Cybersecurity Program 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 17-101, Air Force Risk Management Framework (RMF) Program. 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 Manual 8140.03 Cyberspace Workforce Qualification and Management Program.

5. CONTRACTUAL REQUIREMENTS

The contractor will work projects as directed by the Information Technology Manager. This may include adjusting priorities to accommodate the current level required for mission support. The contractor will provide a monthly status report (MSR) to the Information Technology Manager by the 5th business day of the succeeding month.

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 contractor will perform services on Travis Air Force Base.

5.3 Normal Hours of Operation

The average work week is 40 hours. The average workday is 8 hours and the window in which those 8 hours may be scheduled is between 6:00 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

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)
- 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

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

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

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 AMCI 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 DoDM 5200.02 and DAFMAN 16-1405, Personnel Security Program (Jul 18), 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

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

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

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.

6. SERVICES DELIVERY SUMMARY

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum

acceptable levels of service required for each requirement. These thresholds are critical to mission success. Reports/Deliverables:

No.	PERFORMANCE OBJECTIVE	PWS REFERENCE	PERFORMANCE THRESHOLD
1	Provide distributed and web-based applications in support of the 60th Maintenance Group mission in accordance with PWS requirements.	Section 3, Sub 2	Distributed and web-based applications must meet the requirements of the 60th Maintenance Group mission. Development of new distributed and web-based applications must be completed within 180 days upon initial requirement. All existing and new distributed/web-based applications must be updated within 10 duty days upon initial requirement.
2	Assist users with application interface, operability, and training issues.	Section 3, Sub 4.3	All application interface and operability issues must be addressed within 2 duty days of user request, and application training accomplished within 5 duty days of completion.
3	Implement a review process to ensure continued reliability and desired operation.	Section 3, Sub 1	A review process to ensure 100% reliability of fully operational distributed and web-based applications must be performed at least once a duty day.
4	Manage the configuration of the contractor deployed application servers	Section 3, Sub 4	All application servers are maintained with operational hardware/software configurations/serviceable End of Life (EOL)/upgrades, security updates and backups.
5	Management reports and meetings/progress reviews	Section 5	All monthly reports due on the 5th business day, conduct monthly in-progress reviews

7. SECURITY REQUIREMENTS

7.1 Security Facility Clearance Requirements

The contractor must possess or obtain a favorable background check prior to performing work on this government contract.

If the contractor does not possess a favorable background check the government will request one. The contractor shall notify the 60th Security Forces Squadron, Plans and Programs Flight, Information Protection (60 SFS/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.

7.2 Personnel Security Clearance Requirements

Some or all of the personnel performing work on this contract will require a favorable background check.

7.2.1 Additional Investigation Requirements

Anyone working on the contract 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: DAFMAN 16-1405, and DoDMAN 5200.02 for unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/or sensitive equipment.

7.3 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 this 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.

7.4 Pass and Identification Items

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

- DoD Common Access Card (DAFI 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.

7.5 Visitor Group Security Agreement (VGSA)

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 DoDM 5220.22V2, *Industrial Security Regulation,* Air Force Policy Directive 31-6, *Industrial Security,* DoDM 5200.01, Volumes 1-4, *DoD Information Security Program,* and AFMAN 16-1404, Air Force 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).

7.6 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 Manual 31-401, *Information Security Program Management* and all applicable supplements and operating instructions.

7.7 Computer and Network Access Requirements

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.

(X) 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.

7.8 Reporting Requirements

The contractor shall comply with requirements from AFI 71-101*,* Volume-1 and Criminal Investigations Program, 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.

7.9 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.

7.10 Wireless Electronic Devices

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

7.11 Operating Instructions

The contractor will adhere to 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.

7.12 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.

7.13 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.

7.14 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.

7.15 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.

7.16 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 and Civil Liberties 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 AFI 33-322, Records Management and Information Governance Program; 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/.

7.17 Traffic Laws:

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

7.18 Cellular Phone Operation Policy

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

7.19 Security Education and Training

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

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 DAFI 61-201 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the Government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers and other data for which the Government shall treat as deliverable.

8.1 Data Item Description Deliverables

Sequence Number	Data Item Description	Title
A008	DI-CMAN-80858B	Contractor's Configuration Management Plan
A016	DI-ILSS-80872	Training Materials
A021	DI-IPSC-81427A	Software Development Plan (SDP)
A029	DI-IPSC-81435A	Software Design Description (SDD)
A030	DI-IPSC-81436A	Interface Design Description (IDD)

Sequence Number	Data Item Description	Title
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)
A040	DI-IPSC-81488	Computer Software Product
A047	DI-MCCR-81344	Design Specification
A048	DI-MGMT-80227	Contractor's Progress, Status and Management Report
A049	DI-MGMT-80269	Status of Government Furnished Equipment (GFE) Report
A055	DI-MGMT-80501	Contractor's Corrective Action Plan
A056	DI-MGMT-80507C	Project Planning Chart
A057	DI-MGMT-80555A	Program Progress Report
A068	DI-MGMT-81842	Vulnerability Scan Compliance (VSC) Report
A079	DI-QCIC-81187	Quality Assessment Report
A084	DI-RELI-80254	Corrective Action Plan
A088	DI-SESS-81002E	Developmental Design Drawings/Models and Associated Lists

9. 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.
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.

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.
SYSTEMS ENGINEERING		
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 system designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&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.
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management and DoDM 8140.03	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf; https://public.cyber.mil/wid/dod8140/	Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.

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.
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 33-322, 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.
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).
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.
DAFMAN 16-1405	https://static.e-publishing.af.mil/production/1/saf_aa/publication/dodman5200.02_dafman16-1405/dodm5200.02_dafman16-1405.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.
AFMAN 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 Classified 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
FAR CLAUSES		
DFARS 252.227-7015 Technical Data Commercial Items	252.227-7015 Technical Data - Commercial Products and Commercial Services. | Acquisition.GOV	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.

Appendix A1 – Application Services Performance Parameters

Performance Requirements	Performance Threshold	Monitoring Method
APPLICATION AVAILABILITY		
Unscheduled application downtime	Meets application availability thresholds; Equal or fewer than 24 hours	QAE monthly review of system metrics
Scheduled application downtime	Meets application availability thresholds; Equal or fewer than 50 hours	QAE monthly review of system metrics
User incidents	(X affected users / Y total users) * 100 = % Application Availability; Maximum 96% effected dependent on mission criticality	QAE monthly review of system metrics
APPLICATION PERFORMANCE		
Ports and protocols	Applications are using the port/protocol as specified by policy	QAE monthly review of system metrics
User load/capacity	Services allow for 100 concurrent users required while not impacting system performance	QAE monthly review of system metrics
Response time	Maximum allowable response time for a user transaction; user transaction should not exceed 5 seconds	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
Sustainment activities	Complex application problems are isolated and resolved within 10-duty days	QAE monthly review of system metrics
Database administration	Maintain development and test environments ensuring software upgrades, patches, and hot fixes are applied	Random sampling, 100% inspection, periodic sampling
Backup and Restore Requirements	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

Performance Requirements	Performance Threshold	Monitoring Method
APPLICATION DESIGN, DEVELOPMENT & TESTING		
Application development	New distributed and web-based applications must be completed within 180 days upon initial requirement.	100% inspection
Application coding design	Design baseline, test plans, verify requirements, implementation plan, and list of documented constraints and risks	100% inspection
Application implementation/testing	Tailor for efficiency, update training materials, test readiness and fully integrate within system	100% inspection
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	Configuration management practices are followed as prescribed by AF procedures to include version control	QAE random checks
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/secure application source code	Random sampling, 100% inspection, periodic sampling

Performance Requirements	Performance Threshold	Monitoring Method
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
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	Quality training materials are provided to the customer that accurately reflect and correspond to processes and services	Random sampling, 100% inspection, periodic sampling