Performance Work Statement

For

AMARG Business Systems Support Services

NETCENTS-2 SOLUTIONS

1 November 2016

Review / Coordination

Mission Support Flight Chief **Date**

Director, Production Support **Date**

Quality Assurance Program Coordinator **Date**

Contracting Officer **Date**

Performance Work Statement
For
AMARG Business Systems Support Services

EXECUTIVE SUMMARY

The Contractor shall perform the full spectrum of business systems application support services in support of daily operation activities at the 309th Aircraft Maintenance and Regeneration Group (309 AMARG) located at Davis Monthan Air Force Base (DMAFB). The 309 AMARG reports to the Ogden Air Logistics Complex (OO-ALC), Air Force Materiel Command (AFMC) and complies with policy and regulatory guidance from AFMC; and as a tenant at DMAFB follows HQ Air Combat Command (ACC) policy and regulations where applicable with host responsibilities as identified in the Host Base - Tenant Agreements Operations and Maintenance (O&M) and Consolidated Sustainment Activity Group - Maintenance (CSAG-M).

The 309 AMARG is responsible for the Management, Operations and Maintenance of the 309 AMARG Business Systems (ABS). The 309 AMARG also writes communications/application systems policy, develops and submits budgetary and planning artifacts and manages the 309 AMARG ABS resolution actions.

The ABS follows Air Force (AF) Portfolio Management guidelines and is a Chief Financial Officer Act (CFO) compliant system comprised of a series of commercial off the shelf/Government off-the-shelf (COTS/GOTS) software packages, hardware, appliances and infrastructure. In order to improve the integration of the software packages for use by 309 AMARG personnel, a number of unique queries and reports have been developed to support all aspects of 309 AMARG's business objectives. The 309 AMARG has integrated this series of COTS/GOTS systems into what is now known as the ABS. The use of the ABS must be sustained, enhanced and maintained. The supporting technical infrastructure must also be maintained to ensure all business operations of the 309 AMARG remain competitive, and compliant in the Department of Defense (DoD) environment.

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

The contractor shall provide all personnel, labor, supervision, and management to perform on-site business system application support services, in the form of certified information technology support staff, who will perform the full range of application support services for the 309 AMARG, located at DMAFB, AZ. The contractor shall provide all personnel, supervision, expertise, training and incidentals to design, develop, procure, sustain, maintain and enhance new and existing application packages and their supporting hardware and infrastructure, in accordance with (IAW) this Performance Work Statement (PWS). The PWS defines the full requirement for application support services necessary to support the 309 AMARG. For the purposes of this PWS, the ABS is broadly defined as all software, services and hardware utilized in support of the 309 AMARG mission. The list of supported applications for these various services is outlined under PWS paragraph 2.

2. SUPPORTED APPLICATIONS

The contractor shall provide on-site operational, administrative, technical / management planning and support for all aspects of 309 AMARG's Business System. The list of supported applications will change and is not considered all inclusive. The Contractor shall optimize the use of the 309 AMARG Business Systems (ABS) and identify areas for process improvement initiatives.

Factor	Data
Operating System	HPUX Windows Server 2003 and subsequent Windows 7, 10 and subsequent Windows XP LINUX Red Hat and subsequent VMWare NetApp or current Storage Area Network (SAN) technology Unified Computing System (UCS) Cisco, Juniper, and Aruba Wired/Wireless Networking or subsequent Air Force directed solutions currently100 switches/80 access points; planned phased upgrade to wireless and wired infrastructure
Major Applications	Oracle Financials (Oracle 12x and subsequent) Oracle Database 11x and subsequent Oracle Discoverer/OBIEE and subsequent Oracle OAM/OIM or other directed solution IBM MAXIMO 7 and subsequent Workplace System 7.x, Time and Attendance Accounting (TAA) or other directed solution Air Force directed network management solution Network backup solution (currently NetBackup) Airforce Global Enterprise Tracking (AFGET)/Maintenance Operations Center Visualizer (MOCVIS) Tableau Server MS Project Server MS Sharepoint Server MS SQL Server Unit Productivity Kit (UPK) or similar training development tool
Desktop Applications	Internet Explorer/Edge/Firefox MS Office MS Project Tableau MS Sharepoint Outlook E-mail MAXIMO Production Acceptance Certification Standard System (PACSS) Remedy SBSS IETM/ETools Oracle cMRO Unit Productivity Kit (UPK) or similar training development tool
Outside Systems (not locally hosted)	Non-Secure Intranet Protocol Router Network (NIPERNET) FEMS Consolidated Aircraft Maintenance Management System (CAMS) Reliability and Maintenance Information System (REMIS) Defense Civilian Personnel Data System (DCPS) Automated Business Service System (ABSS)

Factor	Data
	Joint Engineering Data Management Information and Control System (JEDMICS) Electronic Personnel Security Questionnaire (EPSQ) Defense Messaging System (DMS) Consolidated Engine Management System (CEMS) Cargo Movement and Operations System (CMOS)
Databases	Oracle Oracle Client or current SQL Sybase
Programming Languages	Oracle Fusion Middleware (including WebLogic Server 10.3.6, and Forms and Reports v11.1.1.6) or current Java/SQL/WebSphere/HTML
Average number of users	650 users
Average Transactions per day	Inserts: 10,000 Updates: 6,000 Deletes: 3,000
Average Help Desk Call Volume	55 calls per day 2 priority
Code & Data Complexity	Oracle Forms: 225 Oracle Reports: 100 PL/SQL Packages: 300 Oracle Triggers: 145 Oracle Tables: 475 Oracle Table Columns (data elements): 5570 Oracle Unique (primary key) Indexes: 215 Oracle Non-Unique indexes: 195 Oracle Index columns: 850 Oracle Views: 55 Oracle Sequences: 60If there are throughput requirements on batch/background updates or reports, provide the current average and the desired goal/objective.
Web/Software/interface Development Complexity	Simple development; modifications and changes (2-5 day deployment) approx. 50/yr Normal development; interface design, screen development, (5-15 day deployment) approx. 30/yr Complex developments, software rewrite and version changes (15-90+ days) approx. 20/yr AMARG supports internal and external customer interfaces, both simple and complex. These web applications, interfaces, and tools require, creation, upgrades, enhancements and eventual major version changes. These must be completed in a timely manner and meet software/web development flow days outlined above. Flow days include Definition, planning, development, testing, Interface Control Documentation (ICD),and implementation
IT/Peripheral Equipment (approx.)	Personal Computers 700 Laptop computers 500 Collection devices 100 Multi-Function Devices 200 LMR radios 400 Cell phone/Tablets/PWCS 200 Point of Use (POU) 20 Audio Visual Devices 60

3. SYSTEM SUSTAINMENT / IMPROVEMENTS

3.1. Sustainment: The contractor shall design, develop, test and package systems and software changes and provide problem resolutions for the existing system and any future upgrades. The contractor shall maintain the current baseline of the system software and hardware 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. Key tasks shall include:

- Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases, and interfaces in compliance with applicable AF/DoD standards.
- Maintain existing levels of hardware capabilities IAW network direction from the Host.
  - Desktop and Laptop (Etools) hardware availability is critical to the success of the AMARG Mission. Hardware availability shall not fall below 90%
- Support system sustainment activities to include maintaining existing legacy systems and environments and to sustain current and future applications, databases, and interfaces. Including ensuring systems resources are not over utilized.
- Provide application services to support, maintain, and operate systems or services.
- Develop business process maps, user training, and configuration control artifacts using the UPK software.
- Plan for and provide required hardware, appliance and infrastructure support, upgrades, and migration as directed by Government Information Technology (IT) supervisor

3.2. Systems Planning Support: The contractor shall assist Government-designated AMARG personnel in the areas of Systems Strategic Planning and Management. The contractor shall maintain the C4 Systems Installation Records (CSIR), in accordance with Air Force Instructions for the ABS. The contractor shall provide all documentation required to conduct Configuration Control Board (CCB) meetings at the working levels through senior leadership for the 309 AMARG and when required at OO-ALC. Preparation for this task may include (but not limited to):

- Accumulating all the IT requirements, both hardware and software, that are unresolved, assessing those requirements and providing recommendations based upon best utilization of resources and commercial best practices.
- Provide ongoing tracking and reporting of all IT Procurements
- Provide technical solutions, recommendations and assistance for all IT procurements
- Building a prioritization list of requirements for presentation to the voting members of the CCB and supporting the presentation of this information to the CCB.
- Assisting with Maintenance Repair and Overhaul Interactive (MROi) system or equivalent, data management, legacy deconstruction, organizational management, and organizational redesign and fielding implementation working groups to identify data conversion tasking, interface requirements, implementation and sustainment planning and deployment for MROi or equivalent.

3.3. Systems Production Analysis Support: The contractor support shall include, but is not limited to, providing both functional and technical support for the operation and maintenance of the ABS and associated components. Support shall include:

- Developing or assisting in the development of Ad Hoc queries and reports as directed.
- Providing system production analysis support to improve the ABS and associated business processes. The contractor shall provide Government IT supervisor with ongoing ABS performance enhancement suggestions.
- Making recommendations for ABS improvements and ensuring the ABS systems can support 309 AMARG Strategic Planning and Process Improvement efforts through participation in Continual Process Improvement initiatives; research and recommendations on aerospace and industry standards and bench marking enterprises that could contribute to more effective and efficient 309 AMARG system operations.

3.4. Continuous Process Improvements (CPI): The contractor shall provide dedicated support to the 309 AMARG Air Force Smart Operations for the 21st Century (AFS021)/Air Force System Command (AFSC) Way Strategic Planning Process and Process Improvement efforts through participation in CPI event planning and facilitation, research and recommendations on aerospace and industry standards and bench marking enterprises that could contribute to more effective and efficient 309 AMARG operations. The contractor shall provide guidance, training, assistance and execution in the application of industry tools for process evaluation and improvement such as Lean Six Sigma, Theory of Constraints, AFSC Way, Art of the Possible etc. The contractor shall provide assistance in the development, oversight and execution of objectives, personnel training and mentoring of process improvement skills related to the Strategic Planning process through daily support to the 309 AMARG AFS021/AFSC Way office and its projects. The contractor shall assist in the identification of training, education and orientation ventures that will contribute to Leadership Development for all levels of the organization. All projects will be accomplished within the negotiated timelines.

3.5. Change Request (CR) Management: The contractor shall be responsible for the 309 AMARG CR process with the 355th Communications Squadron (355 CS). This includes submitting CR's (AF form 265, *AFO Payment Authorizations (JUMPS)*), tracking and reporting of the CR's to completion. The contractor shall ensure that Subject Matter Expert (SME) is consulted on all CR's prior to submitting.

3.6 Systems Development, Migration, Planning and Integration Support: The contractor shall 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, hardware upgrades, hardware migrations, application and infrastructure integration, 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), if directed by Government IT supervisor.
- Utilize GOTS or approved COTS tools for systems design and development
- Ensure all mobile applications being developed receive their Certification and Accreditation package and they must be developed to be device agnostic. Ensure compliance with the DoD Mobile Development Strategy V2.0 dated May 2012 or current.
- If applicable, ensure compliance with the AF 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.
- Develop, maintain, and ensure operation of manual and automatic system interfaces that support and enhance business process efficiency.

3.7. Information Services: 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.

A. **Data Stores:** The contractor shall ensure performance of the following tasks:

- 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.

B. **Information Exposure Services:** The contractor shall ensure performance of the following:

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

3.8. Systems Operations: Systems operations requirements must comply with applicable documents and standards specified in Section 9 of this Task Order (TO) PWS. The contractor shall provide full 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 Air Force Instruction (AFI) 17-100, *Air Force Information Technology (IT) Service Management,* and DoD 8570.01M, *Information Assurance Workforce Improvement Program*. Key task at a minimum shall include:

A. 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.

B. 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.

C. Customer Training:

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

D. Help Desk Support: The contractor shall provide full spectrum Help Desk support for technical assistance, user account maintenance, order processing, repair dispatch, support of multiple software versions and applications, standard desktop configuration, training, warranty, and maintenance, from 0500 to 2300 hours on regular duty days, and as needed on weekends. At a minimum the contractor shall accomplish the following administrative tasks:

- Maintain a detailed record of each customer contact; to include complaint and eventual resolution.
- Establish a notification process to alert users when trouble tickets are resolved.
- Provide telephone support to include, personal computer (PC) software and hardware troubleshooting and administrative changes, i.e., access user ID, password reset.
- Elevate unresolved trouble tickets.

E. Wireless Local Area Network (WLAN) Support: The contractor shall provide full spectrum support for 309 AMARG, Base Infrastructure Transport Implementation (BITI) Wireless, WLAN and Radio Frequency Identification (RFID) equipment as required. The contractor shall coordinate with 309 AMARG and Combat Information Transport System (CITS) personnel to upgrade and maintain this infrastructure as needed. Wireless LAN support consists of planned wireless coverage in all facilities as well as throughout the desert operations areas (approx. 2600acres)

F. Backup Records: The contractor shall keep records of all backups to include, but not limited to, source of backup, date of backup, person who made the backup, and storage location of the backup. Perform nightly backups of all business data and databases. Maintain weekly backups of all business data and databases on and off site. Backup all Operating Systems and applications on an as needed or as directed schedule. Maintain both on and off-site emergency backups. Off-site backups can be at another operating location's Storage Area Network (SAN). The contractor shall exercise and test contingency operation plans and ensure documented instructions are in place, end users trained and test scripts maintained to recover system to full operation in the event of an emergency- by site or system. Provide a regular backup of data on the existing system. Establish, publish and communicate to process users when the backup of systems and databases occur. The contractor shall exercise and test contingency operation plans. The contractor shall ensure documented instructions are in place, end users trained and test scripts maintained to recover system to full operation in the event of an emergency, by site or system.

G. Time Compliance Network Orders (TCNOs), Notice To Airmen (NOTAMs) and Vendor Patches Installation: The contractor shall ensure all TCNOs, NOTAMs, and vendor patches, etc., are installed on system servers and on all end user PCs as required by the DMAFB Network Control Center (NCC) and Air Force Network Operations and Security Center (NOSC) and as required by the 309 AMARG Configuration Control Board (CCB) and Air Force Instructions.

H. Equipment Management: Key minimum tasks:

- Assist in completion of procurement documentation i.e., purchase request forms, Brand Name Justifications, Sole Source letters, Market Research.
- Take full responsibility of Automated Inventory Management System (AIM) data integrity/accuracy.
- Be responsible for input of all items in AIM, equipment transfers, annual inventories and disposal/turn-in. Only Government personnel can determine which equipment items are transferred and which equipment items are disposed.
- Provide personnel designated as an ECO, alternate ECO, and Information Technology Equipment Custodian (ITEC) who shall adhere to AFM 33-153, *Information Technology Asset Management*, dated 19 March 2014.

3.9 Safety **Requirements:** In performing work under this contract, the Contractor shall:

- Ensure their employees are made aware that the performance of these services may occur in industrial areas.
- While the contractor may perform duties in a marked and signed regulated area there may be contact hazards with these materials during cleanup of dust, metal shavings, etc. The contractor shall ensure proper protective measures and training is taken to protect contracted employees from these hazards.
- Conform to the safety requirements contained in the contract for all activities related to the accomplishment of the work. This includes the wearing of appropriate Personal Protective Equipment (PPE); i.e., hearing protection, safety shoes, protective eyewear. All PPE shall be provided by the Contractor.
- PPE must meet or exceed standards in OSHA 29 CFR 1910, as well as AFI 91-203, Chapter 14.

4. ENGINEERING REQUIREMENTS

4.1 Systems Engineering

4.1.1 Life-Cycle Systems Engineering: The contractor shall employ disciplined systems engineering processes including, but not limited to, requirements development, technical management and control, system/software design and architecture, integrated risk management, configuration management, data management, and test, evaluation, verification and validation practices throughout the period of performance of task orders in accordance with AFI 63-101, *Integrated Lifecycle 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 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: 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: When requested and specified in the task order, the contractor shall establish and maintain a system integrated test environment that is capable of supporting a full range of integration test activities for both the currently fielded system as well as maintenance/modernization releases and any interfaces designated by Government Representative (GR). 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 virtual private network (VPN), Firewall, security configuration of products and operating systems and common access card (CAC) Middleware testing), usability, transition (upgrade paths) and packaging/installation.

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

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

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

4.4.4 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.

4.4.5 System Performance Testing: 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: 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 DOD Instruction 8500.01, *Cybersecurity*, 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, *Risk Management Framework (RMF) For DoD Information Technology (IT)*, and AFI 33-210, *Air Force Certification and Accreditation (C&A) 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 at no cost to Government with, technical and/or management certifications at a minimum of IAT Lev II to ensure compliance with DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005 (with all current changes).

5. CONTRACTUAL REQUIREMENTS

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 shall perform services under this Task Order primarily at the 309 AMARG, located at 4850 S. Wickenburg Ave., DMAFB,Tucson, Arizona; however, on occasion contractor personnel shall be required to perform services, attend training, and attend meetings at other locations on DMAFB, the local Tucson area or other locations serviced by AMARG. Contractor personnel travel within 50 mile radius of the 309 AMARG will be at no extra cost to the Government.

5.3 Normal Hours of Operation: The contractor shall provide coverage on site between 5:00 AM and 11:00 PM, Monday through Friday or as specified in this TO. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. The contractor shall provide Help Desk/technician coverage Monday through Friday from: 0500 – 2300. Peak hours shall be 0630-1530. Occasional weekend coverage shall be required to meet production requirements. The contractor shall provide all Non-Help Desk functional coverage during the core hours of 0730-1530.

5.3.1 Federal Holidays: The contractor is not required to provide routine services on the following recognized Federal holidays (or the actual day set aside for observation): New Year's Day, Martin Luther King Jr's Birthday, Presidents Day, Memorial Day, Independence Day, Labor Day Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

5.3.2 Scheduled and Unscheduled Downtime: The contractor shall support updates and patches of all 309 AMARG servers that are initiated by USAF, currently Sunday mornings from 0100-0600 and as needed during the standard work week. Contractor shall ensure systems are fully operational prior to 0500 first workday of each week. Contractor initiated maintenance shall occur on Sundays. Any unscheduled downtime of 309 AMARG servers, regardless of source of disruption, shall be reported immediately with a resolution or resolution plan of action in place no more than (4) four hours after the problem/issue is detected by contractor or government personnel. Upon resolution of downtime, the Contractor shall provide a lessons learned brief to Government SMEs regarding source of the downtime and corrective actions. The contractor shall provide the Government SME with electronically written daily status report of all system degradation. The contractor shall ensure no portion of the ABS shall experience a down time exceeding 24 hours.

5.4. Government Furnished Property: 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, *Department of Defense Contract Security Classification Specification*, 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 Contracting Officer's Representative (COR) 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. Contractor employees shall not be directed to attend events such as morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Since a contract employee is not a Government employee, contractor employees cannot be granted the same duty time activities as Government employees.

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 TO Contracting Officer 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.

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. Contractor/subcontractor personnel 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/subcontractor personnel 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 TO performance will be monitored by the Government and reported in Contractor Performance Assessment Reporting System (CPARS) or a Customer Survey, depending on the dollar amount of the TO. Performance standards shall include the contractor's ability to provide or satisfy the following:

- Provide satisfactory solutions to application, hardware and device 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.
- Requirement shall be broken into simple and complex tasks with simple tasks of 5 flow days and complex tasks of 20 flow days.
- Ensure solutions to requirements are in compliance with applicable policy and regulation.

5.9. Program Management/Project Management: The contractor shall designate a primary and at least one alternate on-site Contract Manager (CM), who shall be responsible for the contractor's performance. The CM shall have full authority to act for the contractor on all matters relating to the daily operation of the contract, and may be a contractor employee providing services. The contractor shall submit the names and telephone numbers of the primary and alternate CM for after business hours, including nights, weekends, and holidays to the Contracting Officer within (5) five days upon contract award or personnel changes occur. The contractor shall provide updated information to the Contracting Officer when changes to the primary or alternate CM occur. The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this TO, participating in Program/Project Management Reviews, and ensuring all standards referenced herein are adhered to.

5.9.1. Portfolio Management: The contractor shall identify a Portfolio Manager who shall be the primary representative responsible for all portfolio management activities for the ABS including, but not limited to; providing reports to 309 AMARG and other AF or DoD authorities, responding to data calls as needed, and updating and preparing certification, software approval packages and all accreditation packages as needed. The contractor shall ensure ABS data and artifacts are updated and maintained in Enterprise Information Technology Data Repository (EITDR) and Enterprise Mission Assurance Support Service (EMASS) (or subsequent).

5.9.2. Orientation / Transition Period: The contractor shall ensure successful transition of services. Key tasks include

A. Orientation Period. The contractor shall submit within 10 days upon contract award, a ramp-up/orientation plan that shall demonstrate how TO staffing shall be accomplished and utilized through the orientation period and a method to ensure performance, which shall include phase-in timelines. The plan shall also include the number and position titles of personnel to be on site for the orientation period. **(Contract Data Requirements List (CDRL) A001)**

B. Ramp-up Phase. At a minimum, the contractor shall accomplish the following tasks within the initial ramp-up phase of the program:

- Implement their Transition Plan upon TO award.
- Ensure transition from each incumbent shall be completed no later than 10 days following task order award.
- Provide a fully trained team to support all PWS requirements within 30 days of task order award.
- Ensure all employees possess required training, qualifications, proficiency, and security clearances and satisfy all other access requirements.
- Complete familiarization from the incumbent contractor if there is a change in contractor, or the Government if there is no incumbent.
- Participate in task order Post Award "kickoff" meeting.
- Ensure all personnel requiring CACs have such upon task order award.
- Ensure all personnel requiring a security clearance have such upon task order award.
- Ensure all personnel requiring a Secret clearance or higher are updated in the Joint Personnel Adjudication System (JPAS) upon contract award.
- Ensure all personnel have received required training for courses that are not Government only.
- Ensure contractor employees complete all required / mandatory training as identified by the Government.
- Ensure that annual training is completed within 3 days of expiration and that all mandatory training is completed within Air Force designated timeframes."
- Conduct contractor Industrial Hygiene surveys, if the Contractor determines that such are necessary on behalf of and in the best interest of their employees for the sites on the task order.
- The Contractor shall provide Quality System Plan to CO upon contract award. **(CDRL A007)**

5.9.3 Services Summary: Reference Section 6, Services Summary 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 Summary will be in accordance with AFI 63-101/20-101, *Integrated Life Cycle Management*, AFI 10-601, Operational Capability Requirements Development, and FAR Subpart 37.6, *Performance-Based Acquisition*.

5.9.4. Task Order Management: The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce shall include all required certifications for appointment as Contract Site Lead (CSL), alternate Equipment Control Officer (ECO) and alternate Information Assurance Officer (IAO) for those in appropriate positions. The workforce shall include a project/ TO manager who shall 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 to the Government SME and designated COR. 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 TO efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness, and consistently high-quality delivery.

5.9.5. 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. The Contractor shall provide all contract performance reports and related status documents in accordance with the noted requirements below or as noted within this TO:

A. Project Management Review: The contractor shall provide every Thursday a weekly report **(CDRL A005);** which addresses performance to project schedules and timeliness, issues, problems, work in progress (WIP). The report shall include:

- Information on TCNOs, NOTAMs, and vendor patches that have been installed and those pending installation.
- Help Desk Call Volume/Activity.
- All Information Technology (IT)/Audio Visual (AV) activity to include status of systems, change requests, data calls
- Development statuses
- Equipment management lifecycle status including inventory status
- Procurement Activity/tech solution development
- Network and equipment availability rate/status.

B. Software Licenses Administration: The contractor shall provide a semi-annual report that indicates when software licenses require renewal, number of licenses per applications and number deployed per application. The report is due on 15 March and 30 August of each year. **(CDRL A002)**

C. Hardware Warranty Administration: The contractor shall provide a semi-annual report that indicates when hardware warranties and support contracts are due along with recommendations on whether the warranty should be renewed or the hardware replaced. The report is due on 15 March and 30 August of each year. **(CDRL A003)**

D. Network Infrastructure Map/Industrial Enclaves: The contractor shall provide a network infrastructure map of all the switches, access points, sensors and servers on the network, to include software and version numbers. This report is due on 30 January and

30 June of each year. **(CDRL A004).**

E. Annual Manpower Report - The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil. Reporting Period: Contractors are required to input data for the labor executed during the Period Of Performance (POP) for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be recorded anytime during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to the Contractor Manpower Reporting Application (CMRA) help desk. Uses and Safeguarding Information: Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data. Website User Manuals: Data for Air Force service requirements must be input at the Air Force CMRA link. However, user manuals for government personnel and contractors are available at the Army CMRA link at http://www.ecmra.mil.

F. Quality Assurance Plan - The contractor shall establish and provide a Quality Assurance Plan to ensure the requirements of this contract are provided as specified. It shall include identifying methods used to detect, report, track, and resolve process problems and trends. It shall also include a point of contact to interface with the Government and provided to the Contracting Officer upon contract award. **(CDRL #A007)** Key Tasks:

- The contractor shall make appropriate modifications to the Quality Assurance Plan as required by process changes or government guidance which affects current contractor processes.
- The contractor's Quality Assurance Plan shall comply with the minimum quality management systems elements specified in the American National Standards Institute (ANSI)/American Standards Organization (ASO)/International Standards Organization (ISO) family of standards.

5.9.6. 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 Air Force Manual (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 base IDIQ of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

5.9.6.1. Protection of System Data: Unless otherwise stated in the TO, 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, *DoD Freedom of Information Act Program*, and DoD Manual 5200.01(Vol. 1 – Vol. 4), *DoD Information Security Program*, 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.

5.9.6.2. System and Network Authorization Access Requests: 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 DD Form 2875, *System Authorization Access Report (SAAR)*.

5.9.7. Travel: The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or IT Government Supervisor to obtain advance, written approval for the travel. 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 Contracting Officer 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 by the Government.

5.9.8. Other Direct Cost (ODC): The contractor shall identify ODC and miscellaneous items as specified in each TO. No profit or fee will be added; however, Defense Contract Audit Agency (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 Contracting Officer. 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 Contracting Officer. 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: Contractor employees may participate in other Government provided training, on a non-discriminatory basis as among contractors, under the following circumstances:The contractor shall ensure contractor employees attend / complete annual requirements for mandatory Government training. Mandatory training may be classroom and/or intranet web-based. The contractor shall ensure mandatory training is completed within timeframes designated by the Government.The contractor shall ensure that contractor employees complete mandatory training for issuance of CAC cards IAW AFI 31-501, Personnel Security Program Management, and related AF and local supplements.The contractor employees' participation is on a space-available basis, participation does not negatively impact performance of this TO, 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 TO.

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 TO. 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 TO, the contractor shall fully support all unique software developed to support integrated solutions on this contract. The contractor shall 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 maintain documentation for all systems and software supported under this TO. The contractor shall maintain 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, 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: The contractor shall complete Unit Software Licenses management duties. The contractor shall provide maintenance and support of all software licenses to manage its relationship to the overall system life-cycle, which would include applications, license agreements and software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, and sustainment and configuration control, to include providing research and documentation support in the procurement 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
In accordance with DFARS 237.76 – *Continuation of Essential Contractor Services*, the requirements in paragraphs 3 through 5 of this PWS have been determined to be essential during

crisis and the contractor will be required to perform during crisis, unless otherwise directed by the CO. The contractor shall ensure enough skilled personnel are available during a crisis for any operational emergency. A written plan for continuation of services shall be submitted to the CO; which should include 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.

6. SERVICES SUMMARY

The contractor shall comply with the performance standards and meet the thresholds described in the table below. The contractor shall provide and maintain a quality control plan and shall identify failure(s) to deliver services on schedule or failure(s) to meet the performance threshold(s) as described below. Not identifying a failure will result in the specific deliverable being rejected and invoice rejection in the Wide Area Workflow (WAWF) system until deliverables have been corrected and accepted by the Government. All failures must indicate the percentage of error attributable to the contractor and means for overcoming the failure. The performance requirement, standards, method of measurement, and performance thresholds are as follows:

Performance Objective	PWS Para	Performance Standard	Performance Threshold	Method of Surveillance
Program Management / Project Management	**5.9**	The Contractor shall submit the names and telephone numbers of the primary and alternate CM for after business hours, including nights, weekends, and holidays to the Contracting Officer within (5) five days upon contract award or change in personnel. The contractor shall provide updated information to the Contracting Officer when changes to the primary or alternate CM occur. 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.	Submit to the Contracting Officer within (5) five days upon contract award or change in personnel.	100% Inspection five days upon contract award or change in personnel.
Ramp-up / Orientation Plan	**5.9.2**	Documentation must demonstrate how TO staffing shall be accomplished and utilized through the orientation period and a method to ensure performance, to include a phase-in timeliness. **(CDRL A001)**	Final document must be delivered within 10 days of contract award and must be acceptable to the Government.	100% Inspection of final document delivered within 10 days of contract award. **(CDRL A001)**

Performance Objective	PWS Para	Performance Standard	Performance Threshold	Method of Surveillance
Unscheduled application downtime/ Scheduled application downtime	**5.3.2**	Any unscheduled downtime of 309 AMARG servers, regardless of source of disruption, shall be reported immediately with a resolution or resolution plan of action in place no more than (4) four hours after the problem/issue is detected by contractor or government personnel. Upon resolution of downtime, the Contractor shall provide a lessons learned brief to Government SMEs regarding source of the downtime and corrective actions.	Critical applications will not exceed 16 hours a year of unscheduled downtime.	SME monthly review of system metrics/ Trouble ticket system
Technical Order (TO) management systems (ETOOLS)	**3.1**	ETOOLS shall be maintained at an operational availability level of 90%. Measured based on the total number of ETOOLS in the field.	All Production related TO system will be maintained at a minimum of 90% availability. **(CDRL A005)**	Weekly review of CDRL A005.
Computing requirements and resources (virtual environments)	**3.1**	Projected amount of computing resources and requirements is not exceeded; actual versus projected difference in computing resources (CPU, RAM, storage, etc.) acceptable.	System resource usage will not exceed 85% of available capability without approval from GR.	SME to monitor Real-time resource.
User load/capacity	**3.1**	Services allow for the specified number of users required while not impacting system performance,	System resource usage will not exceed 85% without approval from GR.	SME to monitor Real-time resource.
Database administration	**3.8**	Maintain development and test environments and databases; operating system and software upgrades, patches, and hot fixes are applied to all environments	Test environment shall be maintained and utilized 100% of time for any new or updated releases	CDRL A005 will be reviewed weekly
Establish individual User Accounts (including email)	**3.8**	Contractor shall create User Accounts in a timely manner; Accounts shall be created within the same business day that they are received	Number of business hours until completion from time of notification by customer; 8 hours, 90% of the time. (reviewed monthly)	SME to monitor trouble ticket system; random sampling
Password Reset	**3.8**	Contractor shall reset user accounts that are locked out within 1 hour of notification	Number of minutes until completion from time of notification by customer; 60 minutes, 95% of the time (reviewed monthly)	Trouble ticket system review; random sampling

Performance Objective	PWS Para	Performance Standard	Performance Threshold	Method of Surveillance
Delete User Accounts (including email)	**3.8**	Contractor shall be notified by Government IT supervisor, when users are out processing. Contractor shall remove access for user within 1 business day of notification	Number of business days until completion from time of notification by customer; 1 day	Trouble Ticket system review, random sample
Backup and Restore Requirements	**3.8**	Implement and maintain backup and restoration capabilities for all data, applications and component configurations.	Backup frequency – daily incremental, Weekly Full, and End of Fiscal Year ArchiveSnap Shots will be maintained at one hour (1 hr). Maintain ability to recover from a data loss incident with no more than 24hours of lost data.	COR will consult with the SMEs to verify if the Contractor implemented and maintained a backup and restoration capabilities for all data, applications and component configurations; backup frequency – daily incremental, Weekly Full, and End of Fiscal Year Archive. Snap Shots will be maintained at one hour (1 hour). SME will inform COR if this requirement is being met.
Software procurement analysis	**5.15**	Detailed Analysis to include pricing and technical solution.	100% of all requests of IT support, will include a complete technical solutions, including any pricing.	COR will consult with the SMEs to verify if the Contractor entered data into CCBWEB.
Software implementation	**5.15**	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% of Software and web development will follow formal process, test plans will be created and approved before implementation	SME perform 100% inspection. Results reported in the CCBweb application.
Software testing	**5.15**	Software system functional testing must pass all test scenarios prior to software being deployed to all platforms for User Acceptance Testing.	First Pass Yield for all development tests will meet or exceed 85%	SME perform 100% inspection. Results reported in the CCBweb application.
Software acceptance support	**5.15**	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% of development projects will be tracked and testing procedures will be documented	SME perform 100% inspection. Results reported in the CCBweb application.

Performance Objective	PWS Para	Performance Standard	Performance Threshold	Method of Surveillance
Configuration management database (CCBWEB) updates and accuracy	**3.2**	The contractor shall assist Government-designated AMARG personnel in the areas of Systems Strategic Planning and Management. The Contractor shall maintain the C4 Systems Installation Records (CSIR), in accordance with Air Force Instructions for the ABS. The contractor shall provide all documentation required to conduct Configuration Control Board (CCB) meetings at the working levels through senior leadership for the 309 AMARG and when required at OO-ALC.	Configuration management database updated with all new Form 003 or current form system and kept current within 2 duty days.	Random sampling.
IT systems inventory updates and accuracy	**3.8 (H)**	IT system inventories include all hardware and software.	100% accuracy rate is maintained	100% annual review by SME.
Network Infrastructure Map/Industrial Enclaves	**5.9.5 (D)**	The contractor shall provide a network infrastructure map of all switches, access points, sensors and servers on the network to include software and version numbers.	Accurate diagrams will include 100% of network Infrasturcture hardware. Maps will be Current (within 30 days) at time of submittal **(CDRL A004)**	COR to review and verify through SME report submitted on 30 January and 30 June. **(CDRL A004)**
Change request (CR) Status	**3.5**	All Change requests are reported each week in Project Management Review. **(CDRL A005)**	CDRL A005 will include 100% of Open change requests with a current (within 1 week) status **(CDRL A005)**	COR to review and verify through SME change request status included in Thursday's reports **(CDRL A005)**
Change request management resolution time	**3.5**	The contractor shall be responsible for the 309 AMARG CR process with the 355 CS. This includes submitting CR's (AF form 265), tracking and reporting of the CR's to completion. The contractor shall ensure that SME is consulted on all CR's prior to submitting.	CRs will be created and ready for review within 2 business days of notification	Random sampling. **(CDRL A005)**
Software management	**5.9.5 (B); 5.15**	Contractor shall inventory all Software 100% annually and GR will be notified 120 days prior to software license renew or support expiration. . **(CDRL A002)**	Same as performance standard.	COR will review **(CDRL A002)** and verify with SME contractor notified SME 120 days prior to software license renewal or support expiration.

Performance Objective	PWS Para	Performance Standard	Performance Threshold	Method of Surveillance
Equipment disposal	**3.8 (H)**	Contractor shall be responsible for disposal and turn in. Contractor shall follow Air Force and Defense Logistics Agency, DLA guidelines when disposing of hardware or electrical equipment.	100% of all Government excess equipment shall be disposed of appropriately.	COR to verify through SME. **(CDRL A005)**
System security compliance; Application security compliance; System C&A compliance	**4.5.1; 4.5.2**	Maintain C&A compliance IAW applicable DoD, AF, FIAR policy and instruction, particularly DOD Instruction 8500.01, *Cybersecurity.*; Maintain application security compliance IAW applicable DoD, AF, FIAR policy and instruction, particularly the Security Technical Implementation Guide (STIG); Maintain C&A compliance IAW applicable DoD, AF, FIAR policy and instruction, particularly DoD Instruction 8510.01 – DIACAP; particularly AFI 33-210 – AFCAP	STIG Review must address 100% of the items on the checklist. Each finding must be supported with evidence.	100% inspection of STIG report for each release or if STIG version changes
Use Enterprise Information Technology Data Repository (EITDR) to conduct virtual evaluation of systems security and maintain program portfolio data	**5.9.1**	Update and report ABS security, inoperability, sustainability and usability (SISSU) information into EITDR.	100% compliance with updates.	COR to verify/consult with SME on contractor updating and reporting ABS security, SISSU information into the EITDR 100% of the time.
Use Enterprise Mission Assurance Support Service (eMASS) to conduct virtual evaluation of systems security	**5.9.1**	Update and report ABS security, inoperability, sustainability and usability (SISSU) information into eMASS	100% compliance with updates and reporting.	COR to verify/consult with SME on contractor updating and reporting ABS security, SISSU information into the eMASS 100% of the time.
Help desk support	**3.8 (D)**	Help Desk operations shall be available from 0500-2300 hours each business day	100% of assigned calls have a problem resolution unless authorized by SME	COR will consult and verify with SME contractor providing problem resolution for assigned calls 100% of assigned calls authorized by SME.

Performance Objective	PWS Para	Performance Standard	Performance Threshold	Method of Surveillance
Admin Changes (Access user ID, password reset)	**3.8. (D)**	Contractor shall maintain a detailed record of each customer contact; to include complaint and eventual resolution. Contractor shall establish a notification process to alert users when trouble tickets are resolved. Contractor shall provide telephone support to include, PC software and hardware troubleshooting and administrative changes, i.e., access user ID, password reset. Contractor shall be responsible for elevation of unresolved trouble tickets.	100% completed ≤ 1 business days (Changes done electronically)	COR will consult and verify with SME contractor providing Admin changes (access user ID, password resets) electronically within 1 business day.
First Call Resolution	**3.8**	Contractor shall provide problem resolution for assigned calls within 24 hours of assignment.	65 % of all trouble tickets resolved during initial call.	COR will consult and verify with SME 65% of problems resolved during the initial call. COR to review Help Desk Trouble Ticket system monthly with SME.

7. SECURITY REQUIREMENTS

All contractors supporting this TO must have the appropriate Security Clearance in accordance with AFI 31-501, *Personnel Security Program Management*, applicable to the Information Technology responsibility level outlined within DOD Instruction 8500.01, *Cybersecurity*.
, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs, prior to reporting to 309 AMARG to perform services. Technicians, Systems and Network Administrators require a minimum of Secret clearance.

All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02E, DoD *Operations Security (OPSEC) Program* and AFI 10-701, *Operations Security (OPSEC)*. 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 with 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 TO.

7.1. National Agency Check with Inquiries (NACI): As a minimum, contractor employee(s) shall successfully complete a NACI before operating Government-furnished workstations that have access to Air Force automated information systems. Requests for personnel hired at the beginning of the contract, shall be submitted to the Government not later than 45 working days from the contract start date. Requests for personnel hired subsequent to the contract start date shall be submitted to the Government not later than five (5) workdays from the employees first duty day. Contractor employees that receive an unfavorable NACI will not be employed. The Government will submit requests for investigations on an AF Form 2583, *Request for Personnel Security Action*, at no additional cost to the contractor. The contractor shall comply with the requirements of DoD 5200.2-R, *Personnel Security Program*, and AFMAN 17-1201, *User Responsibilities And Guidance For Information Systems.* The contractor is responsible for handling all other security clearance related processing for individuals that require clearances higher than a NACI.

7.2 Procedures for obtaining a National Agency Check with Inquiries (NACI) level favorable clearance. In order for a contractor employee(s) to obtain a favorable NACI clearance, they shall contact their company Security Manager to obtain a Standard Form (SF) 85P, *Questionnaire for Public Trust Positions*. The Contractor's Security Manager shall coordinate with the 309 AMARG Security Office to obtain the SF 85P if they do not have hard copies. Once the contractor employee completes the SF 85P, the contractor employee shall inform the site lead and company Security Manager. The site lead shall schedule a review of the form with the 309 AMARG Security Manager. Once the review is complete the SF 85P will be given back to the contract employee as a reference, at which time the 309 AMARG Security Office will coordinate the official opening of the Electronic Questionnaire for Investigation Processing (EQIP) system with the 355th FW Information Protection Office (355 IP) utilizing the Air Force Form 2583, *Request for Personnel Security Action.* Once notified that the EQIP system is open, it is the responsibility of the contractor employee to complete the forms according to the time line and procedures outlined in the initiation emails and any follow on emails/correspondence relating to fingerprints etc. The 309 AMARG Security Office will also provide contractor employee(s) with information for obtaining a DoD Common Access Card (CAC).

7.3. Government Issued Access Badges. The contractor Site Manager for AMARG shall coordinate all requests and issues pertaining to CAC cards with 309 AMARG Security Office. The Government will issue contractor employee(s) with a DoD Common Access Card (CAC) or a Defense Biometric Identification System (DBIDS) Card for access onto the installation. Contract employees shall be supplied with a Controlled Area Badge (CAB) that allows them to access the AMARG. The CAC/DBIDS/CAB cards shall be under the control of the contractor employee at all times. Upon completion of contract performance or as otherwise directed by the Government, the contractor employee shall return all badges to the 309 AMARG Security Office. Loss or damage to an assigned CAC card must be reported to the 309 AMARG Security Office immediately. Failure to return badges or report loss/damage could result in withholding of payment to the contractor.

7.4. Listing of Employees. The contractor shall maintain a current listing of employee(s) performing services on DMAFB. The list shall include employee's name, social security number, driver's license number and state of issue. The contractor shall submit the list to the Contracting Officer and the COR, prior to the contract start date, and submit an updated list when an employee's status or information changes, within 5 working days of the change. The name of any contractor employee(s) that is terminated during the period of the contract must be reported to the Contracting Officer in writing within one workday of the employee's termination. **(CDRL A006).**

7.5. Security Training. All contractor employee(s) shall receive initial and recurring security education training from the sponsoring agency's security manager. Training must be conducted in accordance with DoDM 5200.01, *Department of Defense Security Program* and AFI 16-1404, *Air Force Information Security Program*, Chapter 6, Security Education and Training Awareness. Contractor personnel who work in Air Force controlled/restricted areas must be trained in accordance with AFI 31- 101, *Integrated Defense* (FOUO).

7.6. Should a security violation occur: The contractor shall record and report to the AMARG Security manager, 520-228-8051, 4851 S. Wickenburg Ave. Bldg. 7615, DMAFB, AZ 85707, and to the Contracting Officer or designated representative within one hour, all available facts relating to the security incident. Key tasks:

- The contractor shall take reasonable and prudent action to establish control of the scene to prevent further violation, and to preserve evidence until released by proper authority.
- The contractor shall cooperate fully and assist government personnel if the government elects to conduct an investigation of the violation.

7.7. Obtaining and Retrieving Identification Media: As prescribed by the AFFARS 5352.242-9000, Contractor Access to Air Force Installations, AFFARS 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 shall 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.

7.8. 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 AFI 36-3026, *Identification Cards For Members of the Uniformed Services, Their Eligible Family Members, And Other Eligible Personnel*.
- 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.

7.9. Computer and Network Access Requirements: 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 DD Form 2875, *System Authorization Access Report (SAAR).*

7.10. 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.

7.11. Physical Security: Contractor employees shall comply with base and site Operations Plans/instructions for Force Protection Condition (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.

7.12. 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 Emission Security (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.

7.13. Operating Instructions: The contractor shall 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.

7.14. 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.

7.15. 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.

7.16. 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. Contractor personnel shall not change combinations to security containers, secure rooms or vaults without written approval by the security officer and the government functional director.

7.17. 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 shall not record alarm access codes without written approval by the government functional director.

7.18. 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 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/.

7.19. Traffic Laws: Contractor employees shall comply with all DM AFB traffic regulations and state traffic laws. Contractor employees are subject to random vehicle speed control checks. Failure to adhere to base traffic regulations may result in the loss of base driving privileges, debarment from the base, or other administrative action. Seat belt use is mandatory for all drivers and passengers of vehicles.

7.20. Cellular Phone Operation Policy: The use of cell phones is strictly prohibited while driving on DMAFB, unless the phone is hands free.

7.21. Security Education and Training: Contractor personnel 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 Antiterrorism, Force Protection (FP), Information Protection (IP), Cybersecurity, OPSEC, and a general security procedures review.

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 acceptable by the Government until the 10 day period has passed, unless the Government explicitly states otherwise.

CDRL Number	Deliverable Title	Number / Format	Due Date
A001	Ramp-up/Orientation Plan	Standard Distribution	10 days after contract award
A002	SW Licenses Administration	Standard Distribution	Quarterly
A003	HW Warranty Administration	Standard Distribution	Quarterly
A004	Network Infrastructure Map	Standard Distribution	30 Jan and 30 Jun
A005	Project Management Review	Standard Distribution	Weekly using current unit reporting requirement.
A006	List of Employees para.	Standard Distribution	Pre-Performance Conference, as information changes
A007	Quality Plan	Standard Distribution	Upon contract award

8. 1. Deliverable Instructions: The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Instruction 5230.24, *Distribution Statements on Technical Documents* 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

Refer to Appendix A3, “Application Services Standards & References,”

Appendix A3 – Application Services Standards & 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).
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.

Documentation	URL	Description
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.
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.

Documentation	URL	Description
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.
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.

Documentation	URL	Description
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. - DOD Instruction 8500.2 was cancelled and incorporated in DOD Instruction 8500.01, *Cybersecurity.*
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).
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.

Documentation	URL	Description
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.
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

Documentation	URL	Description
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 24730/IEC 20000 Wireless Device Standards	http://www.iso.org/iso/home.html	ISO 24730/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 24730/IEC 20000 consist of 5 separate documents, ISO 24730/IEC 20000-1 through 20000-5
AFI 33-115 Air Force Information Technology Service management	http://www.e-publishing.af.mil/	AF IT Service Management and assigns responsibilities for the configuration, provisioning, maintenance, and management of AFIN using an IT Service Management (ITSM) framework to further integrate capabilities and maintain configuration control of AF networks and data servers.
AFI-33-114 Software Management	http://www.e-publishing.af.mil/	It identifies responsibilities for management of commercial off-the-shelf (COTS) and Air Force-unique software acquired by the Air Force
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.
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

Documentation	URL	Description
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.
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.

Documentation	URL	Description
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.
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.

Documentation	URL	Description
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 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.
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)
AFI 10-601 Operational Capability Requirements Development	*http://www.e-publishing.af.mil*	This chapter provides an overview of the Joint Capabilities Integration and Development System (JCIDS) requirements process and highlights the interdependent relationship between the Requirements process and the Defense Acquisition System, Test and Evaluation and the Planning, Programming, Budgeting and Execution (PPBE) processes.
AFI 33-364 – Records Disposition – Procedures and Responsibilities	*http://www.e-publishing.af.mil*	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.
AFI 31-101 Physical Security Procedures for the Air Force	*http://www.e-publishing.af.mil*	Chapter identifies physical security procedures for the AF