NETCENTS-2 SOLUTIONS
Network Operations (NetOps) and Infrastructure Solutions

HEADQUARTERS AIR EDUCATION & TRAINING COMMAND (AETC) COLLABORATIVE SERVICES SUPPORT

Task Order Performance Work Statement (PWS)

PWS Version:	Final FEB 18
Name:	HQ AETC COLLABORATIVE Services Support
Organization:	HQ Air Education & Training Command Support Staff (Clients will be listed in Appendix X)
Locations:	Listed in Appendix X

EXECUTIVE SUMMARY

Headquarters Air Education & Training Command (AETC), Director of Communications & Information (HQ AETC/A6), Director of Integration and Education (A5/8/9), Director of Intelligence, Operations and Nuclear Integration (A2/3/10), Profession of Arms Center of Excellence, Inspector General, Staff Judge Advocate, and 19th Air Force are supported by Collaborative Services (Microsoft SharePoint), the development and sustainment of collaborative applications, and the operation and maintenance of web and database servers in support of the collaborative environment

These services are required due to AETC's lack of in-house capabilities to sustain the existing environment and provide support for legacy applications and new develop initiatives

1. PURPOSE

To provide HQ AETC/A6 with Software Engineer & Database Administration services to support Collaborative Services (Microsoft SharePoint), development for AETC Information Technology Service Provider operations supporting the AETC user community.

2. SCOPE

The contractor will provide proactive, high quality personnel that have the ability to provide software engineering and database administration services to include: Systems operations, systems development, application development (to include cloud platforms and mobile application platforms), deployment, migration, integration sustainment, web services, service lifecycle management, data stores, information exposure services, systems operations, systems engineering, architecture and system design, configuration management and systems Information Assurance (IA) support. This support will provide contracted IT support to AETC/A6 to improve ability to replenish the Air Force's Combat Capability through the efficient and effective use of Information Technology (IT). Systems and applications are hosted on the Non-Secure Internet Protocol Router network (NIPR), Secure Internet Protocol Router (SIPR) network, and on Government own or contracted commercial clouds (accessed from the NIPR network).

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

The contractor (software engineers) shall analyze AETC business requirements, design solutions (desktop, cloud, and mobile), and ensure successful project delivery and overall client satisfaction. The contractor will be involved with customization and documentation management through Microsoft Office SharePoint Server, .NET, enabling partners and clients to easily share information. The contractor shall be responsible for design and approach from the technology perspective; and also for the development and maintenance of the required applications to allow for changes and future initiatives.

The contractor will utilize the .NET Framework, programming languages including C#, Visual Basic, ASP, XML, XSLT, HTML, DHTML, VBScript, JavaScript, Cascading Style Sheets, CAML, and libraries including jQuery, Node, and Vue. The contractor will create and maintain applications supporting a maximum of 100,000 concurrent users. Authorized platforms and tools include Windows Server, SharePoint, SQL Server, Visual Studio, SharePoint Designer, Android, and iOS. The contractor will provide customer support and training.

3.1 Application Sustainment

The contractor shall design, develop, test and package applications and software changes as well as provide problem resolutions for existing applications identified Appendix 2. The contractor shall maintain the current baseline of the application and provide software change and problem fixes to these baselines as required. The contractor shall provide to the AETC CSS all developed, modified, or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to develop each approved systems change request. Specific tasks include the following:

3.1.1 Maintain existing applications and environments as listed in Appendix 2 in accordance with (IAW) disciplined engineering practices and sustain applications, databases, and interfaces in compliance with applicable AF/DoD standards.

3.1.2 Support application sustainment activities to include maintaining existing legacy applications, databases, interfaces and environments listed in support of applications listed in Appendix 2 and in support of AETC enterprise architecture.

3.1.3 Provide application administration and operation services to support, maintain, and operate applications or services.

3.2 Application Development, Migration, and Integration

3.2.1 Utilize waterfall and/or agile software development methodologies to develop mobile applications and web applications hosted locally and in the cloud.

3.2.2 Incorporate access controls including database access control lists and SharePoint user security groups and permissions

3.2.3 Integrate security protections to mitigate vulnerabilities according to applicable Security Technical Implementation Guides (STIGs).

3.2.4 Test contractor-developed software utilizing user testing, test cases, and/or automated test suites.

3.2.5 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.

3.2.6 Utilize government provided Commercial-Off-The-Shelf (COTS) tools for systems design and development.

3.3 Web Services

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

3.4 Service Lifecycle Management

Generate design and implementation artifacts that will support lifecycle management, defined as service development, testing, certification, registration and sustainment as determined by the service manager.

3.5. Data Stores

3.5.1 Support and sustain AETC Collaborative environment and applications outlined in Appendix 2, and development of new applications by:

> 3.5.1.1 The creation and maintenance of data stores
>
> 3.5.1.2 Providing data cleansing, redundancy resolution, and business rule validation services
>
> 3.5.1.3 Monitoring and maintaining these data stores to ensure data availability, accuracy, precision, and responsiveness.

3.6. Information Services.

3.6.1 Provide information services.

3.6.1.1 Transform data for export to target data schema through manual (e.g. scrubbing in Excel) or automated processes.

3.6.1.2 Modify the information source's interface, data, and/or behavior for standardized accessibility.

3.6.1.3 Transform communication interfaces, data structures and program semantic alignment.

3.6.1.4 Provide standardized communication/program wrapping services, data language translation.

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

3.7. Systems Operations

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

3.7.1. Database Development

3.7.1.1 Create database schema, stored procedures, triggers and other database development services.

3.7.1.2 Development of data exposure services with engagement of the database.

3.7.2. Systems Administration

3.7.2.1 Install, support, and maintain computer systems.

3.7.2.2 Plan and respond to service outages.

3.7.2.3 Diagnose software and hardware failures to resolution.

3.7.2.4 Implement and ensure security preventive measures are fully functioning.

3.7.2.5 Monitor and enhance system performance.

3.7.3 Customer Support

3.7.3.1 Provide customer support as it relates to hardware and software supporting Collaborative Services to include second tier and third tier support for technical assistance, order processing, support of multiple software versions, training, warranty, and maintenance, during core duty hours. The contractor shall field calls/emails/inquiries and address them accordingly.

3.7.3.1.1 Tier two is basic application software and/or hardware support

3.7.3.1.2 Tier three is more complex support on application software and/or hardware.

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 in accordance with AFI 63-1201, *Life Cycle Systems Engineering*.

4.1.2. Systems Engineering Process (SEP)

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

4.1.3. Service Development and Delivery Process (SDDP)

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

4.2. Architecture and System Design.

The contractor shall support the design and development of systems and applications business/functional requirements leveraging existing research, prototyping efforts, and proof-of-concepts to assist their integration into the overarching enterprise architecture. The contractor shall create custom Web parts for required site elements using C#, VB.Net, ASP.Net. The contractor shall maintain developed software, updating as needed to satisfy requirement changes and future initiatives. The contractor shall translate user interface, business requirements into implementation plan.

4.2.1 Department of Defense Architectural Framework (DoDAF) Guidance

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

4.2.2. Encryption Mandates

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

4.2.3. 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. CM activities include baseline identification, change control, status accounting, and auditing.

4.4. Testing

The contractor shall design procedures for testing and implementing new applications in the database environment. The contractor shall code, test and install software components. The contractor shall conduct rapid testing and deployment of Core Data Services and Aggregation and Presentation Layer Services using distributed testing environments. The contractor shall develop dynamic testing environments to support Certification and Accreditation (C&A) and functional testing.

4.4.1 Product/System Integration Testing

The contractor shall perform testing and inspections of all system services and applications to ensure the technical adequacy and accuracy of all work, including reports and other documents required in support of that work.

4.4.1.1 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.

4.4.1.2 Testing shall be performed in two steps: operational testing, then system acceptance testing. The contractor shall provide a logical test process that minimized interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing.

4.5. Information Assurance

The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including:

4.5.1 DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M;

4.5.2 Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

4.5.3 Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

4.5.4 Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

4.5.5 In the event there is an error in any AFIs, DoDI's etc., in this PWS, the latest version found at http://www.e-publishing.af.mil/ shall apply.

4.6. System IA

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

4.6.1. 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.

4.6.2 Personnel IA

Personnel performing Information Assurance (IA) activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with DoD 8570.01-M *Information Assurance Workforce Improvement Program*, 19 December 2005, Incorporating Change 4, 11/10/2015, and as stipulated in Section H, Clause H101 of the overarching Application Services RFP.

5. CONTRACTUAL REQUIREMENTS

5.1. Place of Performance

Joint Base San Antonio - Randolph (Randolph AFB), Texas. Telecommuting is permissible at the discretion of the work center supervisor and Contracting Officer Representative (COR). Telecommuting must occur during the same business hours as the work center.

5.3 Normal Hours of Operation

The workweek is 40 hours. The workday is eight (8) hours and the window in which those eight (8) hours may be scheduled is between 6:00 AM and 6:00 PM, Monday through Friday except for days listed in Clause G021, Contract Holidays, in the overarching ID/IQ contract. In the event that an occasional special project may occur, the contractor shall be required to work beyond the normal duty hours stated herein if required by the COR. Alternate working hours or schedule adjustments can be accomplished if the contractor shall be required to complete special project without any additional payment.

Federal Holidays: HQ AETC follows the Federal Government schedule for holidays provided during each work year. The holidays recognized by the Federal Government are: New Year's Day, Dr. Martin Luther King Jr's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans' Day, Thanksgiving Day, and Christmas Day. Family Days and Down Days do not constitute a Federal Holiday.

5.4 Government Furnished Property

The Government shall furnish or make available facilities identified in Appendix XX, at JBSA-Randolph, TX. Government facilities have been inspected for compliance with Occupational Safety and Health Act (OSHA) and environmental regulations. The facilities are provided "as-is" and the government does not represent the condition, quality, or completeness of the property. However, no hazards have been identified which would prevent normal use of the facilities or for which work-arounds were required. The fact that no such conditions have been identified does not warrant or guarantee that no possible hazard exists, or that work-around procedures will not be necessary or that the facilities as furnished will be adequate to meet the responsibilities of the contractor. The Government shall provide the equipment, materials, and services required for the contractor to perform the tasks in this PWS. 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

Online access to government regulations, specifications, standards, technical manuals, design documentation and task documentation Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the Task Order will be provided to the contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the responsible Government COR upon request or at the end of the Task Order period of performance.

5.5 Government Furnished Services. The Government will provide workspace, office furniture, computer resources, telephones, office supplies, test data, and tools necessary to perform the task. The contractor shall have access to Government regulations, technical manuals, and life cycle/program files.

The contractor shall have access to government regulations, specifications, standards, technical manuals, design documentation, and task documentation.

5.6. Non-Personal Services

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Task Order (TO) Contracting Officer (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. Contractor personnel shall not be directed to attend morale and/or recreational activities (i.e., holiday parties, golf outings, sports days and various social events) by the Government. Since contractor personnel are not government employees, they cannot be granted the same duty time activities as Government employees. Participation should be in accordance with the contractor's policies and compensation system.

5.7. Contractor Identification

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

5.8. Performance Reporting

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

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

5.8.2 The contractor shall deliver a Monthly Performance Report, by the 5th day of the month for the previous month, documenting all tasks including those completed, ongoing and started during the period, issues that arose during the period with impact assessments and solution recommendations, requirement changes with impact assessments as well as total hours worked and funds expended during the period.

5.8.3 Performance standards shall include the contractor's ability to:

a. Provide quality services, products and customer support;
b. Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or services during contract performance period: Emergency/critical, Maintenance/Warranty.
c. Provide satisfactory product repairs or advance replacement, as appropriate;
d. Provide timely and accurate reports within three (3) working days of government request;
e. Respond to the customer's requests for proposals and configuration assistance as identified in each delivery order; and
f. Meet subcontracting goals.

5.8.4 The contractor shall notify in writing within 24 hours any personnel changes concerning staffing, qualifications, security clearances and certifications that impact the contractor’s ability to execute/perform responsibilities or meet all requirements as outlined in this PWS.

5.8.5 The contractor shall attend program reviews monthly to present the Monthly Performance Report.

5.8.6 The contractor shall produce and deliver meeting minutes for any meeting attended, except for the Monthly Program Review Meeting, within 5 business days after the meeting has occurred.

5.9. Program Management / Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to. The Program Manager or Project Manager shall be identified in writing and sent to the CO and COR, via email, within 5 calendar days after contract award.

5.9.1. 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.

5.9.2. Management

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

5.9.3 Quality Control

5.9.3.1 General Guidance. Only the Contracting Officer’s Representative (COR) or the designated alternate COR has the authority to inspect, accept, or reject all deliverables. The COR will review all written deliverables for accuracy and completeness within five (5) working days. The contractor shall have five (5) working days to finalize and resubmit deliverables. The COR will have up to five (5) working days to accept or reject final deliverables.

5.9.3.2 Contractor's Quality Control Plan (QCP) The contractor shall develop and maintain a Quality Control Plan (QCP) to identify, prevent and correct any deficiencies for all services set forth in this PWS and shall assure the requirements of the task order are provided as specified. The contractor shall provide one copy of the QCP to the CO for review and acceptance within 15 calendar days after contract award. The CO shall notify the Contractor of acceptance or required changes to the plan. Changes to the plan during contract performance shall be submitted to the CO for acceptance not later than 10 calendar days prior to any change being affected by the contractor. The contractor shall perform all inspections and verifications necessary to substantiate conformance with the plan. The contractor's quality inspection documentation (i.e. metrics, reports, etc.) shall be made available to the COR upon request. The reports should provide information on the methods of inspection, what was inspected, discrepancies found and actions taken to correct and preclude recurrence.

5.9.3.3 Quality Assurance. The government is responsible for evaluating the contractor's performance. For those tasks listed on the Service Delivery Summary (SDS), the COR shall follow the methods of surveillance specified in the Quality Assurance Surveillance Plan (QASP). The COR shall record all surveillance observations. COR surveillance of tasks not listed in the SDS or by methods other than those listed in the SDS may occur during the performance period of this contract on an as needed basis.

5.9.3.4 Quality Meetings. The CO may require the contractor to meet with the CO, contract administrator (CA), COR, and other government personnel as deemed necessary. The contractor may request a meeting with the CO when he or she believes such a meeting is necessary. Written minutes of any such meetings shall be recorded by the COR. A copy of the minutes shall be sent to all attendees via e-mail for their review. A copy of all recorded minutes shall be provided to the contractor, and a copy shall be placed in the official contract file for record keeping purposes. In the event the contractor does not concur with any portion of the minutes, exceptions to the minutes shall be provided, in writing, to the CO within 10 working days following receipt of the minutes. Final resolution to exceptions taken by the contractor resides with the CO.

5.9.4. Records, Files, and Documents

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

5.9.5. Personnel Security

5.9.5.1. For this Performance Work Statement, the highest level of security required is Secret (S). Secret clearances will be required to meet the minimum requirements of all projects. All contract personnel who will be assigned to the contract in capacities that require access to background and reference materials will be required to possess at least a SECRET clearance. Specific security requirements are identified in the DD Form 254, Department of Defense Contract Security Classification Specification. The contractor will comply with DOD 5200.2-R, Personnel Security Program, and AF33-152, User Responsibilities and Guidance for Information Systems requirements for contract personnel operating Government Workstations that have unclassified automated information systems (e.g., e-mail and Internet). Contract personnel will possess and be able to maintain favorable National Agency Check with Local Checks (NACLC) in order to meet the minimum requirements of the project. Contract personnel receiving unfavorable NACLCS will not be allowed to perform on the project. These investigations will be conducted by the Government and the results provided to the contractor at no additional cost to the contractor. Performance under this PWS may generate Government proprietary data categorized as "for official use only" or protected under the Privacy Act of 1974. Contract personnel, although recognized as contractor employees and under the complete control of the contractor, will be required to comply with directives and requirements of the base commander or authorized representative as to security standards and regulations applicable to the work site. Contract personnel involved in crimes and/or other incidents of misconduct may be barred from the base by the base commander. The contractor will inform the Contracting Officer of any information they have relating to crimes committed by the contractor employee. The contractor will comply with DoD Standard 22 - Level 1 AT Antiterrorism Training (AT) Awareness training and associated tasking IAW AFI 10-245, Antiterrorism Program standards.

5.9.5.2. Anti-Terrorism Training

5.9.5.2.1 In accordance with DoDM 5200.01 volumes 1-4, and AFI 16-1404, Information Security, the contractor shall comply with AFSSI 7700, Emission Security (EMSEC) Program. The contractor shall also comply with AFMAN 33-152, User Responsibilities and Guidance for Information Systems; AFI 17-130, *Cybersecurity Program Management*; applicable AFKAGs, AFIs, and AFSSIs for Communication Security (COMSEC); and AFI 10-701, Operations Security (OPSEC). Additionally, the contractor will comply with DoD Standard 22/Force Protection Condition Measures, DoD Standard 25/Level I-AT Awareness Training, and associated tasking contained in AFI 10-245, Antiterrorism (AT) standards. Level I AT Awareness training is available for contractor personnel. In addition, there is an online antiterrorism level 1 training course which can be taken by employees: http://jko.jten.mil/courses/atl1/launch.html

5.9.5.3. Visitor Group Security Agreement (VGSA). The contractor shall enter into a long-term visitor group security agreement if service performance is on base. This agreement shall outline how the contractor integrates security requirements for service operations with the Air Force to ensure effective and economical operation on the installation. The agreement shall include:

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

5.9.5.3.2 Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

5.9.5.3.3 On base, the long-term visitor group security agreement may take the place of a Standard Practice Procedure (SPP).

5.9.5.4 Obtaining and Retrieving Identification Media. As prescribed by the AFFAR 5352.242-9000, Contractor access to Air Force installations, the contractor shall comply with the following requirements:

5.9.5.4.1 The contractor shall obtain base identification and vehicle passes for all contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished identification badges while visiting or performing work on the installation.

5.9.5.4.2 No later than three working days prior to contract commencement, the contractor shall submit a written request on company letterhead to the COR listing the following: contract number, location of work site, start and stop dates, and names of contractor employees needing access to the base. The authorized Unit Security Manager will endorse the request and forward it to the issuing base pass and registration office or security forces for processing. Contractors will present government (state or federal) issued ID, and INS Form 9 (I9), before being issued a pass to enter the installation. Before being issued a pass to enter the installation, a Wants and Warrants check will be conducted for every individual requesting a pass. Personnel employed by the contractor must get a pass for their privately owned vehicles at Visitor Reception Center, with proof of following:

(1) Liability Insurance
(2) Current License Plates
(3) Current State Inspection Sticker (If Required)
(4) Valid State Driver License
(5) A phone number for sponsor on base

5.9.5.4.3 Vehicles owned by the contractor with the company name permanently printed on them are not required to obtain a pass as long as a current work order is presented at the time of entry. However, current liability insurance, state inspection sticker, and registration is required. The person driving the vehicle must have a valid operator license for the type of vehicle.

5.9.5.4.4 The contractor is responsible for ensuring employees report to the Visitor Reception Center, to present their Form I-9 (Employment Eligibility Verification).

5.9.5.4.5 Upon completion or termination of the contract or expiration of the identification passes, the contractor shall ensure that all base identification credentials issued to contractor employees are returned to the issuing office. If a contractor employee has been terminated, the credentials will need to be retrieved and returned to issuing activity so that employee does not have base access. If the credential is not retrieved then SF will need to be notified so base access is not allowed.

5.9.5.4.6 Failure to comply with these requirements may result in withholding of final payment.

5.9.5.5 Pass and Identification Items. The contractor shall ensure the following pass and identification items required for service performance are obtained for employees and non-government owned vehicles:

5.9.5.5.1 Installation Access Pass (IAP) (DBIDS), Visitor/Vehicle Pass (AFMAN 31-116), used for contracts for less than six months to include one-day visits (i.e. warranty work).

5.9.5.5.2 Installation Access Card (IAC) (DBIDS), (AFI 31-113), used for contracts for more than six months or more.

5.9.5.5.3 DoD Common Access Card (CAC), (AFI 36-3026), used for contracts for more than six months and requirement exists for access to the government computer systems and software. CAC applications are accomplished by Trusted Agents via the Contractor Verification System (CVS).

5.9.5.6 Security Clearance Requirements. The contractor must possess or obtain an appropriate facility security clearance (Secret) prior to performing work on a classified government contract. If the contractor does not possess a facility clearance the government will request one. The contractor shall request personnel security clearances (minimum of a NACLC investigation), at the company's expense, for employees requiring access to classified information within 15 business days after receiving a facility clearance or, if the contractor is already cleared, within 15 business days after service award. Due to costs involved with security investigations, requests for personnel security clearances shall be kept to the minimum amount employees required to perform contract requirements.

5.9.5.7 Listing of Employees. The contractor shall maintain a current listing of employees. The list shall include employee's name, social security number, and level of security clearance. The list shall be validated and signed by the company Facility Security Officer (FSO) and provided to the contracting officer and Information Security Program Manager (ISPM) at each performance site 30 days prior to the service start date. Updated listings shall be provided when an employee's status or information changes. A Visit Request for all employees with security clearances is required to be sent through the Joint Personnel Adjudication System (JPAS). The contractor shall notify the (ISPM) at each operating location 30 days before on-base performance of the service. The notification shall include:

a. Name, address, and telephone number of company representatives.
b. The contract number and contracting agency.
c. The highest level of classified information to which contractor employees require access.
d. The location(s) of service performance and future performance, if known.
e. The date service performance begins.
f. Any change to information previously provided under this paragraph.

5.9.5.8 Suitability Investigations. Contractor personnel not requiring access to classified shall successfully complete, as a minimum, a National Agency Check with Inquiries (NACI), before operating government furnished workstations. The contractor shall comply with the DoD 5200.2-R, Personnel Security Program, AFMAN 33-152, User Responsibilities and Guidance for Information Systems, and AFI 33-200, Information Assurance (IA) Management, requirements. NACI investigations requests are initiated using the Standard Form (SF) 85 and are submitted to the installation Information Protection Office through the Unit Security Manager. NACI investigations are different from the Wants and Warrants checks, and are provided by the government at no additional cost to the contractor.

5.9.5.9 Entry Procedures to Controlled/Restricted Areas. Contractor personnel requiring unescorted entry to areas designated as controlled or restricted areas by the installation commander shall comply with base access requirements and will possess, as a minimum, a favorable suitability determination. These requirements are contained in AFI 31-101, Integrated Defense, for installation access and AFI 31-501, Personnel Security, for suitability determinations. The contractor shall comply and implement local base procedures for entry to Air Force controlled/restricted areas. For on-base cleared facilities over-sighted by the base ISPM, contractors shall comply with the National Industrial Security Program Operating Manual (NISPOM), previously referred to as the Industrial Security Manual (ISM), to implement controlled/restricted area requirements. The ISPM shall approve the establishment, construction, and modification of all contractor designated controlled areas before they may be used to limit access.

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

5.9.5.11 Additional Security Requirements. In accordance with DoDM 5200.01, Information Security Program and AFI 31-401, the contractor shall comply with AFSSI 7700, Emission Security (EMSEC) Program; applicable AFKAGs, AFIs, and AFSSIs for Communication Security (COMSEC); and AFI 10-701, Operations Security (OPSEC) Instructions. The contractor will comply with DoD Standard 22/Force Protection Condition Measures, DoD Standard 25/Level I-AT Awareness Training, and associated tasking contained in AFI 10-245, Antiterrorism (AT) standards. Level I AT Awareness training is available for contractor personnel and can be requested by calling the local installation AT Office.

5.9.5.12 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, Privacy Act Program, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall remove or destroy official records only in accordance with AFI 33-322 Records Management, or other directives authorized in AFI 33-364, Records Disposition—Procedures and Responsibilities.

5.9.5.13 Reporting Requirements. The contractor shall comply with AFI 71-101, Volume- 1, Criminal Investigations, and Volume-2, Protective Service Matters, requirements. 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.

5.9.5.14 Physical Security. Areas controlled by contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) 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, ground aerospace vehicles, facilities, support equipment, and other valuable materials shall be secured. During increased FPCONs, contractors may have limited access to the installation and should expect entrance delays.

5.9.5.15 Operating Instructions. For controlled areas used exclusively by the contractor, the contractor shall develop an Operating Instruction (OI) for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations. The OI shall be written in accordance with AFI 31-101, the local base Operations Plan usually referred to as an OPLAN and AFI 10-245, Air Force Antiterrorism (AT) Standards, and coordinated through the ISPM.

5.9.5.16 Key Control. The contractor shall establish and implement key control procedures in the Quality Control Plan to ensure keys issued to the contractor by the government are properly safeguarded and not used by unauthorized personnel. The contractor shall not duplicate keys issued by the government. Lost keys shall be reported immediately to the contracting officer. The government replaces lost keys or performs re-keying. The total cost of lost keys, re-keying or lock replacement shall be deducted from the monthly payment due to the contractor. 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 area chief.

5.9.5.17 Lock Combinations. The contractor shall establish procedures in local OIs ensuring lock combinations are not revealed to unauthorized persons and ensure the procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional area chief. Records with written combinations to authorized secure storage containers or Secure Storage Rooms (SSR), shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers. The contractor shall comply with DoD 5200.1-R security requirements for changing combinations to storage containers used to maintain classified materials.

5.9.5.18 Traffic Laws. The contractor and their employees shall comply with base traffic regulations.

5.9.5.19 Healthcare. Contractor may receive emergency medical treatment by calling 911. The clinic at JBSA-Randolph, TX is not equipped to handle emergencies however the base ambulance service will be dispatched. The contractor will be responsible for the cost of services provided by ambulance service and medical treatment facility.

6.0 Safeguarding Classified Information

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in this task order. All Classified Contracts must have at a minimum, the FAR Clause 52.204-2 Security Requirement, incorporated into the contract.

6.1 Protection of System Data

Unless otherwise stated in the task order, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation 5400.7-R and DoD Manual 5200.01to 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.

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 System Authorization Access Report (SAAR), DD Form 2875.

6.3 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 of this task order will not be paid for by the Government or charged to TOs by contractors.

6.3.1 Other Government-Provided Training

The contractor’s employees may participate in other Government provided training, on a nondiscriminatory basis as among contractors, under the following circumstances:

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

6.3.2 Customer Training

The contractor shall provide over the shoulder training, on the job training (OJT) to AETC technicians (government employees). Training will consist of informal and spontaneous assistance on tasks or inquiries related to software development and database administering.

6.4 Organizational Conflict Of Interest

6.4.1 The Contractor shall be cognizant of FAR 9.5, Organizational and Consultant Conflicts of Interest, and FAR 3.101-1, Improper Business Practices and Personal Conflicts of Interest, Standards of Conduct.

6.4.2 If the Contractor prepares, or assists in preparing, a work statement to be used in competitively acquiring a system or services – or provides material leading directly, predictably, and without delay to such a work statement – the Contractor may not supply the system, major components of the system, or the services unless (a) it is the sole source, (b) has participated in the development and design work, or (c) more than one contractor has been involved in preparing the work statement. To overcome the possibility of bias, the Contractor is prohibited from supplying a system or services acquired on the basis of work statements growing out of its services, unless accepted as stated above.

6.4.3 The Contractor may gain access to proprietary information of other companies during contract performance. The Contractor agrees to enter into company-to-company agreements to (a) protect another company's information from unauthorized use or disclosure for as long as it is considered proprietary by the other company and (b) refrain from using the information for any purpose other than that for which it is furnished. The Contractor also agrees to have its employees who will obtain access to proprietary information of other companies while performing on this contract sign nondisclosure agreements agreeing to (a) protect another company's information from unauthorized use or disclosure for as long as it is considered proprietary by the other company and (b) refrain from using the information for any purpose other than that for which it is furnished. For information purposes, the Contractor shall furnish copies of the company-to-company agreements to the Contracting Officer and shall make the individual employee nondisclosure agreements available for the Contracting Officer's review upon request. These agreements are not intended to protect information which is available to the Government or to the Contractor from other sources and furnished voluntarily without restriction.

6.4.4 The contractor, at his discretion, may provide information having direct bearing upon these restrictions to the Contracting Officer for consideration. Final authority for approvals rests with the Contracting Officer.

6.4.5 Government business shall be conducted in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. Transactions relating to the expenditure of public funds require the highest degree of public trust and impeccable standard of conduct. The general rule is to avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-contractor relationships.

6.4.6 Contractors will comply with AETCI 36-2909 and AFI 36-2909, Professional and Unprofessional Relationships, and will take immediate action to resolve violations of the prohibition on unprofessional relationships. Specifically, contractors should understand the following:

> **6.4.6.1** Unprofessional relationships include relationships involving faculty, staff, trainees, cadets, students, recruiters, recruits, applicants, and first-term Airmen who participate in the Recruiter Assistance Program (RAPpers). Whether pursued on or off duty relationships are unprofessional when they detract from the authority of superiors or result in (or reasonably create the appearance of) favoritisms, misuse of office or position, or the abandonment of organizational goals for personal interests. Unprofessional relationships include relationships between officers; between enlisted members; between recruiters and recruits, applicants, or RAPpers; between RAPpers and recruits or applicants; and between military personnel and civilian employees or contractor personnel. Civilian employees and contractor personnel are an integral part of the Air Force. They contribute directly to readiness and mission accomplishment. Consequently, military members of all grades must maintain professional relationships with civilian employees and government contractor personnel, particularly those whom they supervise or direct, and must avoid relationships that adversely affect or reasonably can adversely affect morale, discipline and respect for authority or that violate law or regulation.

6.5 Transition and Decommissioning Plans
The contractor shall coordinate with AETC CSS/SCSK to provide input to transition and decommissioning plans.

6.6 Section 508 of the Rehabilitation Act
The Contractor shall meet the requirements of the Access Board's regulations at 36 CFR Part 1194, 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 (See 36 CFR Part 1194.22).

6.7 Continuation of Essential Contractor Services During Crisis Declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander
The performance of these services are not considered essential contractor services during crisis declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander.

7.0 Services Delivery Summary

The contractor's performance at the contract level will be assessed monthly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary (SDS) will be in accordance with AFI 63-101/20-101, Integrated Life Cycle and Management, AFI 10-601, Capabilities-Based Requirements Development and FAR Subpart 37.6, Performance-Based Acquisition. PWS Paragraph Performance Objectives Performance Threshold

7.1. The Contractor shall design, develop, test and package systems and software changes as well as provide problem resolutions for existing systems. The Contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as required. No more than one (1) violation/discrepancy (milestones/deadlines) per month, and no more than 5 software defects per 1000 lines of code (KLOC) per release.

7.1.1 Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases, and interfaces in compliance with applicable AF/DoD standards. No more than one (1) violation/discrepancy (milestones/deadlines) per month, and no more than 5 software defects per 1000 lines of code (KLOC) per release.

7.1.2 The contractor shall support the design and development of systems and applications business/functional requirements leveraging existing research, prototyping efforts, and proof-of-concepts to assist their integration into the overarching enterprise architecture. The contractor shall create custom Web parts for required site elements using C#, VB.Net, ASP.Net. The contractor shall translate user interface and business requirements into implementation plan. No more than one (1) violation/discrepancy (milestones/deadlines) per month, and no more than 5 software defects per 1000 lines of code (KLOC) per release.

7.1.3 The contractor shall design procedures for testing and implementing new applications in the database environment. The contractor shall code, test and install software components. No more than one (1) violation/discrepancy (milestones/deadlines) per month, and no more than 5 software defects per 1000 lines of code (KLOC) per release.

	Performance Objective	**Performance Threshold**	
Objective No.		PWS Paragraph Reference	Tolerance
1	Provide end-user support for AF procured/authorized hardware, operating system software and applications, and ensure workstations and mobile device environments are operational. Track and process internal trouble tickets submitted by end-users via Email. Trouble tickets submitted to the contractor shall be assessed within four (4) duty hours after notification. Trouble tickets within the contractor's area of responsibility shall be resolved within two (2) business days after notification.	3.1.3.3	No more than two (2) violation/discrepancy occurrences per month.
2	Install government owned software on customer computer resources, and ensure workstations and mobile device environments are operational. Trouble tickets submitted to the contractor shall be assessed within four (4) duty hours after notification. Trouble tickets within the contractor's area of responsibility shall be resolved within two (2) business days after notification.	3.1.3.4	No more than two (2) violation/discrepancy occurrences per month.
3	Coordinate the creation and administration of network user accounts and groups. Submit account creation requests through the Air Force Enterprise Service Desk's Remedy trouble ticket system within one (1) business day after receipt and complete administrative distribution lists and security groups' updates within one (I) business day after notification.	3.1.3.7	No more than two (2) violation/discrepancy occurrences per month.
4	Manage/Assign network user permission and access to file server directories/volumes to provide functional and secure network environment. Respond to network resource requests within one (1) business day after receipt.	3.1.3.12	No more than two (2) violation/discrepancy occurrences per month.
5	Routinely implement software patches, security fixes when requested and also	3.1.3.14.	No more than two (2) violation/discrepancy

	when AFIN automated processes are unable, this includes other tasks assigned by the Air Force Network Operations and Security Centers (AFNOSC) or local network managers on equipment identified as having issues with normal network compliance processes. Test and validate the proper operation and configuration with the appropriate patches and fixes, prior to restoring any device to the network. Contractor shall comply with all TCNO mandates and local base Network Control Center (NCC) guidance in time parameters given.		occurrences per month.
6	Maintain an accurate inventory of all Information Technology Equipment (ITE) assigned to manage for the Directorate by performing a 6 month inspection of 100% of a single equipment category, such as monitors, external drives, printers, etc.	3.1.5.2	No more than two (2) violation/discrepancy occurrences per month.
7	Perform a formal annual (per 502 Base Equipment Control Officer's timeline) physical inventory of 100% of 9 ADPE accounts with approximately 200--225 items currently on each account. NOTE: Inventory is subject to change (increase or decrease 10%-15% depending on the needs of the Directorate).	3.1.5.3	100% - Annual Inventory List will be compared to existing Inventory List that is managed by the COR.

8. DATA DELIVERABLES

The Contractor will deliver one (1) electronic copy of a Contractor's Progress, Status, and Management Report, to include recommendation summarizing results of analysis of requirements, monthly in Microsoft Word format and one (1) electronic copy of any trip report and meeting minutes detailing interactions with other organizations within two weeks of the event, in the Government approved MS Office format, to the CO, COR, and HQ AETC/A6XR. The documents may be transmitted as attachments to an electronic mail message. Unless otherwise specified, the Government will have ten (10) working days for review and comment following receipt of documents. If the Government does not respond within the specified time, the Contractor may assume approval. Upon receipt of Government comments, the Contractor shall revise the document to address the government comments, if needed, and resubmit as final within (5) working days.

8.1 Continuity Book. Contractor shall develop and maintain a continuity book beginning day one of the contract Period of Performance. At a minimum, the continuity book shall include:

8.1.1 User Network Account Creation Documentation

a. System Authorization Access Requests (DD Form 2875)
b. Network User Agreements
c. Virtual Private Network Agreements
d. Privileged User Agreements
e. List of privileged user accounts
f. Information Technology Equipment Account Inventory
g. Base Equipment Control Officer account listings
h. Hand receipts to all directorate/unit customers' equipment users
i. Disposition documentation
j. Hard drive sanitation documentation

8.1.2 The contractor shall submit a monthly Continuity Book Update Report to the COR documenting additions or changes to procedures used to implement and maintain aspects of the, duties and responsibilities, training plan, etc. The contractor shall inform the COR in writing of any additions or changes before implementation.

8.1.3 Monthly Status Report (MSR). The contractor shall submit an MSR due on the 10th day of the month to the Contracting Officer, AETC/A6X, and COR, which outlines all actions taken in support of this PWS. The MSR shall include at a minimum:

8.1.3.1 A narrative description of PWS tasks in paragraph 3.1 and sub-paragraphs describing progress to date, and other information deemed necessary by the contractor or government.

8.1.3.2 Description of all system changes affecting all directorates/units supported and owned IT equipment on both NIPRNet and SIPRNet.

8.1.3.3 A log of end-user submitted software updates, modifications and or software trouble tickets submitted to the contractor via email and phone.

9. APPLICABLE STANDARDS AND REFERENCES

All applicable documents and standards are referenced in specific paragraphs of this PWS and listed in Appendix XX.

Air Force Program Executive
Office (AFPEO) Business
Enterprise Systems (BES)
Systems Engineering Process
https://org.eis.afmc.af.mil/sites/754elsg/ES/HIJG/SEP/default.aspx
The Systems Engineering Process is a life cycle management and systems engineering process based on the Defense Acquisition Technology, and Logistics Life Cycle Management System as tailored for Information Technology Systems and the Capability Maturity Model Integrated. It provides common

plans, procedures, checklists, forms, and templates that support system life cycle management and systems engineering processes.
AFI 10-601, Capabilities-Based Requirements Development
http://www.epublishing.af.mil/shared/media/epubs/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, Acquisition and Sustainment Life Cycle Management
http://www.af.mil/shared/media/epubs/AFI63-101.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 63-1201, Life Cycle Systems Engineering
http://www.epublishing.af.mil/shared/media/epubs/afi63-1201.pdf
It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost effective products and systems that are operationally safe, suitable, and effective. Federal Desktop Core Configuration (FDCC)
http://nvd.nist.gov/fdcc/index.cfm
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. ICD 503, IT Systems Security, Risk Management, Certification and Accreditation
http://www.dni.gov/electronic_reading_room/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.
DoDD 8500.01E Information Assurance (IA)
http://www.dtic.mil/whs/directives/corres/pdf/850001p.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.
DoDI 8500.2, information Assurance (IA) Implementation
http://www.dtic.mil/whs/directive\s/corres/pdf/850002p.pdf
Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.01E, "Information Assurance."
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management
http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf
Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.
DoD 8570.01-M, Information Assurance Workforce Improvement Program
http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global

Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual.
DoDI 8510.01, Risk Management Framework(RMF) for DoD Information Technology
http://www.acqnotes.com/wp-content/uploads/2016/08/DoDI-8510.01-Risk-Management-Framework-for-DoD-Information-Technology-–-24-May-2016.pdf
Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.

AFI 33-200, Information Assurance
af.mil/shared/media/epubs/AFI33-200.pdf
This AFI provides general Assurance 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://www.epublishing.af.mil/shared/media/epubs/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 System and Guest systems operating on or accessed from the AF-GIG.
Security Technical Implementation Guides (STIGs)
http://iase.disa.mil/stigs/stig/index.html
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.
AFPD 33-3, Information Management
http://www.epublishing.af.mil/shared/media/epubs/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://www.epublishing.af.mil/shared/media/epubs/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.
AFI 33-364, Records Disposition – Procedures and Responsibilities
http://www.epublishing.af.mil/shared/media/epubs/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.
DoDD 5205.02, Operations Security (OPSEC) Program
http://www.fas.org/irp/doddir/dod/d5205_02.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://www.fas.org/irp/doddir/usaf/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.
DoDI 2000.16, Antiterrorism Standards
http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf
Updates policy implementation, responsibilities, and the antiterrorism (AT) standards. This update reorganizes AT standards according to the minimum required elements for an AT program: risk management, planning, training and exercises, resource application, and comprehensive program review.
DoD 5400.7-R, Freedom of Information Act Program
http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf
This Regulation provides policies and procedures for the DoD implementation of the Freedom of Information Act (5 U.S.C. 552, as amended) and DoD Directive 5400.7, and promotes uniformity in the DoD Freedom of Information Act (FOIA) Program.

9.1 Qualifications.

9.1.1 Software Engineer

9.1.1.1 The government prefers that the awarded contractor have at a minimum three to five years of web development experience in developing web applications.

9.1.1.2 The contractor shall have at a minimum two to three years' experience in design and application development using .NET Framework, C# and/or VB .NET, ASP .NET, XML, XSLT, HTML, DHTML, VBScript, JavaScript, Cascading Style sheets, JQuery, and CAML.

9.1.1.3 The contractor shall have at a minimum two to three years' experience in Sequential Query Language (SQL) Server 2005 or later, Database Management, Architecture, Development, SQL Reporting Services, and OLAP cube development.

9.1.1.4 The contractor shall have at a minimum two to three years' experience in design and development of management dashboards, Business Intelligence tools and data visualization tools (i.e. Key Performance Indicators (KPIs)).

9.1.1.5 The contractor shall have at a minimum two to three year's development experience in developing applications for Microsoft Office SharePoint Server (MOSS) 2010 or greater.

9.1.1.6 The contractor shall have at a minimum two to three years' experience using visual studio 2008 or later, SharePoint Designer (most recent government approved version)

9.1.17 Working knowledge of current operating systems, e-mail systems, standard network services and protocols, systems software, automated tools, directory services, transmission media, and all other components comprising network architectures.

9.1.1.8 Knowledge of emerging technologies such as Voice over IP, virtual private networks (VPN), personal digital assistants (PDAs), mobile applications (Android and IoS), Cloud computing, and wireless solutions.

9.1.1.9 Knowledge of security requirements in the DoD and methods to secure Commercial off the Shelf (COTS) products on a DOD network.

9.1.2 Database Administration Manager

9.1.2.1 The contractor at a minimum shall have at award of contract a CompTIA Security + Certified SYO-501 certification and maintain this certification at no cost to the government throughout contract performance.

10.2 Qualifications.

10.2.1 Software Engineer

10.2.1.1 Microsoft Developer

10.2.2 Database Administration Manager

10.2.2.1 The contractor shall have at a minimum knowledge of the Air Force Network Operations and Security Center (NOSC) and Network Control Center (NCC) infrastructure including roles and responsibilities of each function.

10.2.2.2 The contractor shall have knowledge of the Air Force Combat Information Transport System (CITS) program.

10.2.2.3 At a minimum the contractor shall have five years industry experience in a Department of Defense (DoD) or Air Force IT related discipline.

10.2.2.4 The contractor shall have at a minimum a working knowledge of Web Services, InfoPath, WebParts, AJAX, and Active Directory services software.

10.2.2.5 Shall have a working knowledge of 3rd party tools such as K2.net, K2 BlackPearl, Dundas, Infragistics, Notepad++ software platform tools.

10.2.2.6 Shall have a working knowledge of MS Project and MS Excel.

10.2.2.7 Microsoft Certified Engineer

11. Contract Manpower Reporting.

The contractor shall report all contractor related labor hours (to include subcontractor labor hours) and unburdened direct labor dollars required for performance of services provided under this contract. The prime contractor has overall responsibility for ensuring subcontractors enter their respective data. The contractor must completely fill in all required data fields.

11.1 The Contractor Manpower Reporting Application (CMRA) secure data website (http://www.ecmra.mil) is the collection point for this information. Data for Air Force service requirements must be input at the Air Force CMRA link at http://www.ecmra.mil . User manuals are available at the Army CMRA link on the website. Contractors may direct questions to the CMRA help desk.

11.2 Reporting. Reporting inputs will be for the direct labor executed during each Government fiscal year (FY), which runs 1 October through 30 September.

11.2.1 While inputs may be reported any time during the FY, all data for the FY shall be reported no later than 31 October of each calendar year.

11.2.2 Notify the contracting officer via e-mail when all prime contractor and subcontractor input is complete.

11.3 Safeguarding Classified Information.

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operations Manual (NISPOM) and the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the Task Order. All Classified Contracts must have at a minimum, the FAR Clause 52.204-2 Security Requirement, incorporated into the contract.

Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the 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.

11.4 Information Management

11.4.1 Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

11.4.2 Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.

11.4. 3 Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.

11.4.4 Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.

11.4.5 The Government Agency owns the rights to all data/records produced as part of this contract.

11.4.6 The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

11.4.7 Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].

11.4.8 No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

11.4.9 Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

12. Quality Processes

As a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the SEI SCAMPI, a method by an SEI-authorized lead appraiser, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the prime offeror's organizational level performing the contract. If not ISO certified or SEI appraised, acceptable comparable System Engineering processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance. The Government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

Small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must comply with the quality processes requirements. This means that at the time of award and as a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method by an SEI-authorized lead appraiser and must be held at the prime offeror's organizational level performing the contract for the entire performance period of the contract, inclusive of options. Evidence of comparable Systems Engineering (SE) processes will not be accepted.

13. Products Standards and Compliance Requirements

13.1 Information Assurance (IA) Technical Considerations

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

Appendix 1: Software Implementation, Operations and Testing Solutions, Standards & References

Purpose:

The following certifications, specifications, standards, policies and procedures represent documents and standards that may be placed on individual contract task orders. Individual task orders may impose additional standards to those required at the contract level. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant Task Order, such as specific FIPS, NIST, or MIL-Standards. Web links are provided wherever possible.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
1.	AFI 10-208 Air Force Continuity of Operations (COOP) Program.	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-208/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).
2.	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.
3.	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.
4.	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	Records Disposition Procedures
5.	36 CFR Part 1194, Electronic and Information Technology Accessibility Standards	http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title36/36cfr1194_main_02.tpl	The purpose of this part is to implement section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
6.	AFI 63-101/20-101 Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	This publication implements Air Force Policy Directive (AFPD) 63-1/20-1, Integrated Life Cycle Management. This instruction establishes the Integrated Life Cycle Management (ILCM) guidelines and procedures for Air Force (AF) personnel who develop, review, approve, or manage systems, subsystems, end-items, services, and activities (for the purpose of this publication referred to as programs throughout this document) procured under Department of Defense (DoD) Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System.
7.	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 Department of Defense (DoD) Directive (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.
8.	AFMAN 17-1303 Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman17-1303/afman17-1303.pdf	This Air Force Manual (AFMAN) implements Department of Defense (DoD) Directive (DoDD) 8570.01, Information Assurance Training, Certification, and Workforce Management; DoD 8570.01-M, Information Assurance Workforce Improvement Program; Air Force Policy Directive (AFPD) 33-2, Information Assurance Program and Air Force Instruction (AFI) 33-200, Information Assurance Management. This manual applies to Air Force military, civilian and contractor personnel under contract to the DoD who develop, acquire, deliver, use, operate, or manage Air Force information systems.
9.	AFMAN 33-152 User Responsibilities and Guidance for information Systems	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. This manual applies to all Air Force military, civilians, contractor personnel under contract by the Department of Defense (DOD), and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This manual applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		**URL**	**Description**
10.	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 Air Force Manual (AFMAN) implements Executive Order (E.O.) 13103, Computer Software Piracy and Air Force Policy Directives (AFPD) 33-1, Cyberspace Support and supports AFPD 33-2, Information Assurance (IA) Program; AFPD 63-1/20-1, Integrated Life Cycle Management; and AFPD 10-6, Capabilities-Based Planning & Requirements Development. This AFMAN provides the overarching guidance and direction for managing IT hardware and software. The hardware management guidance identifies responsibilities for supporting Air Force (AF) IT hardware (IT assets) and maintaining accountability of Personal Wireless Communications Systems (PWCS) including cellular telephones and pagers. The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS) and AF-unique software acquired/developed by the AF (other than software internal to a weapon system; see AFPD 63-1/20-1, Integrated Life Cycle Management).
11.	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 17-130, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 17-130.
12.	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.
13.	DoDI 8510.01 - DoD Risk Management Framework (RMF) for DoD Information Technology	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). Revised from 2007 version on 12 March 2014.
14.	DoDI 8500.01 – Cyber Security (CS)	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	The purpose of the Defense Cybersecurity program is to ensure that IT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DoD information, and to make choices based on that confidence
15.	DoDI 8551.01 – Ports, Protocols and Services Management	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf	
16.	DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
17.	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
18.	DoDD 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf	This instruction 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.
19.	AFI 17-130, Air Force Cybersecurity Program Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-130/afi17-130.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. Using appropriate levels of protection against threats and vulnerabilities help prevent denial of service, corruption, compromise, fraud, waste, and abuse.
20.	AFI 17-101, Risk Management Framework (Rmf) For Air Force Information Technology (It))	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf	Implements Air Force Policy Directive (AFPD) 17-1, Information Dominance Governance and Management, 12 April 2016, AFPD 33-3, Information Management, 8 September, 2011, DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014, and associated processes outlined on the AF RMF Knowledge Service (KS), for managing the life-cycle cybersecurity risk to Air Force Information Technology (IT) consistent with the Federal Information Security Modernization Act (FISMA) of 2014, DoDI 8500.01, Cybersecurity, 14 March 2014, and DoD Directive 8000.01, Management of the Department of Defense Information Enterprise, 10 February 2009.
21.	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)).
22.	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.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
23.	Air Force Instruction 16-1406, Air Force Industrial Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16.../afi16-1406.pdf	Provides guidance for implementing the National Industrial Security Program and is applicable to AF personnel, the Air National Guard, the Air Force Reserve, and DoD contractors performing under the terms of a properly executed contract and associated visitor group security agreement as determined appropriate by the servicing installation commander.
24.	Air Force Policy Directive 16-14, Security Enterprise Governance	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afpd16-14/afpd16-14.pdf	This directive establishes Air Force policy and responsibilities for the oversight, management and execution of the Air Force Security Enterprise.
25.	DoDI 5220.22-R National Industrial Security Program	www.dtic.mil/whs/directives/corres/pdf/522022p.pdf	Establishes policy and assigns responsibilities for administration of the NISP in accordance with Executive Orders 10865 and 12829 (References (c) and (d)) to ensure that classified information disclosed to industry is properly safeguarded.
26.	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.
~~27.~~	FedRAMP Security Controls for Cloud Service Providers	http://cloud.cio.gov/document/fedramp-security-controls	The attachment at the link contains a listing for the FedRAMP low and moderate baseline security controls, along with additional guidance and requirements for Cloud Service Providers. Those controls, guidance, and requirements are key standards for NetOps vendors to meet for any Cloud-related task orders that might have issues on NetOps.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
~~28.~~	Homeland Security Presidential Directive 12 (HSPD 12)	http://www.dhs.gov/homeland-security-presidential-directive-12	Federal law signed by George Bush that directed promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. NIST has been designated as the approval and testing authority to certify products. FIPS 201 implements this policy.
~~29.~~	ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.dni.gov/files/documents/ICD/ICD_503.pdf	This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation. 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.
~~30.~~	IEEE/EIA 12207.0 Standard for Information Technology	http://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.
31.	DODI 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

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
32.	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.
33.	DODI 8320.02 Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense	http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf	Establishes policies and responsibilities to implement data sharing, in accordance with Department of Defense 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.
34.	Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) 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.
35.	Security Technical Implementation Guides (STIGs) CJCSI 6510.01F Information Assurance (IA) AND Support To Computer Network DEFENSE (CND)	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO is in the process of moving the STIGs towards the use of the NIST Security Content Automation Protocol (S-CAP) in order to be able to “automate” compliance reporting of the STIGs.
36.	NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations	http://disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/NIST-SP80053-SecurityandPrivacyControls.pdf	Guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet requirement FIPS Publication 200.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
37.	CNSSI 4009: National Information Assurance (IA) Glossary	http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf	This revision of CNSSI 4009 incorporates many new terms submitted by the CNSS Membership. Most of the terms from the 2006 version of the Glossary remain, but a number of them have updated definitions in order to remove inconsistencies among the communities.
38.	DoD Instructions, 8500 Series	http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Issuances
39.	NIST SP 800-88, Revision 1: Draft: Guidelines for Media Sanitization	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf	This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.
40.	NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf	This document provides guidelines for a risk-based approach to protecting the confidentiality of PII. The recommendations in this document are intended primarily for U.S. Federal government agencies and those who conduct business on behalf of the agencies, but other organizations may find portions of the publication useful.
41.	NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf	The purpose of this publication is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
42.	Defense Information Systems Agency, the Security Technical Implementation Guide (STIG)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) 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.
43.	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
44.	DoDD 8140.01 Cyberspace Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf	Reissue and renumber DoDD 8570.01 to update and expand establish polices and assigned responsibilities for managing the DoD cyberspace workforce.
45.	Committee on National Security Systems (CNSS) Instruction 1253, Security Categorization And Control Selection For National Security Systems	CNSS Webpage	The Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems, provides all Federal Government departments, agencies, bureaus, and offices with guidance on the first two steps of the Risk Management Framework (RMF), Categorize and Select, for national security systems (NSS).
46.	Department of Defense 5400.7-R DoD Freedom of Information Act (FOIA) Program	DoD 5400.7-R	Provides guidance on the implementation of the Freedom of Information Act, as amended by the “Electronic Freedom of Information Act Amendments of 1996.”

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
47.	Federal Information Processing Standards Publication (FIPS-Pub) 199 Standards for Security Categorization of Federal Information and Information Systems	FIPS Pub 199	FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
48.	NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans	NIST SP 800-53A	The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology.
49.	Air Force Instruction 17-101, Risk Management Framework (RMF) For Air Force Information Technology (IT)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-101/afi17-101.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 17-1, Information Dominance Governance and Management, 12 April 2016, AFPD 33-3, Information Management, 8 September, 2011, DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014, and associated processes outlined on the AF RMF Knowledge Service (KS), for managing the life-cycle cybersecurity risk to Air Force Information Technology (IT) consistent with the Federal Information Security Modernization Act (FISMA) of 2014, DoDI 8500.01, Cybersecurity, 14 March 2014, and DoD Directive 8000.01, Management of the Department of Defense Information Enterprise, 10 February 2009.
50.	Department of Defense (DoD) 5200.2-R, Personnel Security Program	DoD 5200.2-R	Establishes policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense, and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.
51.	Air Force Instruction 10-245 Antiterrorism (AT)	http://static.e-publishing.af.mil/production/1/af_a4/publication/afi10-245/afi10-245.pdf	This instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and Department of Defense Instruction (DoDI) 2000.16, DoD Antiterrorism (AT) Standards.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
52.	Air Force Instruction 10-701 Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf	This publication implements Air Force Policy Directive (AFPD) 10-7, Air Force Information Operations. The reporting requirements in this publication have been assigned Report Control Symbol (RCS) DD-INTEL (A) 2228 in accordance with DoDD 5205.02, DoD Operations Security (OPSEC) Program.
53.	Air Force Instruction 31-101 Integrated Defense (FOUO)	http://static.e-publishing.af.mil/production/1/af_a4/publication/afi31-101/generic_wms.pdf	
54.	Air Force Manual 31-116 Air Force Motor Vehicle Traffic Supervision	http://static.e-publishing.af.mil/production/1/af_a4/publication/afman31-116/afman31-116.pdf	It sets forth Air Force guidance related to the Interservice publication AFI 31-218 (I), Motor Vehicle Traffic Supervision, and provides additional Air Force specific guidance.
55.	Air Force Instruction 31-501 Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi31-501/afi31-501.pdf	It provides guidance for personnel security investigations and clearance needs. Use this instruction with Department of Defense (DOD) Regulation 5200.2-R, DOD Personnel Security Program, January 1987, and Executive Order 12968 —"Access to Classified Information."
56.	Air Force Instruction 33-322 Records Management Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-322/afi33-322.pdf	It establishes roles and assigns responsibilities for the Air Force Records Management Program.
57.	Air Force Instruction 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.
58.	Air Force Instruction 71-101 Vol 1 Criminal Investigations Program	http://static.e-publishing.af.mil/production/1/saf_ig/publication/afi71-101v1/afi71-101v1.pdf	
59.	Air Force Instruction 71-101 Vol 2 Protective Service Matters	http://static.e-publishing.af.mil/production/1/saf_ig/publication/afi71-101v2/afi71-101v2.pdf	This Instruction implements AFPD 71-1, Criminal Investigations and Counterintelligence; DoD Instruction O-2000.22, Designation and Physical Protection of DoD High Risk Personnel (HRP)

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
60.	Department of Defense 5200.1-R Information Security Program	DoD 5200.1-R	This Regulation implements Executive Order 12958 (reference (e)), "Classified National Security Information," and associated OMB directives within the Department of Defense.
61.	Department of Defense 5400.7-R Air Force Supplement AFMAN 33-302 Communications and Information	DoD5400.7-R_AFMAN 33-302	This Air Force Manual (AFMAN) implements DoD Regulation 5400.7-R, DoD Freedom of Information Act Program, and Air Force Policy Directive (AFPD) 33-3, Air Force Information Management.
62.	Air Force Systems Security Instruction 7700 Emission Security	https://cs.eis.af.mil/sites/10060/_layouts/15/osssearchresults.aspx?u=https%3A%2F%2Fcs%2Eeis%2Eaf%2Emil%2Fsites%2F10060&k=afssi%207700	This instruction implements the Emission Security (EMSEC) program as defined in Air Force Policy Directive (AFPD) 33-2, Information Assurance (IA), and its implementing departmental publications. It establishes Air Force IA countermeasures and EMSEC requirements for IA compliance with Committee on National Security Systems (CNSS) Policy No.300, National Policy on Control of Compromising Emanations.
63.	Department of Defense Instruction 2000.16 DoD Antiterrorism (AT) –Contains Standards 22 FPCON Measures and 25 Level I AT Awareness Training	DoD Standard 22	Reissues Reference (a) to update policy implementation, responsibilities, and the antiterrorism (AT) standards for the DoD Components under the authority of Reference (b) for the protection of DoD elements and personnel from acts of terrorism.

Appendix 2: Applications for Sustainment and Further Development

Name
AETC Reorganization
AETC Strategic Planning Dashboard
AETC WORCshop
Commander's Inspection Program
Conference Telephone Operator
Continuous Process Improvement
Education & Training Course Announcements
Fully Integrated Resource Scheduling Tool
Information Technology Service Provider
Information Technology Service Provider - Cybersecurity Workforce Improvement Tracker
Information Technology Service Provider - Document Management System
Interpersonal & Self-Directed Violence
PACE Props
Sexual Assault Prevention & Response
SharePoint Administration Requirements Tool for Apps
Staff Assistant Visit
Studies Registry Program