PERFORMANCE WORK STATEMENT (PWS) FOR

DISTANCE LEARNING

WEB-BASED TRAINING COURSEWARE

DEVELOPMENT & MAINTENANCE

FOR THE

U.S. AIR FORCE, EXPEDITIONARY OPERATIONS SCHOOL (USAF EOS), NJ

(Version 28 Jul 26)

Performance Work Statement (PWS)

Name:	USAF EOS DISTANCE LEARNING WEB-BASED TRAINING COURSEWARE DEVELOPMENT & MAINTENANCE
Organization:	USAF Expeditionary Operations School (USAF EOS)
Address:	5656 Texas Ave Ft Dix, NJ 08640

EXECUTIVE SUMMARY

The USAF Expeditionary Operations School (USAF EOS) is the Air Force's Center of Excellence for advanced mobility and expeditionary combat support training and education. The school offers in-resident and online web-based training courses, graduating over 28,000 students annually. The USAF EOS provides for America's defense by preparing Airmen to survive and operate as an indispensable partner in support of Combatant Commanders across a Joint, Interagency, Intergovernmental, and Multi-national (JIIM) Environment. The USAF EOS is a selectively manned schoolhouse dedicated to educating Air Force and DoD personnel across the full range of expeditionary knowledge and skills. The USAF EOS provides in-residence and distance learning instruction to include operations, transportation, logistics, contingency response, aircrew management, theater C2, intelligence, resiliency, and field-craft skills. In addition to the training mission, the EOS also gathers, refines and disseminates Combat Support Tactics, Techniques, Procedures and Lessons Learned for the USAF. The USAF EOS Currently possesses 26 web-based training courses/products which cover various aspect of meeting Air Force mission requirements. The USAF EOS is seeking an external vendor with Air Force and Air Mobility Command mission subject matter expertise and experience utilizing the Air Force Instruction Development System process to maintain 26 web-based training products and develop new training products in a timely manner to meet mission needs of the US Air Force when new training requirements are requested.

1. PURPOSE

The USAF EOS is tasked with providing training to DoD personnel in numerous Air Force mission requirements and is tasked to provide, maintain and improve online training courseware to meet these mission needs. The contractor will be expected to have the capabilities to

1) convert existing courseware to HTML-5,
2) provide regular updates to existing web-based courseware and
3) to develop storyboards and create new courseware using AF Instructional System Development (ISD) guidelines and information gathered from workshops.

2. SCOPE

2.1 The purpose of this PWS is to provide support for education and training of designated airmen approved by the Air Force. This non-personal services performance work statement (PWS) is to provide maintenance support for web-based courses in support of the Air Force on-line education and training mission.

2.2 Courseware, curriculum, and instruction will be jointly accomplished by the Government and the contractor to meet USAF EOS standards and capable of meeting rapidly changing course requirements, per the direction of the course functional manager. The government takes responsibility for courseware, curriculum, and instruction that is jointly accomplished by the government and the contractor.

2.3 Work under this contract will include updating and maintenance of established web-based courseware, conversion of older courseware to HTML-5, and to develop new courseware from storyboards created from Instructional System Development (ISD) workshops.

2.4 The contractor may be required to participate in (ISD) workshops when new curriculum/courseware needs to be created to meet mission requirements contractors' task will include but is not limited to build storyboard(s), development of courseware, curriculum, and testing assessments in a web-based format.

2.5 The Government anticipates an annual student load of approximately 28,000 students requiring access the web-based training. The average daily student load may be up to 1,500 students with up to 26 training products operating concurrently on the AF Learning Management training website.

3. CONTRACTOR PERSONNEL

The contractor shall employ degreed, professional, technically qualified personnel who possess the necessary experience and knowledge to perform the tasks, meet all technical requirements, and exercise administrative control necessary to meet the requirements outlined in this PWS.

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

This (PWS) contains the following contractor requirements:

4.1 Qualifications

Possess and provides National Institute of Standards and Technology (NIST) 800-53 certification. NIST provides a list of controls that support the development of secure and resilient federal information systems. This catalog of security controls allows federal government agencies the recommended security and privacy controls for federal information systems and organizations to protect against cyber-attacks and is required by many DoD and U.S. Government contracts, in software development. Certification must be current and held for over 12 months.

4.2 Possess Subject Matter Expertise

Provided two (2) samples of previously built Air Force courses in any of the (5) the subject matter areas listed below for evaluation. *Prior courseware produced within last (3 years) in these process areas can be used to qualify SME experience and the expertise to reduce development time.* Must possess knowledge and have previous subject matter experience producing courseware for the following process areas for the US Air Force;

1. Air Mobility Command operations/logistics
2. AMC Aircraft Operations
3. Air Force Cargo and Air Transportation
4. Air Force Command and Control (C2)
5. Air Force Deployment Operations

Must possess staff personnel with knowledge developing courseware from referencing Air Force Technical Orders regarding C-5, C-17, C-130, KC-135, KC-46 aircraft.

Interface with government provided Subject Matter Experts (SMEs) through email, phone or meetings to meet updating requirements and ensure courseware is meeting training objectives and development timelines.

4.3 Possess Instruction System Development (ISD) Expertise

Must be knowledgeable with designing courseware using the Air Force Instructional System Development (ISD) process (AFM 36-2235 volumes 1-10) or Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model.

Utilize ISD processes to create web-based training products, lessons, assessment quizzes and training activities with subject matter experts from the field during workshops or training enhancement request.

If required, attend/facilitate ISD workshops at government facility or contractor location to review and collect source information provided by Subject Matter Experts (SMEs).

Provided (2) course storyboards documentation shall include;

- Course Title
- Course objective
- Lesson titles
- Lesson objective
- Lesson samples of behavior(s)
- Main points
- Identified reference sources
- Voice over statements
- Supporting graphics
- Developer notes

- Test questions that line up with lesson objectives and identify correct answer with student feedback statement

4.4 Possess Technical Support and Expertise

Develop/update courseware listed in (Par 6.1.2) “List of Current Courseware” with Commercial Off-The-Shelf (COTS) software.

Possess high level of proficiency on creating/setting up curriculum, building and setting up assessments and test, setting up classroom curriculum by utilizing the built in functionality on the Moodle Learning Management System.

Possess (5 years) experience troubleshooting and manually updating SCORM packages that will interface with LMS operations, PC desktop, or mobile APP device requirements.

Possess licensed copies and be highly proficient (5 years or more) using the following programming/coding software; Rise 360 Articulate Storyline 360, Articulate Storyline Desktop, Adobe Captivate, Cascading Style Sheets (CSS), JavaScript, and Interactive HTML5 coding.

Produce/update media production resources for courseware creation to include: digital photography, graphic artwork, video production, animation and sound.

Update/develop courseware to have the ability to: read text content from a data file, integrate multiple media types on a single screen, interact with the Learning Management System (LMS) software, and properly function when integrated in various combinations.

Possess experience using the Moodle Learning Management System activity toolsets to creating learning activities such as learning books, quizzes, HP5 content.

Establish version control for course configuration management.

Update/develop courseware standardized template to match the look and operation of existing courseware.

Provide and develop all modules and lesson material to include storyboards (Par 6.2.1) for newly developed courseware.

Provide government access to contractor provided LMS for operational and update quality check for any updated or developed LMS training courseware prior to delivery.

4.5 Meet Required Operational Design Requirements

Courseware interactions to be designed up to the level 3 of moderate interactions level. Courseware updates and developed courses must pass functional testing and meet all system operations requirements per established standard identified below.

- Course Outline Matches Design Document
- Identifies Overall Course Objective
- Identifies Lesson Samples of Behaviors

- Build in Module with multiple Lesson(s) Format
- Multiple Activity-Based (exercises) Training Lessons
- Knowledge Check Questions Throughout Lesson(s)
- Navigation/Glossary/Resources Function
- Student Progress Tracking (bookmarking at lesson level)
- Voice over and or video for covered curriculum

4.5.1 Knowledge Assessment & Final Course Test Design Requirements

There shall be knowledge check assessments in the course lessons where appropriate. These testing interactions will link directly to the lesson samples of behaviors and allow students to know whether they are learning the material as they are taking the training and will not be scored. The final assessment is used to provide a measurement on the students ability to recall the course material to a level of satisfaction to pass the course and will allow for multiple attempts with the ability of the student to know where they are lacking and need to restudy the course material if they do not pass.

.

Knowledge Check Design Requirements

- Allows at least two tries to answer correctly
- Can be locked for students to answer before advancing in training
- Feedback is provided after an incorrect or correct answer is selected

Final Course Test Design Requirements

- Require password to access for training applications requiring proctored testing
- Assessment randomizes questions and answers on each attempt
- Provides completion score to Learning Management System (LMS)
- Provides printable review feedback scoresheet with missed/incorrectly answered areas and students name
- Provides test item analysis information to LMS

4.5.2 PC/Online Product Operation Requirements

- Operates using USAF Standard Desktop Configuration
- Operates in latest versions of Edge, Chrome, Firefox browsers
- PC-Compatible computer/Laptop
- Intel® Core™ i7-6700HQ CPU @ 2.60GHz or Above
- 32G RAM or greater (Windows 10 or higher)
- Graphics card 128 bit color or greater
- 64 Bit or compatible sound card (if sound is required)
- 1Gbps Broadband internet access or higher
- Unity WebGLv1.0 or higher (http://unity3d.com)
- Screen Resolution: 1020 x 800 pixels
- Color Display: 256/32 bit or higher
- Conform to SCORM 1.2 or 2004 compliant for product placement on Learning Management System (LMS)

4.5.3 Meet Standard Coding and Government Requirements

Update training products as outlined in (Par 6.1.2) “List of Current Courseware” that will interface with Moodle LMS operations using SCORM 1.2 and 2004 standards on government PC desktop.

Provided sample courses meet or exceed OPM policies for Training and Development Requirements
http://www.opm.gov/policy-data-oversight/training-and-development

Meet or exceed section 508 standards when developing training products
https://www.access-board.gov/ict/#:~:text=These%20Revised%20508%20Standards%2C%20which,794d)

Provide final courseware products and updates with version control to government (Par 10.6).

Update interactive courseware per the requirements established in the update requirement documentation.

4.6 Skilled Labor Hour Category Duties

Curriculum Designer Manager

Qualifications: Requires a bachelor's degree. Typically reports to a head of department. Typically requires 5 years’ experience in the related area as an individual contributor. 1 - 3 years supervisory experience may be required. Extensive knowledge of the function and department processes.

Duties: Manages the design of training programs, including classroom lectures, online courses, and self-study sessions, directed at employees, organization members, or those who use the organization's products or services. Oversees team of specialists to ensure training and learning needs are addressed in accordance with policy and strategy.

Curriculum Specialist

Qualifications: Requires a bachelor's degree. Typically reports to a Manager. Typically requires 4 to 7 years of related experience.

Duties: Designs training programs, including classroom lectures, online courses, and self-study sessions, directed at employees, organization members, or those who use the organization's products or services. Develops and updates course content and coordinates learning curriculum to reflect learning needs.

Application Developer/Programmer

Qualifications: Requires a bachelor's degree. Typically reports to a manager or head of a unit/department.

Duties: Designs procedures to solve complex application programming problems, taking computer equipment capacity and limitations, operating time, and form of desired results into consideration. Oversees the development or modification of applications programs. Leads all

phases of applications programming. Designs, codes, tests, debugs, and documents applications at the highest levels of complexity. Evaluates applications for quality assurance.

Graphic Designer

Qualifications: Typically requires a bachelor's degree or its equivalent. Must remain abreast of technological advances in the field and be able to identify areas of use in the organization. Typically requires 4 to 7 years of related experience.

Duties: Generates and manipulates graphic images, animations, sound, text and video into consolidated and seamless multimedia programs. Uses knowledge of current graphic design software to produce graphic art and visual materials for promotions, advertisements, films, packaging, and informative and instructional material through a variety of media outlets such as websites and CD-ROMs.

Audio Visual Specialist

Qualifications: May require an associate's degree or its equivalent. Typically requires 1-3 years of related experience or additional training, or certification.

Duties: responsibilities include setting up and adjusting audio-visual equipment, performing routine maintenance, creates and edits audio files, or tapes. Works with producers/directors on design, testing, installation and positioning of equipment and props for live events or meetings.

Project Manager

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/project manager who will oversee all aspects of the requirement. The contractor shall establish and 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 during weekly meetings. 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 requirement efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high-quality delivery. The contractor shall provide transition in and transition out plans as required.

Shall be responsible for the performance of the work under this contract. The name of this person and alternate(s) shall be designated in writing to the CO upon initial assignment and whenever a change in personnel is made.

Have full authority for the contractor and all contractor employees on all matters relating to daily operation of the contract.

If on leave or off station, designate an alternate who is on station and who can assume his/her duties. In this case, the Program Manager will notify the COR.

Ensure government-provided student feedback tools are used in accordance with Expeditionary Operations School established policies and procedures.

Coordinate academic activities with the Dean of Academics, Unit Commander, Director of Operations, Course Director, and COR, and other organizations and customers as appropriate.

Make recommendations to COR on all matters relating to efficient and effective operations of the web based training.

5. PERFORMANCE REQUIREMENTS

5.1 Contractor Management

The Contractor shall perform continual management of the functional areas contained within this PWS and shall provide a Project Manager physically present at the Contractor location during normal duty hours. The Project Manager shall conduct overall management coordination and shall be the central point of contact (POC) with USAF EC for performance of all work under this PWS. A Contractor employee shall be designated to act for the Project Manager when work is being performed outside of duty hours, or during the Project Manager's absence. Both the Project Manager and the Contractor employee filling in for the Project Manager, shall have full authority to act for the contractor on all Contract matters relating to daily operation of this contract.

5.2 Contractor Responsiveness

The Project Manager or designated alternate shall be available for telephone communication or site attendance, with the government POC, as required by the government POC during the hours of 0730 to 16:30 hrs Eastern Standard Time. A personal answering service is permitted at other than normal Contractor workdays and work hours for receipt of callas within a time not to exceed one hour after notification of the call by the answering machine and/or service. The Project Manager and any individuals designated to act in that capacity shall have full authority to contractually bind the Contractor for prompt action on matters pertaining to execution of this PWs.

6. DELIVERABLES

Deliverable include the following.

1) Make updates to existing course (Para 6.1) and meet time requirements (Par 6.1.1)
2) Converting any existing courseware (Para 6.1) to HTML-5
3) Develop story boards and develop new web based courseware meeting all design requirements (Par 4.5 - 4.5.3)

6.1 Updates Existing Courseware

Perform Monthly Updates/ Enhancements/ Critical Bug Fixes as requested by the government on existing courseware. The government will provide detailed descriptions, source documents, and desired outcomes for the requirements for contractor to provided estimate quote for requested services as outline in the weekly status meetings.

Actions related to maintaining and upgrading the courseware include but not limited to the addition of:

1) New reference sources or changes to processes

2) Pictures of new equipment or personnel with current apparel

3) Replacing curriculum (media) with new material

4) Adding scenario into training

5) Correcting operation capabilities in training to operate correctly on LMS or convert courseware to HTML5 format

6.1.1 Existing Course Listing

(this listing is not all inclusive and may change due to course attrition or deletion)

1	AMC Stage Management
2	Aerial Port Vehicles
3	Air Freight
4	Air Terminal Operations Center
5	HARM Fundamentals
6	SARM Fundamentals
7	Data Records Processing
8	GATES M1-Air Terminal Ops Center
9	GATES M2-Cargo Processing
10	GATES M3-Passenger Service
11	Passenger Service Operations
12	Load Planning M1 Fundamentals
13	Load Planning M2 Aircraft Fundamentals
14	Load Planning bi-annual Assessment
15	Hazardous Material Handling
16	AF Fundamental of Expeditionary Mobility Operations
17	Equipment Preparation Introductory
18	Introduction to Expeditionary Site Survey Process
19	CCAF Instructor Preparation Course
20	UDM M1-Basic
21	UDM M2-LOGMOD
22	Customer Service & bi-annual Assessment

23	Aircraft Maintenance Supervision and Production
24	Rapid Global Mobility (I & II)
25	APEX Refresher Assessment C-5
26	APEX Refresher Assessment C-17

6.1.2 Update Timeline Requirement

Meet required timeline established by Contract Officer Representative (COR) for monthly updates based on identified status of update/changes by government. Contractor production requirements must be scalable to perform work on multiple projects at one time based on government needs.

Existing course/project service update request based on status set by COR on needs of mission requirement.		
High Status 1-4 workday completion	Medium Status 5-15 workday completion	Low Status 16-30 workday completion

6.2 New Courseware Development

6.2.1 New Courseware (Storyboards)

The contractor shall support the design and development of systems and applications and their integration into the overarching enterprise architecture. The contractor shall provide all required design and development documents, and supporting architectural documentation, for any frameworks as identified in this PWS. See AFH 36-2235 V5 pg 272 for further guidance.

6.2.2 Course Testing and Feedback Collection

Vendor shall provide access to website or services (Provide Link) that meets requirements below.

- Provide courseware operation testing capability and identifies all version releases (Alfa, Beta)
- Provide capability of capturing government identified user feedback when testing/reviewing courseware
- Identifies version numbers of courseware during development

The Contractor shall deliver several major document or software releases throughout the development phases for approval as detail in the weekly meetings. A description of each release is listed in (Par 6.2.5 through 6.2.9) below. The Contractor shall supply all releases on the Internet for evaluation. All source files used to develop training on (COTS) software to include story boards, and source support media such as videos and graphics shall be provided to the Government at the completion of this PWS requirement.

6.2.3 Interim Deliveries during Development

The Contractor shall design and develop the course modules, as defined in the ISD workshop. The Contractor shall provide an initial “on-line” draft of each course module for Government review, including all course content, graphics, exercises, test questions, and remedial content.

The Contractor shall provide the Government with access to the Contractor’s server so that the Government can review the draft modules, as they will appear over the Internet within an existing Learning Management System or system to allow full functionality of courseware operation. The Contractor shall incorporate into the final course all corrections or updates provided by the Government during this “on-line” review.

6.2.4 Meet Priority and Delivery Schedule

Provide training development storyboards design documents within 30 days after ISD workshop.

Provide access to project management web site for courseware development and maintenance update tracking.

Incorporate government recommendations to the design documents within 5-15 work days of receipt from government.

Meet product development milestone dates established in design document No Later Than (NLT) 7 days past established deadline in design document or final delivery NLT 4 months after initial ISD workshop for each project.

Deliver final courseware files via (Contractor or Government) secure File Transfer Protocol (FTP) system.

Fix identified programming/product errors within 1-5 days after identified by the government during the initial testing review period of 90 business days after delivery.

6.2.5 Design Document Release

When developing new training courseware the design document (story boards IAW AFH 36-2235 V5 pg 272) shall contain a listing of program features, functionality and user interaction algorithms along with the technical approach to convert the existing course/application content to electronic form. All major components and overall product architecture shall be defined. Alfa, Beta and final software release dates shall established based on time to fully develop courseware. The design document will also include milestone dates for completion of training product.

6.2.6 Alpha Software Release

The alpha software is a complete working version of the courseware program with sample content loaded into at least one program area. The menu system shall contain final graphical artwork, buttons and hyper-links. Sample content can be evaluated for usability prior to formatting the remainder of the content for import into the training product. Content will be

evaluated until product meeting requirements as outlined during the weekly meeting. Preferred platform for evaluation shall be on the Contractor's web site.

6.2.7 Beta Software Release

The beta software release is the final test version of the product. The beta software release contains no known errors or omissions with the exception of final narration audio, which shall be imported after any required beta release changes are incorporated. The beta release shall contain the full functionality of the design document with final content loaded into each program area. After evaluation of the beta software release by the COR and SMEs per established milestones, the Contractor shall meet with personnel to resolve any software abnormalities or non-conformance with the design document or operation requirements (Par 4.6-4.8).

6.2.8 Final Software Release

The final software release is the finished product ready for duplication and release to the user base. It contains no known errors or omissions and conforms to the design document and any agreed upon changes that resulted from the beta software release evaluation.

6.2.9 Narration for Final Release

The final release shall include professional voice narration. The Contractor shall quote pricing for professional voice talent. Currently all voice narration shall be in English

6.3 Data Deliverables

The Government reserves the right to review all data deliverables for a period of 60 working days upon receipt of final version of course files through FTP delivery process. No data deliverable will be assumed to be accepted by the Government until the 60-day period has passed, unless the Government explicitly states otherwise. If required, assist with loading courseware on Government-hosted LMS.

Sequence Number	Data Item Description	Title
A016	DI-ILSS-80872	Training Materials
A021	DI-IPSC-81427A	Software Development Plan (SDP)
A040	DI-IPSC-81488	Computer Software Product
A048	DI-MGMT-80227	Contractor's Progress, Status and Management Report

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the Government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed

STINFO regardless of media type, stage of completeness or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers and other data for which the Government shall treat as deliverable

7. MEETINGS

The Contractor shall attend, participate in, and furnish input during:

7.1 Weekly status meetings

These meetings may include but not limited to all milestones, comment and review areas on new courseware development or update maintenance requirements.

7.2 Quarterly status meetings

These meetings will outlining the work accomplished during the last quarter period and problems encountered/anticipated on each training product.

Meeting attendees shall at times include Contractor managerial, supervisory, and other personnel knowledgeable of the subject matter.

8. TRANSFERING COURSEWARE

Course ware files will be transfer to the Contracting Officer Representative (COR) through the Department of Defense Secure Exchange File Exchange (SAFE).

9. CONTRACT PROCESS

9.1 Task Orders. CO will issue task orders NLT 10 working days after notification from COR.

9.2 Travel

Three to five ISD design meetings may be held at the Government facility or Contractor facility or through a teleconference review process on an annual bases. A joint decision will determine which avenue would be appropriate for each project. Contractor personnel may be required to travel in performance of assigned functions consistent with the scope of this PWS. The contractor shall coordinate with the Course Director and submit a request for travel to the CO identifying the purpose, location, dates, personnel (name and title) needed for the travel, and an estimate of total cost(s) to the government (General and Administration expenses should not be included). It will not be unusual for the government to require the contractor to travel on short notice.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed, on a daily basis, the maximum per diem rates in effect at the time of the travel.

Travel will be a cost reimbursable item IAW FAR 31.205-46 and Joint Travel Regulations (JTR) Vol. II, Appendix D, Part III. Five days after completion of travel, the contractor shall submit an invoice via Wide Areas Work Flow (WAWF) with a detailed breakdown of reimbursable travel costs incurred and receipts for all expenses of $75.00 or more.

The Joint Travel Regulations (JTR), while not wholly applicable to Contractors, shall provide the basis for the determination as to what is reasonable and allowable. Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. All necessary travel meeting the above criteria shall be approved in advance by the Contracting Officer. Exceptions to these guidelines shall be approved in advance by the Contracting Officer's Designee. Additional travel may be required for the optional tasks and will be approved and funded as required via Technical Direction Letters. Travel will only be allowed for new course development.

If any travel arrangements cause additional costs to the requirement that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use economy class or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid.

9.3 Place of Performance The place of performance shall be performed at the contractor location. Travel to Government facilities may be required at the request of the Contract Officer Representative (COR). The contractor may be requested by the (COR) to perform work at the (Government) site if the need arises such as attending ISD design meetings to initiate the development of courseware. The contractor may also be provided access to government learning management system (Moodle) to build or load course content.

9.4 Work Statement

A contractor that 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 – that contractor may not supply the system, major components of the system, or the services unless it is (a) 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, contractors are prohibited from supplying a system or services acquired based on work statements growing out of their services, unless waived as stated above.

The above restrictions shall be included in all subcontracts, teaming arrangements, and other agreements calling for performance of work related to this contract, unless excused in writing by the Contracting Officer. The above prohibitions do not apply to developmental work, even if the development was funded under a Government contract IAW FAR 9.505-2(3).

9.5 Billable Hours

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

Provided labor hour cost on requested monthly work performed per course project.

Provided total labor hour cost on requested development project. Government will be invoiced for monthly service hours used per month during development.

9.6 Contractor Identification

When granted access to attending any ISD workshop at the government facility by the COR 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.

9.7 Base Access

If the contractor does not possess a facility clearance the government will request one. The COR will be the point of contact for base access.

9.7.1 Pass and Identification Items

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

1) DoD Common Access Card (AFI 36-3026).
2) Base-specific identification as required by local base and/or building security policies.
3) Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

9.7.2 Computer and Network Access Requirements

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

(X) AIS-II Position - Noncritical-Sensitive Positions. Security Clearance: UNCLASSIFIED

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

( ) AIS-III Position - Nonsensitive Positions. No security clearance required but is a

Trusted Position based on a favorable NACI background investigation. All other positions involved in U.S. Government computer activities.

9.7.3 Reporting Requirements

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

9.7.4 Physical Security

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

9.7.5 Wireless Electronic Devices

The following devices are not allowed in areas where classified information is discussed, briefed or processed: cell phones, camera cell phones, cordless telephones, wireless microphones, wireless keyboards, wireless mice, wireless or Infrared Local Area Networks (LANs). The term *"Area"* above refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed or

processed, wireless pointer/mice devices are allowed for presentations only. This is an acceptable EMSEC risk. All other Personal Electronic Devices, PEDs. All other wireless PEDs not specifically addressed above, that are used for storing, and processing and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed or transmitted.

9.7.6 Operating Instructions

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

9.7.7 Government Authorization

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

9.7.8 Access Lock Combinations

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

9.7.9 Security Combinations

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

9.7.10 Security Alarm Access Codes

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

9.7.11 Freedom of Information Act Program (FOIA)

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

9.7.12 Traffic Laws

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

9.7.13 Cellular Phone Operation Policy

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

9.7.14 Security Education and Training

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

9.7.15 Standards of Performance

9.7.15.1 The contractor shall not employ persons for work on this contract if such employee is identified to the contractor by the Contracting Officer (CO) as a potential threat to the health, safety, security, general well-being, or operational mission of the installation and its population.

9.7.15.2 Contractor employees shall wear appropriate attire with the contractor's name/picture badge, or USAF issued civilian ID with employee's and contractor's name. Contractor employees may remove their ID if participating in instruction requiring physical activity.

9.7.15.3 The contractor shall not employ any person who is an employee of the U.S. Government if employing that person would create a conflict of interest.

9.7.15.4 Contractors will comply with CCAF and EC-established Policies on Professional and Unprofessional Relationships, and will take immediate action to resolve violations of the prohibition on unprofessional relationships.

9.7.15.5 Unprofessional relationships include relationships involving faculty, staff, and students. 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) favoritism, misuse of office or position, or the abandonment of organizational goals for personal interests.

10. QUALITY CONTROL

10.1 Quality Control Plan (QCP)

The contractor shall be responsible for establishing, implementing, and maintaining a current QCP for web based training. The contractor shall submit a QCP with the proposal, which will identify the standards, processes, procedures, and checklists for all tasks performed. The plan shall become a compliance document after evaluation and acceptance by the CO. The contractor shall monitor quality processes and perform technical audits and reviews in accordance with the QCP to verify adherence to organizational standards, processes, and procedures. Changes to the QCP during contract performance shall be submitted to the CO for acceptance not later than 10 calendar days prior to any changes being affected by the contractor.

The QCP will describe, at a minimum, the inspection system used to cover all services listed in the Services Summary (refer to Section 2). The description will include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title and organizational placement of the inspectors. Areas will include, but are not limited to, in-progress training, reviewing documentation, utilizing student critiques, questioning personnel on instructional techniques, review of safety standards and procedures, review of courseware drafts, and review of finalized courseware. The QCP will describe the records to be kept to document inspections and corrective or preventive actions taken.

The QCP shall include a random drug-testing program for all contractor personnel assigned to this contract. The contractor shall notify the CO and COR in the event of a positive drug test on any contractor personnel assigned to this contract at any time during the performance period of this contract. The contractor will provide a quarterly report to the CO and COR with the number of random drug test conducted in the previous quarter.

10.2 The QCP and documentation

Shall be kept and made available to the Government, upon request, throughout the contract performance period and for the period after contract completion until final settlement of any claims under this contract.

10.3 Records, Files, and Documents

All developed and or updated training products, physical records, source 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).

10.4 Protection of System Data & OPSEC Information

Unless otherwise stated in the PWS, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation 5400.7-R and DoD Manual 5200.01(v1-v4) to include latest changes, and applicable service/agency/combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by the contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption. The contractor shall be responsible for safeguarding military information as outlined by the JB MDL Commander. Contractor personnel will not take photographs of military facilities, equipment or personnel unless cleared through the proper channels.

10.5 Software License Management

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

10.6 Transition and Decommissioning Plans

The contractor shall create transition and decommissioning plans that accommodate all of the non-authoritative data sources (non-ADS) interfaces and ensure that necessary capabilities are delivered using approved ADSs.

10.7 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.

10.8 United States Government Configuration Baseline (USGCB)

All services provided under this PWS shall function and be in compliance with the (USGCB).

10.9 Configuration Management

The contractor shall accomplish Configuration Management (CM) activities to maintain accurate identification of current training products. CM activities include baseline identifications during development and version number control for maintenance update completions.

10.10 Information Assurance

The contractor shall ensure that all system or application deliverables outlined in (Par 6) "Deliverables" to meet the requirements of DoD and AF Information Assurance (IA) policy. Furthermore, the contractor shall ensure that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications.

10.11 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.

10.12 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.

10.13 Personnel IA

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

11. GOVERNMENT FURNISHED PROPERTY

None will be provided.

12. 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 Contracting Officers (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. These operating procedures may be superseded by Theater Commander's direction during deployments.

13. PERFORMANCE REPORTING

Surveillance Methods: Surveillance will be accomplished by the COR on a monthly basis using the methods in accordance with (IAW) the Service Summary below. The contractor's 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 areas identified in "Performance Objectives Chart":

1) Provide satisfactory solutions to meet requirements with the necessary customer support.
2) Provide solutions and services that meet or exceed specified performance parameters in.
3) Deliver timely and quality deliverables to include accurate reports and responsive proposals.

4) Ensure solutions to requirements are in compliance with applicable policy and regulation.

14. SERVICE SUMMARY

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

PERFORMANCE OBJECTIVES CHART

SS#	Performance Requirement	PWS Paragraph	Performance Standard	Method of Assessment
New Course Development				
1	Provide design documentation for new course development.	6.2.4	NLT 30 Days after ISD workshop.	100% inspection utilizing monthly QASP performance reporting.
2	Meet product development milestone dates.	6.2.4	Meet established milestones in design document NLT 7 days past milestones or final delivery NLT 4 months after ISD workshop.	100% inspection utilizing monthly QASP performance reporting.
3	Incorporate government recommendations to the design document.	6.2.4	Within 5-15 work days of receipt from government.	100% inspection utilizing monthly QASP performance reporting.
4	Fix identified programming/product errors during the initial testing review period of 90 business days after delivery.	6.2.4	Within 1-5 days after identified by the government.	100% inspection utilizing monthly QASP performance reporting.
Perform Updates for Existing Courses				
5	Meet time requirements for courseware update completion.	6.1.1	High (within 1-4 workdays) Medium within(5-15 workdays) Low within 16-30 workdays) No more than 2 missed requirements per month.	100% inspection utilizing monthly QASP performance reporting.
6	Courseware passes functional testing and meets all system operations requirements per established standard.	4.5 and all sub paragraphs	Software must pass functional testing and meet all system operations requirements Product releases must have no errors.	100% inspection utilizing monthly QASP performance reporting.
7	Attend weekly and quarterly status meetings.	7	Weekly and quarterly review and establish milestones, requirements	100% inspection utilizing monthly QASP performance reporting.

			and comments for each project that requires updates or development.	

15. PERIOD OF PERFORMANCE

The period of performance for the required services shall be one (1) base year from 01 Oct 2026 to 30 Sep 2027 with subsequent four (4) option years as follows:

Base Year: 01 October 2026 to 30 September 2027

Option Year 1: 01 October 2027 to 30 September 2028

Option Year 2: 01 October 2028 to 30 September 2029

Option Year 3: 01 October 2029 to 30 September 2030

Option Year 4: 01 October 2030 to 30 September 2031

16. APPLICABLE STANDARDS AND REFERENCES

The PC online and mobile application courseware shall be designed to operate with the following expected operation system requirements.

Documentation	URL	Description
ENTERPRISE STRATEGY		
DoD CIO Net-Centric Data Strategy	http://dodcio.defense.gov/Portals/0/documents/Net-Centric-Data-Strategy-2003-05-092.pdf	This document describes the Net-Centric Data Strategy for the Department of Defense (DoD), including DoD intelligence agencies and functions. It describes a vision for a net-centric environment and the data goals for achieving that vision. It defines approaches and actions that DoD personnel will have to take as users—whether in a role as consumers and producers of data or as system and application developers.
DoD CIO Net-Centric Services Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf	The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.

Documentation	URL	Description
DODI 8320.02, Data Sharing in a Net-Centric Department of Defense	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832002p.pdf	Establishes policies and responsibilities to implement data sharing, in accordance with DoD Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002.
DoD Discovery Metadata Specification (DDMS)	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf	Visibility, accessibility, and understandability are the high priority goals of the DoD Net-Centric Data Strategy. Of these goals, visibility and discovery are intimately linked. Visibility of a resource is, in a practical sense, useless, if the resource is not easily discoverable. With the express purpose of supporting the visibility goal of the DoD Net-Centric Data Strategy, the DDMS specifies a set of information fields that are to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services.
CJCSI 6211.02D, Defense Information Systems Network Responsibilities	https://www.dtic.mil/home	This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain).
CJCSI 6212.01F, Interoperability and Supportability of Information Technology and National Security Systems	https://www.dtic.mil/home	Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs. Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs and systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment.
Joint Vision 2020	https://www.govinfo.gov/content/pkg/GOVPUB-D5-PURL-LPS5598/pdf/GOVPUB-D5-PURL-LPS5598.pdf	Strategic Guidance: Joint Vision 2020 builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing transformation of America's Armed Forces.
ENTERPRISE ARCHITECTURE		

Documentation	URL	Description
DoD Global Information Grid Architectural Vision	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&Location=U2&doc=GetTRDoc	The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information – the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.
Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework.aspx	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.
AFPD 33-4, Information Technology Governance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-4/afpd33-4.pdf	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.
AFI 33-401, AIR FORCE ARCHITECTING	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.

Documentation	URL	Description
GiG Technical Guidance Federation GIG-F	https://gtg.csd.disa.mil/uam/registration/register	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.
SYSTEMS ENGINEERING		
Business and Enterprise Systems (BES) Process Directory	https://acc.dau.mil/bes	The BES Process Directory (BPD) is a life cycle management and systems engineering process based on the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System; as tailored for Information Technology (IT) systems via the Defense Acquisition Process Model for Incrementally Fielded Software Intensive Programs
AFI 10-601, Capabilities-Based Requirements Development	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.
AFI 63-101, Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	The purpose of this instruction is to implement direction from the Secretary of the Air Force as outlined in Air Force Policy Directive (AFPD) 63-1/20-1, Acquisition and Sustainment Life Cycle Management. The primary mission of the Integrated Life Cycle Management (ILCM) Enterprise is to provide seamless governance, transparency and integration of all aspects of weapons systems acquisition and sustainment management.
AFI 99-103, Capabilities-Based Test and Evaluation	http://static.e-publishing.af.mil/production/1/af_te/publication/afi99-103/afi99-103.pdf	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature sys-tem designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.
DoD Open Technology Development Guidebook		This roadmap outlines a plan to implement Open Technology Development practices, policies and procedures within the DoD.

Documentation	URL	Description
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	http://www.sei.cmu.edu/library/assets/soabest.pdf	This document was developed under the Net-Centric Operations Industry Forum charter to provide industry advisory services to the Department of Defense (DoD), Chief Information Officer (CIO). It presents a list of industry best practices in achieving Service Oriented Architecture (SOA).
INFORMATION ASSURANCE		
ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.dni.gov/files/documents/ICD/ICD_503.pdf	This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.
DoDI 8500.01 Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) Information Assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf	Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.
DoD 8570.01-M, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf	Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual.
DoDI 8510.01,Risk Management Framework (RMF) for DoD Information Technology (IT)	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf	Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).
AFI 33-200, Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-200/afi33-200.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process.
AFI 33-210, AF Certification and Accreditation Program (AFCAP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf	This AFI implements DIACAP for authorizing the operation of Air Force ISs consistent with federal, DoD, and Air Force policies. It is used to ensure IA for all Air Force procured Information Systems, and Guest systems operating on or accessed from the AF-GIG.
Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Documentation	URL	Description
Air Force Guidance Memorandum (AFGM), End-of-Support Software Risk Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afgm2015-33-01/afgm2015-33-01.pdf	This Guidance Memorandum supersedes AFGM 2014-33-03, Microsoft Windows XP End-of-Life, and highlights current policies and SAF/CIO A6 authorities to mitigate cybersecurity vulnerabilities introduced by unsupported software. Compliance with this Memorandum is mandatory.
AFMAN 33-282, COMPUTER SECURITY (COMPUSEC)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-282/afman33-282.pdf	This AFMAN implements Computer Security in support of AFPD 33-2, Information Assurance Program and AFI 33-200, IA Management Computer Security (COMPUSEC) is defined within the IA Portion of AFI 33-200.
AFMAN 33-285, Cybersecurity Workforce Improvement Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-285/afman33-285.pdf	This rewrite identifies cybersecurity baseline certification requirements for the AF cybersecurity workforce; stipulates minimum certification requirements for various cyber roles and risk management positions; sets qualifications criteria; clarifies the cybersecurity-coding position process; and codifies the waiver policy for baseline certification requirements.
DoDI 8540.01, Cross Domain (CD) Policy	http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf	Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) in accordance with the authority in DoD Directive (DoDD) 5144.02
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.
INFORMATION TECHNOLOGY STANDARDS		
Federal Information Processing Standards (FIPS)	http://www.nist.gov/itl/fipscurrent.cfm	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
IEEE/EIA 12207.0, "Standard for Information Technology	http://www.ieee.org/	IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes", is a standard that establishes a common framework for software life cycle process. This standard officially replaced MIL-STD-498 for the development of DoD software systems in May 1998.[1] Other NATO nations may have adopted the standard informally or in parallel with MIL-STD-498.This standard defines a comprehensive set of processes that cover the entire life-cycle of a software system—from the time a concept is made to the retirement of the software. The standard defines a set of processes, which are in turn defined in terms of activities. The activities are broken down into a set of tasks. The processes are defined in three broad categories: Primary Life Cycle Processes, Supporting Life Cycle Processes, and Organizational Life Cycle Processes.
DoDD 8000.01 Management of the Department of Defense Information Enterprise	http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf	Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense

Documentation	URL	Description
AFI 10-208 Air Force Continuity of Operations (COOP) Program	http://www.fas.org/irp/doddir/usaf/afi10-208.pdf	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs); and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).
US Government Configuration Baseline (USGCB)	http://usgcb.nist.gov/	The United States Government Configuration Baseline (USGCB) is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. USGCB continues to be one of the most successful government IT programs aimed at helping to increase security, reduce costs, and accelerate the adoption of new government technologies, while creating a more managed desktop environment.
DoD Mobile Application Strategy	http://www.defense.gov/news/dodmobilitystrategy.pdf	It is intended to align the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from such activities and aligns with efforts composing the Joint Information Environment.
ISO/IEC 20000	http://www.iso.org/iso/home.html	ISO/IEC 20000 is an international standard for IT Service Management (ITSM). It allows IT organizations to ensure the alignment between ITSM processes and their overall organization strategy. It requires the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system (SMS). ISO/IEC 20000 consist of 5 separate documents, ISO/IEC 20000-1 through 20000-5
QUALITY ASSURANCE		
AFPD 33-3, Information Management	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-3/afpd33-3.pdf	This policy directive establishes Air Force policy for the management of information assets (all forms of data and content), across all AF information sources, as both a strategic resource and corporate asset supporting the warfighter during mission and support operations.
AFMAN 33-363, Management of Records	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-363/afman33-363.pdf	This manual implements DoDD 5015.2, *DoD Records Management Program*, and Air Force Policy Directive (AFPD) 33-3, *Information Management*. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.
DoD Instruction 5015.02, DoD Records Management Program	http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf	Establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic
AFI 33-364, Records Disposition – Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management,* by listing program objectives and responsibilities, guiding personnel in disposing of special types of records, retiring or transferring records using staging areas, and retrieving information from inactive records.

Documentation	URL	Description
DoDI 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoDD_523024.pdf	This Directive updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
AFI 61-204, Disseminating Scientific and Technical Information	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi61-204/afi61-204.pdf	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.
AFMAN 33-152 Communications and Information	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-152/afman33-152.pdf	This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*, AFPD 33-2, *Information Assurance (IA) Program*, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities.
AFMAN 33-402 - Service Development and Delivery Process (SDDP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-402/afman33-402.pdf	This Air Force Manual (AFMAN) provides guidance for the definition, design, acquisition, implementation and delivery of Business Mission Area (BMA) capabilities using the Service Development and Delivery Process (SDDP). The SDDP is end user-centric to better align the assistance required by an end user to address a process-based problem across a holistic set of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) solutions. The SDDP details the processes and procedures by which Information Technology (IT) capabilities supporting Air Force (AF) processes are identified, defined, developed and delivered in a way that ensures IT capabilities are necessary, and maximize the potential for successful implementation of IT investments. The SDDP is applicable to large and small scale problems and can be used to implement IT capabilities of all sizes and types.
AFMAN 33-153 Information Technology (IT) Asset Management (ITAM)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afman33-153/afman33-153.pdf	This is a total revision to replace and incorporate Air Force Instruction (AFI) 33-112, Information Technology Hardware Asset Management, and AFI 33-114, Software Management, into a single IT asset management manual. This revision incorporates the PWCS asset management portions of AFI 33-106, Managing High Frequency Radios, Personal Wireless Communications Systems, and the Military Affiliate Radio System, to remove that guidance; and identifies Tiered waiver authorities for unit level compliance items.
DoDD 5205.02E, Operations Security (OPSEC) Program	http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf	Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations.
AFI 10-701, Operations Security (OPSEC)	http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf	This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.

Documentation	URL	Description
DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).
DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf	This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
Section 508 of the Rehabilitation Act of 1973	http://www.opm.gov/html/508-textOfLaw.asp	On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.
DoDI 1100.22 Policy and Procedures For Determining Workforce Mix	http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf	In accordance with the authority in DoD Directive 5124.02, this Instruction establishes policy, assigns responsibilities, and prescribes procedures for determining the appropriate mix of manpower and private sector support. It implements policy established in DoDD 1100.4 and incorporates and cancels DoDI 3020.37. This Instruction provides manpower mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently governmental (IG); commercial (exempt from private sector performance); and commercial (subject to private sector performance). It reconciles and consolidates the definitions and examples of IG from section 306 of title 5, U.S.C.; sections 501 (note), 1115, and 1116 of title 31, U.S.C., Attachment A of OMB Circular A-76; and Subparts 2 and 7.503(c) of the FAR into a set of criteria for Defense-wide use. This Instruction also implements aspects of sections 113, 188(b), 129a, and 2463 of title 10, U.S.C., and reissues and cancels DoDI 1100.22.

Documentation	URL	Description
DoDD 8320.1 Data Administration	https://acc.dau.mil/adl/en-US/33650/file/6823/DoDD83201%20Data%20Admin.pdf	This Instruction applies to the administration and standardization of DoD standard data elements generated within the functional areas of audit and criminal investigations for DoD. It also applies to the administration of DoD standard and non-standard data elements generated, stored, or used by the DoD. Data elements will be administered in ways that provide accurate, reliable, and easily accessible data throughout the DoD, while minimizing cost and redundancy. Data elements will be standardized to meet the requirements for data sharing and interoperability throughout the DoD. Data administration will be encouraged and promoted within the DoD.
AFI 33-332, Air Force Privacy and Civil Liberties Program	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-332/afi33-332.pdf	Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
AFI 31-501, Personnel Security Program Management	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi31-501/afi31-501.pdf	Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5 to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013.
AFI 16-1404, Air Force Information Security Program	http://static.e-publishing.af.mil/production/1/saf_aa/publication/afi16-1404/afi16-1404.pdf	This publication implements Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance; Department of Defense (DoD) Directive 5210.50, Management of Serious Security Incidents Involving Classfied Information, DoD Instruction (DoDI) 5210.02, Access and Dissemination of RD and FRD, DoDI 5210.83, DoD Unclassified Controlled Nuclear Information (UCNI), DoD Manual (DoDM) 5200.01, DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4; and DoDm 5200.45, Instructions for Developing Security Classification Guides.

Documentation	URL	Description
Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	FISMA was enacted as part of the E-Government Act of 2002 to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets," and also to "provide for development and maintenance of minimum controls required to protect Federal information and information systems." FISMA requires Federal agencies to: •designate a Chief Information Officer (CIO), •delegate to the CIO authority to ensure compliance with the requirements imposed by FISMA, •implement an information security program, •report on the adequacy and effectiveness of its information security policies, procedures, and practices, •participate in annual independent evaluations of the information security program and practices, and •develop and maintain an inventory of the agency's major information systems. FISMA requires the Director of the Office of Management and Budget (OMB) to ensure the operation of a central Federal information security incident center. FISMA makes the National Institute of Standards and Technology (NIST) responsible for "developing standards, guidelines, and associated methods and techniques" for information systems used or operated by an agency or contractor, excluding national security systems.
ISO/IEC 19770-2, Software Tagging	http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670	ISO/IEC 19770-2:2009 establishes specifications for tagging software to optimize its identification and management. (http://en.wikipedia.org/wiki/ISO/IEC_19770)
MIL-HDBK-29612-1A	http://www.navair.navy.mil/nawctsd/Resources/Library/Acqguide/296121a.pdf	Provides guidance that can be used by all Services for the preparation of solicitations and evaluation of solicitation responses for training. Emphasis has been placed on reducing costs, promoting commercial products and practices, and promoting the use of the latest technologies.
AF HANDBOOK 36-2235 Instructional System Design (ISD),V1-10	https://www.e-publishing.af.mil/Product-Index/#/?view=org&orgID=10141&catID=1&isForm=false&modID=449&tabID=131	ISD is a systematic, flexible, proven process for determining whether instruction is necessary in a given situation, for defining what instruction is needed, and for ensuring development of effective, cost-efficient instruction.
FAR CLAUSES		

Documentation	URL	Description
DFARS 252.227-7015 Technical Data Commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1079_80393	Provides the Government specific license rights in technical data pertaining to commercial items or processes. DoD may use, modify, reproduce, release, perform, display, or disclose data only within the Government. The data may not be used to manufacture additional quantities of the commercial items and, except for emergency repair or overhaul and for covered Government support contractors, may not be released or disclosed to, or used by, third parties without the contractor's written permission.
DFARS 252.227-7014 Rights in Noncommercial Computer Software	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P683_47378	Guidance on rights in technical data and computer software small business innovation research (SBIR) program.
DFARS 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P1182_92447	Provides requirements for the identification and assertion of technical data.
DFARS 252.227-7013 Rights in Technical Data---Non-commercial Items	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P295_15657	Provides guidelines for rights in technical data on non-commercial items