

Statement of Work
For
SUBMARINE SKILLS-TRAINING NETWORK -
VIRTUAL INTERACTIVE SHIPBOARD INSTRUCTIONAL TRAINER -
UNMANNED AERIAL SYSTEMS TRAINING

1.0 SCOPE

This statement of work (SOW) defines and documents the general requirements to be met via products and capabilities to be delivered under this Submarine Skills-Training Network (SUBSKILLSNET) - Virtual Interactive Shipboard Instructional Tour (VISIT) – Unmanned Aerial Systems (UAS) training Indefinite Delivery-Indefinite Quantity (IDIQ) Contract. The SUBSKILLSNET-VISIT-UAS training and research test bed development effort consists primarily of end item deliverables consisting of data items, including: media, research support products, test and evaluation products, technical documentation, life cycle support products, software integration products, Navy workstation simulation products, and training software products consisting of re-used and expanded SubSkillsNet-VISIT-UAS, research, and related code, libraries, and data. Additionally, as specified under individual delivery orders (DOs), material procurement and integration of hardware with SubSkillsNet, VISIT, and UAS software, life cycle support activities, research support activities, and data collection and analysis activities will be required to directly support product development and research execution. All SubSkillsNet products will run within the SubSkillsNet network environment.

The detailed requirements for products will be defined in a SOW for each specific SUBSKILLSNET-VISIT-UAS DO. Appendix A contains a list of acronyms used in this SOW and their meanings. The Naval Air Warfare Center Training Systems Division (NAWCTSD) anticipates that all future software and software modifications that will be delivered to the Submarine Research Applications Team (SubRAT) laboratory will be placed under this IDIQ Contract.

1.1 Background

The SUBSKILLSNET-VISIT-UAS suite consists of both software and hardware components that are primarily focused on submarine navigation, piloting and contact management; customizable photo-centric spatial awareness training systems (i.e., virtual tours); UAS training; and training research.

SUBSKILLSNET consists of networked software applications that currently include the following list of workstation simulations and capabilities: radars, fathometers, Automatic Identification Systems (AIS), Electrically Suspended Gyro Navigator (ESGN) capabilities, Ring Laser Gyro Navigator (RLGN) capabilities, Global Positioning Systems (GPS), helm controls and displays, image generators (IGs), dynamic bridge views, periscope and photonics simulations, navigation and tactical plots, UAS IGs, and ship's data displays. Additionally, SUBSKILLSNET includes a set of networked software applications that provide instructional capabilities consisting of: scenario authoring, environment authoring, run-time scenario control, instructional exercise configuration, launch and control, three dimensional (3D) model pre-viewing, and student performance monitoring and feedback display. SUBSKILLSNET, VISIT

and UAS also include software interfaces to external simulations, instructor tools, and tactical equipment.

VISIT consists of software capabilities that enable the display of digital spherical photographs, linking of the spherical photographs so that they may be navigated by a user via graphical user interface (GUI), linking of instructional media throughout the tours that may be authored and accessed by the user, and spatial location and multiple choice test authoring and presentation capabilities. VISIT also consists of the software tools required to create and edit new tours and to create, edit and display instructional presentations that incorporate virtual tour components. The current set of virtual tours includes multiple submarine, surface, aviation, Special Forces, and other platforms.

1.2 Method of Tasking

Government requirements issued under the basic IDIQ Contract will be met through individual DOs with a DO SOW containing the requirements for specific tasks relating to training system products. DOs may be issued at any time during contract performance, and will be related generally to tasks outlined in the basic SOW. Additionally, the Government will include a set of data item requirements for the DO in the form of contract data requirements list (CDRL) items.

2.0 APPLICABLE DOCUMENTS

The following documents form a part of this SOW to the extent specified herein. In the event of a conflict between documents referenced herein and the contents of this SOW, the contents of this SOW take precedence. Nothing in this SOW, however, supersedes applicable laws and regulations, unless a specific exemption has been obtained. Additional documents may be defined in each individual DO. Carnegie Mellon (CM)- Software Enterprise Institute (SEI)/Capability Maturity Model Integration (CMMI) documents and points of contact can be found through the website <http://www.stsc.hill.af.mil/index.html>. American National Standards Institute (ANSI) information and documents can be found at website <http://www.ansi.org>. Institute of Electrical and Electronics Engineers (IEEE) information and documents can be found at website <http://www.ieee.org>.

2.1 Government Documents

Department of Defense (DOD) and Department of the Navy (DON) Security and Information Assurance (IA) Instructions, Handbooks, Guides, and Policy Documents:

- a) DODI 8500.2 – Information Assurance (IA) Implementation, dated 6 February 2003
- b) ISA Security Technical Implementation Guide (STIG)
- c) DODI 8510.01 – Information Assurance Certification and Accreditation Process (DIACAP) 28 November 2007
- d) DON DIACAP Handbook (Unnumbered) – DON DOD Information Assurance Certification and Accreditation Process (DIACAP) Handbook series, dated 15 July 2008
- e) DOD 8570.01-M - Information Assurance Workforce Improvement Program dated 19 December 2005 (Incorporating Change 2, dated April 20, 2010)

The preceding documents are downloadable from:

<http://nawctsd.navair.navy.mil/Resources/Library/IA/Index.cfm> and DOD STIGs guides are at <http://iase.disa.mil/>

- f) AIR-4.6.2 In-House Development Process (iDP) - Process Description Document (PDD). This is a NAWCTSD document.

2.2 Non-Government Documents

Unless otherwise noted elsewhere in the document, the latest version of the listed documents shall apply.

CM-SEI CMMI Guidelines for Process Integration and Product Improvement
ISBN 0-321-15496-7

American National Standards Institute (ANSI)/American Society for Quality Control (ASQC)

- a) Quality Management and Quality Assurance Standards - Guidelines for Selection and Use.
- b) Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation, and Servicing.
- c) Quality Systems - Model for Quality Assurance in Production and Installation.
- d) Quality Management and Quality System Elements.

IEEE/Electronic Industries Association (EIA)

- a) IEEE Standard for Distributed Interactive Simulation (DIS, Series 1278)
- b) Industry Implementation of International Standard International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 12207:1995 –
- c) Standard for Information Technology - Software Life Cycle Processes
- d) Common Object Request Broker Architecture, v3.1.1: Part 1: Interfaces; (ISO# 19500-1:2012) Part 2: Interoperability (ISO# 19500-2:2012) ; Part 3: Components (ISO# 19500-3:2012) - <http://www.omg.org/spec/>

High Level Architecture (HLA) Interface Specifications (obtainable by email to HLA@dmsa.mil)

- a) HLA Interface Specification Annex B: C++ API
- b) HLA Interface Specification Version 1.3
- c) HLA Object Model Template Specification (Version 1.3)

d) HLA Rules (Version 1.3)

EWin Library (<http://sourceforge.net/projects/ewin>)

ISO/IEC Technical Report (TR) 29110-5-1-2: 2011 – Software engineering – Lifecycle profiles for Very Small Entities (VSEs): Part 5-2-1: management and engineering guide: Generic profile group: Basic profile

3.0 REQUIREMENTS

3.1 General Requirements

The requirements defined herein form the basis for all work and products delivered to the Government as a part of the contract. This SOW defines the scope of the projects which apply to the contract. The Contractor shall organize, coordinate, and control all program activities under contract to ensure compliance with the contract requirements and delivery of the required products and incidental services. The Contractor shall perform the necessary tasks to implement the requirements of each DO into finished, delivered, and supported products. Requirements to use Government standards and non-Government standards will be addressed as needed in each DO. The Contractor shall possess the capability to analyze, design, develop, modify, test, document, deliver, install, and sustain all SUBSKILLSNET-VISIT-UAS software developed for the Government as defined in DOs. The Contractor shall provide the necessary software design and engineering, computer generated graphics art, 3D modeling, multimedia production, technical documentation, photography and video, testing, research assistance, training analysis, and technical leadership for the efforts specified in DOs. The Contractor shall monitor the progress of all work under the contract and shall report monthly to the Government as specified in paragraph 3.1.7 (Contractor's Progress, Status and Management Report, CDRL B001). This status report shall be compiled into one monthly submission for easy administration. The Contractor shall conform to Government-specified process improvement program practices as specified in paragraph 3.1.6. (Conformity to Specified Process Improvement Program).

3.1.1 Government Property

The Government will provide office space, desk and office supplies necessary to accomplish taskings. The Government will furnish the SubRAT laboratory with equipment (computing, photographic) that will be available to the Contractor for use in developing required products and capabilities to be executed under individual DOs. The listed property [see Attachment X] is representative of the hardware that will be available in the lab for use by the Contractor. It will remain under Government custody and will be maintained by the Government and replaced as needed to meet technical refresh requirements. Software licenses for commercial software will also be maintained by the Government (See paragraph 3.2.4.1.1 for Software Development Languages, Libraries and Tools).

3.1.2 Location of Contractor

The Contractor personnel developing products and capabilities under the contract shall be located in Government-provided space in the NAWCTSD SubRAT laboratory located at 12350 Research Parkway, Orlando, Florida.

3.1.3 System Safety Program

All work shall be conducted in a safe manner and shall comply with Occupational Safety & Health Administration (OSHA) standards. The Contractor shall establish and maintain a System Safety Program (SSP) that ensures Contractor personnel are informed of the hazards associated with their tasking and ensure these personnel understand how to conduct their work in accordance with (IAW) OSHA standards. Work typically occurs in an office environment although as individual DOs require, work may be conducted on Navy vessels, aircraft or on other DOD or DOD-contractor facilities. The objective of the SSP will be to inform and enlist personnel into being active participants in identifying and resolving safety hazards to both personnel and equipment to prevent unsafe incidents.

3.1.4 Hazardous Materials/Environmental Safety Program

The Contractor shall institute an environmental, occupational health, and personnel safety (EOPS) program that meets applicable OSHA and Environmental Protection Agency (EPA) standards for all work performed. The EOPS will ensure Contractor personnel are aware of the dangers of hazardous material endemic to their tasking.

3.1.5 Security

Parts of this program require a security classification level of Secret. The Contractor shall be required to work with classified data that does not exceed the Secret security classification level. In the performance of this contract, the Contractor shall use the secure facility within the SubRAT laboratory for developing and processing classified software and media. All Contractor personnel under the SUBSKILLSNET-VISIT-UAS contract shall have the clearance needed to work on the tasks they are assigned. The Contractor shall comply with all security requirements as identified by the latest revision of the following documents: the DOD Contract Security Classification Specification (DD Form 254), which is executed IAW DOD 5220.22-M and DODI 5200.01. Additional program security requirements shall be identified in each DO as needed.

When on-site at NAWCTSD and during travel, the Contractor shall also adhere to all local security procedures required by the facility. The Contractor shall arrange for security badges and passes ensuring Contractor personnel and Contractor vehicles are granted access to buildings and sites to complete individual DOs. The Common Access Card (CAC) shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. Possible sites include locations listed in paragraph 3.22 (Travel) of this SOW, but are not limited to those locations included.

3.1.5.1 Security Requirements for Classified Programs

The Contractor shall safeguard classified information and meet the security requirements identified in the DD Form 254. The Contractor shall enforce these safeguards throughout the life of the contract, including the transport and delivery phases.

3.1.5.1.1 Operations Security (OPSEC)

The contractor shall deliver an OPSEC Plan IAW the security policy, procedures, and requirements for classified information provided in DOD 5220.22-M and the Operations Security (OPSEC) Plan CDRL A004. If the contractor does not have an established security plan that addresses the protection of classified, proprietary, sensitive, or CUI, the contractor shall prepare

the OPSEC Plan IAW the security policy, procedures, and requirements for classified information provided in DOD 5220.22-M and the Operations Security (OPSEC) Plan CDRL A004. The Contractor shall provide OPSEC protection for classified information, sensitive information, and critical program information IAW the OPSEC Plan. The Contractor shall enforce these safeguards throughout the life of the contract from development through support as required and specified in the individual DO.

3.1.5.1.2 Personnel Security - Background Check (Physical Access to and Working on DOD Installations)

A National Agency Check with Inquiries (NACI) or equivalent national security clearance (e.g. National Agency Check with Local Agency Checks including Credit Check (NACLIC)) shall be required for permanent issuance of the CAC credential. The Government may issue the credential upon favorable return of the Federal Bureau of Investigation's (FBI) fingerprint check, pending final favorable completion of the NACI or equivalent. There shall be no additional NACI or equivalent submission for an individual holding a valid national security clearance. Access to restricted areas, controlled unclassified information (CUI; sensitive information), or Government equipment by Contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NACI (or equivalent) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NACI (or equivalent) shall be conducted and favorably reviewed by the appropriate DOD component, agency, or activity prior to permitting such access. The Contractor shall use the Standard Form 85P (Questionnaire for Public Trust Positions) in order to obtain the CAC and access to CUI. The Contractor shall submit the Standard Form 85P as required and specified for the individual DO.

3.1.5.1.2.1 Government-Issued Personal Identification Credentials

The Contractor and Subcontractor(s) (when applicable) shall account for all forms of U.S. Government-provided identification credentials (CAC or U.S. Government-issued identification badges) issued to the Contractor (or their employees in connection with performance) under the contract. The Contractor shall return such identification credentials to the issuing agency at the earliest of any of the circumstances listed below, unless otherwise determined by the U.S. Government.

- a) When no longer needed for contract performance.
- b) Upon completion of the Contractor employee's employment.
- c) Upon contract completion or termination.

3.1.5.1.3 Information Assurance and Personnel Security Requirements for Accessing Government Information Technology (IT) Systems - Suitability/Positions of Public Trust

The Contractor shall comply with the IA and personnel security requirements for accessing U.S. Government information technology (IT) systems specified in the contract. Contractors requiring access to U.S. Government IT systems will be subject to a background check. The Contractor shall review and become familiar with the suitability factors presented in 5 CFR, 731.202 (b) a requirement for contractor personnel. The NAWCTSD Security Office will verify and authorize personnel.

3.1.5.1.4 Information Security Requirements for Protection of Unclassified DOD Information On Non- DOD Systems

The Contractor shall safeguard unclassified DOD information stored on non-DOD information systems to prevent the loss, misuse, and unauthorized access to or modification of this information. The Contractor shall:

- a) Not process DOD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.
- b) Protect information by no less than one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
- c) Sanitize media (e.g., overwrite) before external release or disposal.
- d) Encrypt the information that has been identified as CUI when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best available encryption technology.
- e) Limit information transfer to Subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.
- f) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS).
- g) Encrypt organizational wireless connections and use encrypted wireless connection, where available, when traveling. When encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using no less than application-provided password protection level encryption.
- h) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.
- i) Not post DOD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).
- j) Provide protection against computer network intrusions and data exfiltration, including no less than the following, unless specifically exempted by the Government:
 - (1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
 - (2) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

- (3) Prompt application of security-relevant software patches, service packs, and hot fixes.
- k) Comply with other current Federal and DOD information protection and reporting requirements for specified categories of information (e.g., critical program information, Personally Identifiable Information (PII), export controlled information) when required by individual DOs.

3.1.5.2 Security Requirements for Unclassified Programs

The security requirements specified herein shall apply to the Contractor and their Subcontractors (if applicable). The Contractor shall comply with applicable on-site security regulations related to facility access and building access. The Contractor shall safeguard U.S. Government CUI IAW the Contractor's established security plan. The Contractor shall enforce these safeguards throughout the life of the contract including the transport and delivery phases and the disposition and storage of CUI at contract completion as required and specified for the individual DO. If the Contractor does not have an established security plan that addresses the protection of proprietary, sensitive, or CUI, the Government will provide a template for the development of an OPSEC Plan. The Contractor shall prepare the OPSEC Plan IAW the CDRL. Regardless of the Contractor's established security plan, the Contractor shall comply with the requirements specified in the following subordinate paragraphs.

3.1.5.2.1 Information Assurance (IA)

Contractor personnel accessing information systems with privilege accounts (i.e., System Administrator, Root Level) shall have the IA training and certification required by DFARS 252.239-7001. The Contractor shall safeguard all unclassified Government proprietary information throughout the life of the contract and shall ensure that software applications delivered to the Government are free from elements that might be detrimental to the secure operation of the resource operating system.

- a) The Contractor shall ensure software products will operate in systems configured with DOD Security Technical Implementation Guides (STIG) and shall comply with the DOD ports, protocols, and services guidance (Available at <http://iase.disa.mil/index2.html>). It is acknowledged that legacy SUBSKILLSNET-VISIT-UAS software is in process of being updated for compliance with this requirement. Existing SUBSKILLSNET-VISIT software will be brought under compliance under individual DOs. All contractor personnel requiring administrative rights to systems shall be certified IA Technical Level I personnel to perform IA duties as required in DOD 8570.01-M/Appendix 3, paragraph AP3.2.6. Certifications shall be made available for government verification. The contractor shall obtain the following to better satisfy program requirements:
 - (1) Security+ certification and enroll in the Continuing Education Program through CompTIA.
 - (2) Training in one of the following Operating Systems – Windows 7, Windows Server 2008, or Linux.
- b) The Contractor shall support Government efforts to design, develop, document, integrate, verify, and deliver a security architecture for trainers and laboratories (e.g., SubRAT Mini-SPAN and SMMTT connected assets) that satisfies the System IA controls as defined in DODI 8500.2 for a Mission Assurance Category III (MAC III),

- classified system. The Contractor shall design, develop, document, integrate, verify, and deliver a security architecture for Government Off-The-Shelf (GOTS) developed Automated Information System (AIS) Software Applications (e.g., SubSkillsNet and VISIT) that satisfies the System IA controls as defined in DODI 8500.2 for a Mission Assurance Category III (MAC III), Sensitive system.
- c) The Contractor shall support Government efforts to design, develop, document, integrate, verify, and deliver a security architecture for GOTS developed AIS Software Applications (e.g., SubSkillsNet and VISIT) that satisfies the System IA controls as defined in DODI 8500.2 for a Mission Assurance Category III (MAC III), Classified system.
 - d) The Contractor shall support Government efforts to design, develop, document, integrate, verify, and deliver a security architecture for GOTS developed AIS Software Applications (e.g., SubSkillsNet and VISIT) that satisfies the System IA controls as defined in DODI 8500.2 for a Mission Assurance Category III (MAC III), sensitive or classified system as appropriate.

3.1.5.2.2 Processing of National Security Information

The Contractor shall use commercial IA and IA-enabled IT products, which have been evaluated and validated, as appropriate, IAW the National Information Assurance Partnership (NIAP) (<http://www.niap-ccevs.org/cc-scheme/vpl/>) or Common Criteria (CC) evaluation and validation scheme (<http://www.commoncriteriaportal.org/public/consumer/>) shall be used to enter, process, store, display, or transmit national security information, to the maximum extent practicable.

3.1.5.2.3 IA requirements for Operating Systems

The Contractor shall support Government efforts to incorporate IA and IA-enabled devices for trainer installation locations (e.g., Mini-SPAN, SMMTT connected assets) that:

- a) Have been validated or are under evaluation by NIAP or CC scheme.
- b) Are configurable IAW applicable DOD STIGs or System and Network Attack Center (SNAC) guides. DOD STIGs and SNAC guides are available at <http://iase.disa.mil/>.
- c) Can incorporate the DOD Information Assurance Vulnerability Management Program (IAVMP) IAW DODI 8500.2.
- d) Are supportable for the expected life cycle of the trainer.

3.1.5.2.4 IA requirements for GOTS developed AIS Software Application Systems

The Contractor shall develop GOTS AIS Software Application Systems (e.g., SubSkillsNet, VISIT) that:

- a) Function with employed IA-Enabled Operating Systems that have been configured IAW the applicable DOD STIGs.
- b) Maintain operational capabilities with managed network control devices and boundary defense mechanisms that have been validated and certified by NIAP (<http://www.niap-ccevs.org/>) or CC evaluation and validation scheme (<http://www.commoncriteriaportal.org/products.html>).
- c) Supports Government efforts to ensure configuration and development IAW the DOD Application Security and Developmental STIG.

3.1.5.2.5 Intrusion Detection

The Contractor shall support Government efforts to incorporate the DOD-approved Host-Based Security System (HBSS) Common Management Agent (CMA, a.k.a ePO agent) software on computers hosting operating systems with functional compatibility. The HBSS CMA software is Government-furnished and available at the following DOD website:

<https://powhatan.iiee.disa.mil/tools/hbss/software/>.

3.1.5.2.6 Virus Protection

The Contractor shall support Government efforts to incorporate the DOD licensed virus protection software available at the following DOD website:

<https://patches.mont.disa.mil/Default.aspx> .

3.1.5.2.7 Application Registration

The Contractor shall support Government efforts to register each version of the AIS Software Application products (e.g., SubSkillsNet, VISIT) in the DON Applications and Database Management System (DADMS).

3.1.5.2.8 Third Party Software

The Contractor shall support Government efforts to ensure that shareware or freeware are not implemented unless compelling circumstances exists, in which case the developer shall evaluate and verify the software is free of malware, back doors, or buffer overflows. If the application relies on third party software products or libraries selected by the developer, the developer shall report the shareware and freeware in the software documentation.

3.1.5.2.9 Database Management System

The Contractor shall configure any Database Management Systems (DBMSs) for the trainer installation locations (e.g., MiniSPAN, SMMTT) and AIS Software Application products IAW the applicable Database STIG.

3.1.5.2.10 Ports, Protocols and Services

The Contractor shall ensure that all ports, protocols, and services for the AIS Software Application products are required, implemented, documented, and registered in the Ports, Protocols, and Services Management (PPSM) central registry IAW DOD Instruction 8551.1, Ports, Protocols, and Services Management.

3.1.5.2.11 Audit Logging

The Contractor shall support Government efforts to incorporate a centralized auditing functionality to consolidate security and audit events from operating systems and host-based security systems. The system(s)' centralized auditing functionality shall provide the means to:

- a) Consolidate audit activity as required by DODI 8500.2, IA control engineering compliance and reporting (ECAR)-3.
- b) View the events using a GUI, sort and filter events, and generate reports.
- c) Export events to a file for a specified period of time, while preserving the integrity of the file.
- d) Import events from its own exported file format for a specified period of time, so that the file is viewable using the GUI.

3.1.5.2.12 Software Management System

The Contractor shall support Government efforts to incorporate a centralized software management system to support updates to the Commercial Item software components used in the trainer (e.g., Mini-SPAN), including anti-virus software.

3.1.5.2.13 Backup Management System

The Contractor shall support Government efforts to incorporate an enterprise-type backup management system that provides the means for the System Administrator to perform back up operations weekly for connected trainer (Mini-SPAN) components from one central location and restore, within time limits prescribed in individual DOs, to its previous state in case of catastrophic failures.

3.1.5.3 IA Certification and Accreditation Support

The Contractor shall support the IA certification process IAW SOW paragraph 3.1.5.2.1 (Information Assurance) and the implementing guidance contained in the DON DIACAP Handbook pertaining to a Platform IT Type accreditation.

3.1.5.4 Software Integrity Testing and Certification

The Contractor shall support Government efforts to test and certify that the trainer application software functions as designed in a properly secured operating system environment and is free of elements that might be detrimental to the secure operation of the resource operating system, as described in DODI 8500.2. The Contractor shall provide a completed Vendor Integrity Statement (VIS) for SubSkillsNet and for VISIT IAW DD254. Commercial Item software does not require a Vendor Integrity Statement. The Contractor shall prepare the Scientific and Technical Reports (Vendor Integrity Statements for Software) IAW the CDRL.

3.1.5.5 IA Compliance

The Contractor shall support Government efforts to test, verify, and document that the security architecture and configuration of the trainer and GOTS developed AIS software applications are in compliance with the security requirements and IA controls identified in DODI 8500.2 for a MAC III, sensitive or classified system. The Contractor shall support Government efforts to test, verify, and document that GOTS developed AIS software applications function on systems that have been configured IAW the DOD STIG commiserate with the deployed, or intended, operating system. The Contractor shall support Government efforts to use DOD-authorized automated assessment tools to perform IA testing (e.g. Retina, Gold Disk), document, verify, and validate each applicable operating system IA configuration. Prior to testing, the Government will provide a list of assessment tools that the Government intends to use during testing. The Contractor shall support Government efforts to document the IA compliance results in the Platform IT (PIT) Risk Approval/AIS DIACAP Certification and Accreditation (C&A) Package. The Contractor shall work with NAWCTSD during coordination efforts with the Designated Accrediting Authority to support NAWCTSD in obtaining a system PIT Risk Approval (PRA) concurrent with delivery of the trainer and an Authorization to Operate (ATO) for the GOTS AIS software applications.

3.1.5.6 Network Devices

On all Government owned lab and trainer assets, the Contractor shall incorporate network switching devices that are equipped with the means to manage ports and that have been validated

and certified by NIAP (<http://www.niap-ccevs.org/>) or Common Criteria (CC) evaluation and validation scheme (<http://www.commoncriteriaportal.org/products.html>) The contractor shall develop procedures to address device administration, as identified by the Government.

3.1.5.7 Application Registration

The Contractor shall register each version of the software application products (e.g., SubSkillsNet, VISIT) in the DON Applications and Database management System (DADMS).

3.1.5.8 Encryption

The Contractor shall incorporate DOD-authorized encryption products in the laboratory and fielded training systems, for data at rest that is stored on mobile computing devices such as laptop computers and personal digital assistants or removable storage media (e.g., CD, DVD, USB flash memory). The cryptography shall be FIPS 140-2 compliant.

3.1.5.9 Recovery of Encrypted Data

The Contractor shall establish a mechanism to ensure encrypted data can be recovered in the event the primary encryption system fails. The Contractor shall document all recovery procedures in the laboratory Battle Binder.

3.1.5.10 IA Vulnerability Management Program (IAVMP)

The Contractor shall incorporate the applicable DOD and DON IAVMP messages issued through developmental testing. The Contractor shall document the unincorporated IAVAs, IA Vulnerability Bulletins (IAVBs), and IA Vulnerability Technical Advisories (IAVTs). The Contractor shall provide justification for each unincorporated IAVMP message (describe the specific negative impact of incorporation). The Contractor shall document the information resulting from this task in the DIACAP C&A package. The Contractor shall document this information in the Plan of Action and Milestones. The Contractor shall use the DOD-authorized assessment tools to perform IAVA compliance validation and verification (e.g., Retina).

3.1.6 Conformity to Specified Process Improvement Program

The Contractor shall participate in developing the Government's process improvement program plans, procedures, and processes. The Contractor shall produce technical data documentation, software development documentation, software engineering documentation, and computer software end item deliverables as prescribed by the Government's process improvement program. In areas not yet brought under the Government's process improvement program, the Contractor shall support development of lab processes consistent with the, "AIR-4.6.2 In-House Development Process (iDP) - Process Description Document (PDD)". Prior to establishment of the in-house development processes, the Contractor shall use established SubRAT laboratory practices and take under advisement Government technical guidance and Government insight into Contractor technical performance, cost and schedule, risk management, program control, product design, development, integration, testing, production, and support for specific DOs. As new plans, procedures, and processes are instituted in the Government's process improvement program, the Contractor shall accept and adapt to these newly established practices. The Contractor shall review emerging processes tailored to the demand of VSEs engaged in software engineering and shall support Government efforts to reduce development inefficiencies and to improve the quality of deliverables (ISO/IEC TR 29110-5-1-2).

3.1.7 Contractor's Progress, Status and Management Report (CPSMR)

The Contractor shall provide a single consolidated CPSMR for all active DOs which shall contain contractually required data (IAW Contractors Progress, Status and Management Report CDRL B001).

3.1.8 Data Preparation and Management

The Contractor shall develop, manage, and deliver all contractually required data as specified in DOs. For software development DOs including computer 3D and two-dimensional (2D) modeling and graphics, and photography and video production, the Contractor shall include CDRL F001 items including digital media of the software and items developed and all required documentation as required by CMMI. The Contractor shall use Microsoft Team Foundation (MSTF) software source control utilities to manage SUBSKILLSNET-VISIT-UAS data.

3.1.9 Quick Reaction Capability for Proposals

The Contractor shall maintain the capability to respond within 30 Government working days to a DO Request for Proposal (RFP).

3.1.10 Schedule Pressures

Many tasks are the result of emergent fleet needs with short delivery timelines. Rapid development of creative solutions demands maximal re-use of existing Government-owned SUBSKILLSNET-VISIT-UAS libraries, code, databases, and data. The majority of the development tasks require a high level of computer software engineering skills and companion sets of skills such as in-depth mathematical knowledge and reasoning. Additionally, most of the development tasks are directly related to navigation systems simulations (e.g., submarines, ships), virtual tours, UAS training, and research test beds.

3.2 Specific Requirements

3.2.1 Post Award Conference (PAC)/Administrative Requirements

The Contractor shall attend a Government-scheduled one (1) day PAC at the Government's facility within 30 days after PAC delivery order award. One important general goal of the conference shall be to establish the framework of the Contractor and Government interaction during the contract's performance period and contract overview. The Contractor's management leads, functional leads, technical leads, and contractual personnel should be in attendance.

3.2.1.1 Software Development Plan (SDP)

The SDP is the key document for any software development activity and will be incorporated into the basic contract when accepted. Vague and high level SDPs will be deemed less acceptable, suggesting a lack of a standard corporate process and uncertainty regarding the appropriate activities, tasks, and techniques to be applied. The SDP may be formatted as desired by the contractor, but must contain the information described by the SDP CDRL A001.

After SDP CDRL has been submitted and approved, the Navy will use the SDP for monitoring progress and providing indications of emerging risks and problems. As a formal CDRL, the SDP will be placed under configuration control, with all changes subject to Navy approval. The SDP should be reevaluated at least once every six (6) months.

3.2.1.1.1 Software Engineering Approach

The Contractor shall define an overall software development approach appropriate for the computer software development products described in the Basic SOW. This approach shall be documented in a Software Development Plan (IAW the Basic Contract CDRL A001; Software Development Plan). The Contractor shall follow this SDP for all computer software to be developed, enhanced, or maintained under this effort.

The SDP shall define the Contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is defined in IEEE/EIA Std. 12207.0. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work contained in this SOW. IAW the framework defined in IEEE/EIA Std. 12207.0, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. IEEE/EIA Std. 12207 does not prescribe how to accomplish the task. The Contractor must provide this detailed information.

The SDP shall contain the information defined by IEEE/EIA Std. 12207.1, Section 5.2.1 (generic content) and the Plans or Procedures in Table 1 of IEEE/EIA Std. 12207.1. The level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must minimally include specific standards, methods, software languages, software and media tools, actions, strategies (e.g., coding and commenting standards) and responsibilities associated with development and qualification. Specific and relevant detail sufficient to clearly illustrate the Contractor's capability to be productive upon contract award shall be provided.

3.2.2 Software Development Products

3.2.2.1 SubRAT Products

This paragraph contains a representative list of products and capabilities likely to be delivered and activities to be performed under this contract as requirements emerge. The Contractor shall execute tasks and subtasks required to deliver products as specified under individual DOs and as generally described in paragraph 3.2.2.2.1 (Software Engineering Approach). Software products/capabilities will be delivered IAW the Basic Contract CDRL A002 (Computer Software Product).

- a) Design, develop, re-use, modify, expand, interface, and add SUBSKILLSNET-VISIT-UAS training and research software libraries, code and media, including:
 - (1) Networked real-time workstation simulations and displays and instructor support software applications.
 - (2) Image generators for simulation-based training.
 - (3) VISIT immersive photography-based training system products.
 - (4) Windows software using the SubRAT's Government-owned GUI framework library, Visual Studio C++ under Windows XP and Windows 7.
 - (5) Linux software (using Red Hat and CentOS) using Wine and other Linux based libraries.
 - (6) SubRAT's Government-owned networked simulation library and Instructor Interface.

- (7) Software interfaces to other simulators and tactical software systems.
- (8) UAS Common Control System prototype.
- (9) Training research transition test beds.
- b) Design and develop digital media, including computer generated 2D and 3D models, animations, photography, videography, sound effects, and scripts in required formats as specified in individual DOs to support:
 - (1) Workstation simulation GUIs
 - (2) Environmental effects
 - (3) SUBSKILLSNET gaming areas, vessels, and environmental features (.e.g., water towers)
 - (4) VISIT product development
 - (5) Browser-based training and documentation
 - (6) Reports and briefings
 - (7) Presentation media
 - (8) Trainer documentation (e.g., transfer documents, digital video disk (DVD), compact disk (CDs) labels, and training story boards)
- c) Life cycle support of:
 - (1) Training systems
 - (2) Training data products
 - (3) Trainer installation locations (including delivery, installation, upgrades)
- d) Using Government provided enterprise tools ((Microsoft Team Foundation Server, (MSTFS) and Perforce, both located in the SubRAT laboratory at NAWCTSD Orlando)), provide configuration management and source control of:
 - (1) Software
 - (2) 2D and 3D graphics
 - (3) Trainer installation configuration
 - (4) Photographic and videographic imagery
 - (5) Documentation
 - (6) Browser-based training and presentations
- e) Develop, conduct, and document software testing and evaluation using Government methods.
- f) Conduct research and analysis activities to support enhancement or modifications of training systems, including:
 - (1) Design and develop software test beds and research plans
 - (2) Explore new technologies
 - (3) Participate in research execution
 - (4) Psychological/educational/research technical documents and media
- g) Employ, document, and refine Government process improvement procedures and practices.
- h) Produce and maintain documentation, including:
 - (1) Trainer support documents
 - (2) Technical manuals
 - (3) Training software documentation
 - (4) Product user guides, training, reference media
 - (5) Research, analysis, and planning reports

3.2.3 Software Design

Prior to documenting software design, the Contractor shall develop a requirements description document (RDD) to demonstrate clear understanding of the requirements. Using the RDD, the Contractor shall design networked real-time workstation simulations and exercise control and monitoring applications and virtual tour instructional capabilities. The Contractor shall identify new functionalities to be added to the SUBSKILLSNET, VISIT, UAS, and related applications to meet new requirements, whether, when, and how a new library should be created, and how to maintain existing libraries so that changes do not negatively affect other applications that use them.

3.2.4 Software and Data Asset Re-Use and Shared Repository

The Contractor shall design and develop networked real-time workstation simulations by re-using, expanding and adding to Government-owned SUBSKILLSNET-VISIT-UAS software, libraries, data, databases, and other code. SUBSKILLSNET-VISIT-UAS trainers, training technologies, training software baselines, code, libraries, data, databases and models, training scenarios, instructor station capabilities, and research test beds shall be compatible, re-usable and transferable among all submarine and Naval Reserve Officer Training Corps (NROTC) training facility electronic classrooms, all tactical and navigation team-training simulation laboratories, and on training local area networks on all submarines. Unique versions of SUBSKILLSNET-VISIT-UAS deliverables are produced and delivered to multiple customers. These products shall be developed, modified, or maintained from the common set of SUBSKILLSNET-VISIT-UAS software and data assets hosted on a Government server/configuration management system in the SubRAT laboratory. Configurations shall be maintained for each product-line variant.

SUBSKILLSNET and VISIT product lines have been developed by leveraging a common set of Government-owned libraries, including:

- a) EWin, a library that consists of a class framework for Win32 application development
- b) Naiad, a simulation library used for developing SubSkillsNet client applications
- c) View3DX, a library that consists of a class framework used for developing visual simulation applications using Microsoft DirectX-Direct 3D

These Government-owned libraries are expanded as customer requirements emerge. The Contractor shall continue this practice of maximal leveraging of Government-owned software capabilities. The Contractor shall re-use, extend, and improve Government-owned SUBSKILLSNET, VISIT, UAS, and related software capabilities as tasked under DOs. Contractor-owned software and data shall not be used in lieu of re-using, expanding or improving functionality of Government-owned software and data. The Contractor shall prepare data items IAW specific provisions of individual DOs.

3.2.5 Development Environment and Practices

The Contractor shall follow established SUBSKILLSNET-VISIT-UAS coding and commenting conventions and use software languages specified in 3.2 (Specific Requirements). The Contractor shall design and develop Windows software using the Government-owned software libraries (Naiad, EWin, View3DX), data and code. The Contractor shall re-use, extend and improve the Naiad networked simulation library used to connect and share SUBSKILLSNET, VISIT, and UAS and their derivative simulation capabilities (e.g., Mariner Skills Simulator) and

shall re-use, extend and improve other Government-owned libraries as required. As specified by a DO, the Contractor shall design and develop Linux software (using Red Hat and CentOS) using Wine and other Linux based libraries. As specified by a DO, the Contractor shall deliver software interfaces to other simulations and tactical software systems re-using and extending capabilities previously developed by the SubRAT laboratory.

3.2.6 Software Development Languages, Libraries and Tools

The Contractor shall employ C++, extensible markup language (XML), EWin, Naiad, View3DX, Microsoft Visual Studio, Microsoft Team Foundation, Microsoft DirectX Application Programming Interface (API), Microsoft Direct3D Vertex/Pixel shader assembler, Microsoft Direct3D high level shader language (HLSL), InstallShield (authoring install scripts), Open GL API, Linux (Red Hat, CentOS), DNC, DTED, Common Object Request Broker Architecture (CORBA), HLA, DIS, Component Object Model (COM), Windows API, object oriented concepts, algorithm analysis, Win32 sockets and threads, structured query language (SQL), and MSTF software configuration management tools (SCM). Additionally, the Contractor shall employ as defined by individual DOs: Java, Java Script, C, C#, Visual Basic, VB Script, Perl, HyperText Markup Language (HTML), Hypertext Preprocessor (PHP), cascading style sheets (CSS), and MultiGen Creator (See paragraph 3.1.1, Government Property).

3.2.7 Digital Media/Art Development Languages, Libraries and Tools

The Contractor shall employ 3D Studio Max 2010 Adobe Photoshop CS4 or 5, Adobe Illustrator CS4 or 5, Autodesk Stitcher, SCM tools (specifically SVN) Adobe After Effects CS4 or 5, Adobe InDesign CS4 or 5, Adobe Flash CS4 or CS5, Mechanical Drawing, MSTF, Adobe Premiere Pro CS4 or CS5, Adobe Soundbooth, Animation/Rigging, and Scripting as needed to meet requirements of specific DOs.

3.2.8 Image Generator Development and Support

The Contractor shall develop enhancements for SubRAT's existing image generators (e.g., periscope, photonics, UAS) and deliver new image generators by leveraging existing SUBSKILLSNET-VISIT-UAS product capabilities. The Contractor shall deliver new GUIs, additional visual filters (e.g., low light level television, infrared, color gain, black and white), enhanced visual scenes, expanded employment of database variables (e.g., as from DNC, DTED, TOD), higher functional fidelity ocean modeling, and other enhancements as specified in individual DOs. Software products/capabilities will be delivered IAW the Basic Contract CDRL A002 (Computer Software Product).

3.2.9 Digital Media Products

The Contractor shall deliver 3D models, 2D graphics, photography, videography, animation and other media products in required formats (e.g., Autodesk .3ds) as specified in individual DOs. The Contractor shall produce, maintain, deliver, and integrate computer-generated graphics such as 3D models and 2D graphics, into existing software and immersive photographic training systems, as well as software under development and into the SUBSKILLSNET View3DX and EWin libraries. Additionally, the Contractor shall produce, edit, maintain, document, deliver, and integrate photographic imagery and video into existing software and immersive virtual tour training systems. The Contractor shall deliver modeling and photographic data items IAW specific provisions of individual DOs.

3.2.9.1 Photographic Image Products

The Contractor shall deliver still photography to support development of training systems. This includes the use of digital Single-Lens-Reflex (SLR) cameras to produce digital still photography. The Contractor shall prepare photographic data items IAW individual DOs and CDRL F001 (Instructional Media Package).

3.2.9.2 Videographic Image Products

The Contractor shall deliver digital video to support development of training systems and training research test beds. The Contractor shall prepare video data items IAW individual DOs.

3.2.9.3 Checkout Procedures of Government Photographic Property

Government photographic and video property will be located in the SUBSKILLSNET-VISIT-UAS laboratory (i.e., SubRAT Lab) to facilitate production and for local use, storage, and safe-keeping. The Contractor shall be required to travel as described in paragraph 3.7 (Travel), and as specified in individual DOs, for photographic and video production. When required to travel, a list of necessary Government Furnished Property (GFP) shall be detailed on a Department of Defense (DD) Form 1149 for custody transfer to the Contractor. The Contractor shall obtain standard Government property passes for this GFP from NAWCTSD security to facilitate travel and access to Government installations with this equipment. The Contractor shall conduct inspection and inventory prior to travel, while on travel, and subsequent to travel, the following:

- a) To detect damage
- b) To ensure completeness (item is whole) and proper type
- c) To ensure proper and satisfactory operation
- d) To protect from improper use or disposition
- e) To verify quantity

Also, subsequent to travel, GFP custody shall be returned to the Government using the DD-1149, and GFP equipment shall be returned to the SUBSKILLSNET-VISIT-UAS laboratory.

3.2.10 Networking

For SUBSKILLSNET-VISIT-UAS training and research systems, the Contractor shall apply network infrastructures, protocols, and secure interconnections between collocated and widely distributed interactive training devices, applications, and real-time simulations. The Contractor shall apply IEEE 1516 series of HLA standards for federation management interchange control functions and simulation interactions when interoperating with external simulators, as well as IEEE 1278 for DIS within a common tactical and physical synthetic training environment. Additionally, the Contractor shall follow CORBA standards cited in paragraph 2.2 (Non-Government Documents) of this SOW.

Additionally, the Contractor shall use the SUBSKILLSNET Naiad networking library for SUBSKILLSNET-VISIT-UAS products in classroom environments running as host simulation.

3.2.10.1 Networking within SUBSKILLSNET-VISIT-UAS Training and Research Products

SUBSKILLSNET employs the Instructor Interface for training session set-up and administrative control and the Naiad networking library for real-time interaction. The Contractor shall develop networked simulations (synchronizing data between server and clients with position keeping

algorithms, containing robust, extendable simulation data packets) and event-based simulation (e.g., synchronizing entities' creation between simulations, synchronizing entity state change) as specified by individual DOs.

3.2.10.2 Interfacing to External Systems

There are external software interfaces between SUBSKILLSNET (including related and derived products) and numerous simulations and tactical systems developed by other organizations and teams. The Contractor shall develop new interfaces between SubRAT laboratory products and other systems and components and extend existing interfaces as specified by individual DOs.

3.2.11 Configuration Management

The Contractor shall use the SubRAT in-lab repository (e.g., MSTFS, Perforce) to execute configuration management of software, installation baselines, documentation, and media and to execute software source control. This repository is not networked outside the SubRAT laboratory, and is also used by Government team members to store Government developed SUBSKILLSNET, VISIT, UAS, and research test bed software, media, and documentation and to track repository status.

3.2.12 Database Employment and Maintenance

The Contractor shall use, expand, and maintain existing, and develop new, databases in support of SUBSKILLSNET-VISIT-UAS training and research applications (e.g., for student performance evaluation data, digital media, contact and navaid models, gaming areas, image components). The Contractor shall employ externally provided databases, including DNC; DTED; and TOD (e.g., by file parsing and 3D display) and others as appropriate (e.g., satellite imagery for UAS sensor display) to enhance 3D model engine ocean realism (e.g., over-the-horizon visualization, ocean modeling, roll-pitch-yaw ocean physics) to provide improved trainer functional and visual fidelity. Software products/capabilities will be delivered IAW the Basic Contract CDRL A002 (Computer Software Product).

3.2.13 Product Installation Support

When required by an individual DO, the Contractor shall provide installation media (software versions, installation instructions, CD or DVD prepared with Install Shield or other specified product, media label) tailored to the requirements of the specified installation site. These include specialized versions of SUBSKILLSNET-VISIT-UAS and research products, elements of interactive courseware, and browser-based instruction and media. The Contractor shall support delivery, integration, certification, installation, and upgrade of training systems consisting of commercial and Government developed items. As specified in individual DOs, the Contractor shall provide off-site technical assistance to trainer installation sites. Technical assistance shall consist of problem resolution, trouble-shooting, installation support, and other services to support SubSkillsNet products, including its hardware and software.

3.2.14 Product Life Cycle Support

The Contractor shall provide life cycle support of training systems and training data products as directed by the Government in individual DOs, to include correcting software bugs found following delivery, preparing patch installation CDs, keeping SUBSKILLSNET-VISIT-UAS applications used in these trainers at their current delivery version level by preparing

SUBSKILLSNET-VISIT-UAS updates for delivery, and identifying hardware requirements to support SUBSKILLSNET-VISIT-UAS in these trainers.

3.2.15 Hardware and Software Integration

The Contractor shall provide the engineering tasks necessary to deliver performance specifications of training system hardware and to integrate system hardware and software to meet the requirements as defined in specific DOs. The Contractor shall support efforts to conduct hardware and software integration in the SubRAT laboratory and at delivery sites as specified in individual DOs.

3.2.16 Test and Evaluation (T&E)

The Contractor shall follow the SubRAT laboratory's T&E process and methods to verify requirements are met as defined by each DO and shall maintain updates to the process in the SubRAT laboratory's configuration management system (MSTFS, Perforce). Results of testing shall identify, and contribute to the diagnosis of root causes of, software malfunctions and IA vulnerabilities that may be caused by poor software implementation.

3.2.16.1 T&E Planning

The Contractor shall develop, and submit to the Government for discussion, the testing and evaluation plans and procedures for all instances of tests (e.g., prior to delivery to a fleet customer). If a need for changes is revealed during discussion, the Contractor will make necessary revisions prior to test execution. All testing and evaluation plans and procedures will be developed IAW CMMI or other specified Government Process Improvement Program as documented for the SubRAT laboratory. Final versions of test plans and procedures shall be hosted on the SUBSKILLSNET-VISIT-UAS configuration management system.

3.2.16.2 T&E Knowledge Resources

The Contractor shall employ knowledge of software development best practices, of the capabilities being tested, and of the actual software components to execute testing of SUBSKILLSNET, VISIT, UAS-related, and research test bed software and hardware products to ensure that deliverables comply with requirements documented in individual DOs.

3.2.16.3 Test Repository

The Contractor shall maintain a repository of all software tests following CMMI or other specified guidance stored in the SUBSKILLSNET-VISIT-UAS laboratory's configuration management system (i.e., MSTFS, Perforce).

3.2.17 Product Acceptance

The Government shall be the sole acceptance authority in determining whether products and integration, test, and evaluations meet DO requirements. Acceptance will follow:

- a) US Navy Fleet Subject Matter Expert (SME) acceptance,
- b) Integration of products into SUBSKILLSNET-VISIT-UAS training and research products, respective to the individual tasks,
- c) Successful test and evaluation IAW the T&E paragraph (3.2.16) in this SOW.

The Contractor shall execute corrective action when required to meet DO requirements.

3.2.18 Presentation and Publication Products

3.2.18.1 Documentation

The Contractor shall produce and deliver training and trainer support documents, technical manuals, training software documentation, psychological/educational/research technical documents, training requirements analysis documents, presentation support media (e.g., PowerPoint, animations), computer graphics to support CD/DVD packaging and media products, brochures and informative publications (hardcopy and electronic), user manuals, user tutorials, and browser-based presentations and documentation. The Contractor shall integrate digital media as needed to meet requirements of individual DOs. The Contractor shall deliver modeling and photographic data items IAW specific provisions of individual DOs. Documentation deliverables will be IAW with specified CDRLs.

3.2.18.2 Training Requirements Analysis Reports

The Contractor shall systematically investigate specified training needs and problems. The training needs and problems shall be clearly identified through the use of data collection, document review, interviews, and meetings. All supporting analysis data (e.g., task frequency, importance, difficulty, how long it takes to learn, how difficult it is to learn, rate of skill decay, performance delay tolerance, immediacy of assigned task performance after training, type of knowledge/performance (e.g., recall, procedural, analysis, decision-making, physical manipulation, lifting), risk severity, and how specific it is to the specified incumbent job performer) will be retained in the SubRAT laboratory's data repository. Analysis results shall be quantified and organized in a manner that makes clear the trade-offs to be weighed by the Government and fleet customer during subsequent prioritization of training requirements.

Alternative training solutions shall be identified via work with team members consisting of software engineers, media artists, hardware engineers, psychologists, and SMEs to identify existing or potential overlap between customer training needs and training capabilities that can be provided by existing or upgraded versions of SUBSKILLSNET, VISIT or UAS software, libraries, databases, data or other assets, or by re-using and expanding component parts of these product-lines' capabilities or whether new development will be required. The training needs analysis results and recommended instructional tool/trainer alternatives and plans shall be documented and delivered to the Government as required by individual DOs in compliance with specified CDRLS and shall be retained in the SubRAT laboratory's data repository.

3.2.19 Risk Management

3.2.19.1 Risk Management Plan

The Contractor shall provide a risk mitigation plan that shall describe specific contract start-up plans to ensure adequate productivity during the first DO to include: plans to track, manage and report schedule and performance risk issues; technical staff knowledge of, and skills related to re-use of, Government-owned software libraries, databases, and code; and required software languages, tools and media skills; and approach to track and mitigate issues related to developing software interfaces to systems developed by other DOD agencies and commercial organizations. The plan shall clearly demonstrate how the Contractor will adapt to variable contract task loading and changing skill mix demands for each DO and for management of multiple concurrent DOs, which is expected to be a recurring situation throughout the life of the contract.

When required in an individual DO, the Contractor shall conduct risk management to systematically control the uncertainty in the project's ability to meet cost, schedule, and performance requirements. The Contractor shall provide the Government visibility into the Contractor's tools, assessment, mitigation, and control techniques. When required in an individual DO, the Contractor shall define, document, manage, and apply a risk management process IAW IEEE Std 12207-2008, Section 6.3.4. The Contractor shall report risk information, data, and analysis as required and specified in the individual DO.

3.2.20 Research Products – Test beds, Studies, Data, Analysis, Documentation

The Contractor shall execute research projects by delivering novel capabilities within SUBSKILLSNET-VISIT-UAS derived and related research products that enable required experimental stimulation (e.g., emerging technologies, such as speech recognition, instructional adaptability, and virtual world features) and data collection (e.g., automated data capture capabilities, integrated database storage and data manipulation capabilities). The Contractor shall conduct software prototyping and development in support of research, modification and updating of existing and future training software, and software that stimulates and emulates hardware and software used by the military, for the purpose of integrating advanced training research technology and approaches into laboratory training product deliveries. The Contractor shall execute experimentation (e.g., develop research design documents; execute and document research results, conclusions, and recommendations) as required in individual DOs to design, develop, and evaluate innovative training technologies and approaches to support multiple training communities.

3.2.21 Material

Material procurements are intended to facilitate flexibility and capabilities to perform research, development and data collection. On a limited basis, the Contractor shall purchase Commercial-Off-The-Shelf (COTS) Personal Computer (PC) software and hardware-related equipment and photographic supplies in support of software development and trainer delivery. Hardware procurements will generally be limited to specific cases where Contractor personnel require an enhanced workstation capability to develop new software features to bring workstations back online for development, testing, or training, and when Contractor personnel need storage media or memory (e.g., DVDs, CDs) to facilitate backup and filing of data. Software procurement will be limited to COTS software tools to develop software. Photographic equipment such as cameras, video cameras, lights and tripods may be procured to replace broken items or to refresh worn-out or outdated inventories, but generally photographic supplies will be limited to memory cards, film, lens paper, and ancillary photographic consumables which facilitate on-site production. Special-purpose or unique materials required for the execution of contracted research studies and experiments may be procured under this contract.

3.2.22 Travel

Contractor personnel shall travel as required by the Government in support of efforts as specified in DOs. Typically, the purpose of travel is to attend and participate in conferences, reviews, software testing, integration, certification and installation, and to conduct photographic and video image capture. Although travel is estimated and planned during requirements development, the Contractor must take into account that some issues can necessitate a shift of planned travel dates. Representative sites include, but are not limited to, Naval Submarine Training Center Pacific, Pearl Harbor, HI; Naval Submarine Training Center Pacific Detachment, San Diego, CA; Naval

Submarine Training Center Pacific Detachment, Guam; Trident Training Facility, Bangor, WA; Trident Training Facility, King's Bay, GA; Naval Submarine School, New London, CT; Submarine Training Facility, Norfolk, Naval Undersea Warfare Center, Newport, RI; Patuxent River, MD, and Naval Surface Warfare Center, Carderock, MD. All travel shall be IAW the Joint Travel Regulations (JTR).

Appendix A

Acronyms

| | |
|--------|---|
| 2D |two dimensional |
| 3D |three dimensional |
| AIS |Automatic Identification System (a tool for electronic piloting) |
| AIS |Automated Information System (computer and software used for information handling) |
| ANSI |American National Standards Institute |
| API |Application Programming Interface |
| ASQC |American Society for Quality Control |
| ATO |Authorization To Operate |
| C&A |Certification and Accreditation |
| CAC |Common Access Card |
| CC |Common Criteria |
| CD |Compact Disk |
| CDRL |Contracts Data Requirements List |
| CFR |Code of Federal Regulations |
| CM |Carnegie Mellon |
| CM-SEI |Carnegie Mellon-Software Enterprise Institute |
| CMA |Common Management Agent |
| CMMI |Capability Maturity Model Integration |
| COM |Component Object Model |
| CORBA |Common Object Request Broker Architecture |
| COTS |Commercial Off The Shelf |
| CPSMR |Contractor's Progress, Status and Management Report |
| CSS |Cascading Style Sheets |
| CUI |Controlled Unclassified Data |
| DADMS |DON Application and Database Management System |
| DBMS |Database Management System |
| DD |Department of Defense (prefix on DOD form numbers) |
| DIACAP |DON/DOD Information Assurance Certification and Accreditation Process |
| DIS |Distributed Interactive Simulation |
| DNC |Digital Nautical Chart |
| DO |Delivery Order |
| DOD |Department of Defense |

DODIDOD Instruction
DONDepartment of the Navy
DTEDDigital Terrain Elevation Data
DVDDigital Video Disk
ECAREngineering Compliance Auditing and Reporting
EIAElectronic Industries Association
EOPS.....Environmental, Occupational health, and Personnel Safety program
EPAEnvironmental Protection Agency
ESGNElectrically Suspended Gyro Navigation
EWinSubRAT's Windows API wrapper
FBIFederal Bureau of Investigation
GFPGovernment Furnished Property
GOTSGovernment off The Shelf
GPSGlobal Positioning System
GUIGraphical User Interface
HBSSHost Based Security System
HLAHigh Level Architecture
HLSLHigh Level Shading Language
HTMLHyper Text Markup Language
IAInformation Assurance
IAVA.....IA Vulnerability Alert
IAVB.....IA Vulnerability Bulletins
IAVMP.....Information Assurance Vulnerability Management Program
IAVT.....Vulnerability Technical Advisory
IAWIn Accordance With
IDIQIndefinite Delivery Indefinite Quantity
iDPIn-House Development Process
IECInternational Electrotechnical Commission
IEEE.....Institute of Electrical and Electronics Engineers
IGImage Generator
ISBNInternational Standard Book Number
ISOInternational Organization for Standardization
ITInformation Technology
JTR.....Joint Travel Regulations
MACMission Assurance Category
MiniSPANMini Submarine Piloting and Navigation (trainer)
MSTFMicrosoft Team Foundation
MSTFS.....Microsoft Team Foundation Server

NACINational Agency Check with Inquiries
NACLICNational Agency Check with Local Agency Checks including Credit Check
NAIADSUBSKILLSNET's simulation engine
NAIPNational Information Assurance Partnership
NAIPNational Information Assurance Partnership
NROTCNaval Reserve Officer Training Corps
OPSECOperations Security
OSHA.....Occupational Safety and Health Agency
PAC.....Post Award Conference
PCPersonal Computer
PDDProcess Description Document
PERLsoftware language
PHPHypertext Pre-Processor
PIIPersonally Identifiable Information
PITPlatform IT
PPSMPorts, Protocols and Services Management
PRAPlatform IT Risk Approval
RDDRequirements Description Document
RFPRequest For Proposal
RLGN.....Ring Laser Gyro Navigation
SCMSoftware Configuration Management
SDPSoftware Development Plan
SEI.....Software Engineering Institute
SLRSingle Lens Reflex
SMESubject Matter Expert
SMMTTSubmarine Multi-Mission Team Trainer
SNACSystem and Network Attack Center
SOW.....Statement of Work
SQLStructured Query Language
SSP.....Systems Safety Program
STIGSecurity Technical Implementation Guides
SubRATSubmarine Research Applications Team
SUBSKILLSNET Submarine Skills-training Network
T&E.....Test and Evaluation
TLSTransport Layer Security
TODTactical Ocean Data
TRTechnical Report
UAS.....Unmanned Aerial System

View3DXDirectX API wrapper (with additional capabilities)
VISVendor Integrity Statement
VISITVirtual Interactive Shipboard Instructional Trainer
VSE.....Very Small Entity
XML.....Extensible Markup Language