PERFORMANCE WORK STATEMENT (PWS)

NATO IMPROVED LINK ELEVEN TRAINING SERVICES

Dated 12 July 2022

1. SCOPE

The Naval Information Warfare Systems Command (NAVWAR), in support of the Program Executive Office Command, Control, Communications, Computers, and Intelligence (PEO C4I), Navy Command and Control Program Office (PMW 150), is conducting training on behalf of the North Atlantic Treaty Organization (NATO) Improved Link Eleven (NILE) Nations.

This Link 22 Training Performance Work Statement (PWS) establishes the requirements for the training offered to the nations, both on-line and in person and related to Link 22, the System Network Controller (SNC) from a technical and an operational perspective, interfaces with the LLC 7M and all other Link 22 equipment and processes associated with operating a Link 22 network.

The Contractor shall comply with the NATO Improved Link Eleven In-Service Support Memorandum of Understanding as amended, specifically Section VI (Contracting Provisions) (specifically paragraphs 6.4 and 6.5), Section VIII (Disclosure and Use of Project Information), Section IX (Controlled Unclassified Information), Section XI (Security), Section XII (Third Party Sales and Transfers), and Section XVII (General Provisions).

2. BACKGROUND

During the late 1980s, NATO, agreeing on the need to improve the performance of Link Eleven (Link 11), produced a Mission Need Statement (MNS) that became the basis for the establishment of the NILE Project.

The NILE Project was initially developed collaboratively by seven nations under the aegis of a Memorandum of Understanding (MoU). The original seven nations were Canada (CAN), France (FRA), Germany (DEU), Italy (ITA), the Netherlands (NLD), the United Kingdom (UK) and the United States of America (USA). Spain (ESP) replaced the Netherlands in 2003. The current seven nations are hereinafter referred to as the “NILE Nations”.

This multi-nationally funded project is guided by a Steering Committee (SC) consisting of a representative appointed by each NILE Nation. The project is managed by the NILE Project Management Office (NILE PMO), located at PEO C4I, PMW 150.

In terms of governance, the NILE PMO consists of one representative from each NILE Nation and a Project Manager (PM) who is appointed by the United States Department of the Navy and endorsed by the NILE Steering Committee (NILE SC). The configuration control function is exercised, on behalf of the SC, by a Configuration Control Board (CCB). The CCB is composed of a representative of each NILE Nation and is chaired by the NILE PM.

NILE has been designated Link 22 by NATO. Link 22 is a standard for wireless and secure information interchange between military units. Link 22 provides improved High Frequency (HF) and Ultra High Frequency (UHF) radio communications of tactical data. Link 22 offers a more robust terrestrial Beyond Line of Sight (BLOS) Waveform than Link 11. It also provides better Real Time Tactical access compared to Satellite Communications, and improves Allied Interoperability through a Common Design. Link 22 offers a BLOS tactical data link that is designed to fully complement its Link 16 Line of Sight (LOS) counterpart, but without the complex planning, monitoring and network management overhead.

As the project progresses through each life cycle phase, each phase demands a new amendment to the MoU. A summary of the project's life cycle history is as follows:

Project Definition	Nov 87 – Jun 92 (Completed)
Design and Development Sub-phase 1	Jul 92 – Jun 97 (Completed)
Design and Development Sub-phase 2	Jul 97 – Jun 02 (Completed)
In-Service Support Phase (Amendments 1-4)	Jul 02 – Jan 20 (Completed)
In-Service Support Phase (Amendments 1-5)	Jan 20 – Dec 29 (On-going)

The primary objective of Sub-phase 1 of the Design and Development (D&D) Phase of the NILE Project was to design a system consisting of a computer-to-computer, digital data link among Tactical Data System (TDS) equipped platforms, in order to meet the NATO Staff Requirement for NILE. An additional NILE objective of the D&D Phase was to develop common specifications and project information sufficient to enable the participating nations to develop Link 22 systems, which will be interoperable and compatible with those of other nations.

The objective of Sub-phase 2 of the Design & Development Phase was to design, develop, build, and test a System Network Controller (SNC), a NILE Reference System (NRS) and the Link 22 element of MLST3 (Multi-Link System Test and Training Tool) that met the requirements of the specifications referenced herein, and to develop sufficient technical data to enable each NILE Nation to utilize and maintain the SNC, NRS and MLST3, as part of their national Link 22 implementation programs.

The objective of the In-Service support phase is to provide in-service support for, maintain commonality of, and pursue improvements to the products of the NILE project including the System Network Controller (SNC), NILE Reference System (NRS), NILE Interoperability Test Tool (NITT) and associated baseline product specifications, and to support interoperability between Link 22 systems in a multi-link environment.

The NILE system is depicted by Figure 1 below. All NILE interface specifications (the arrows in Fig. 1) and the SNC have been either jointly defined, designed and developed by the NILE Nations, or selected and adopted by the NILE Nations from industry.

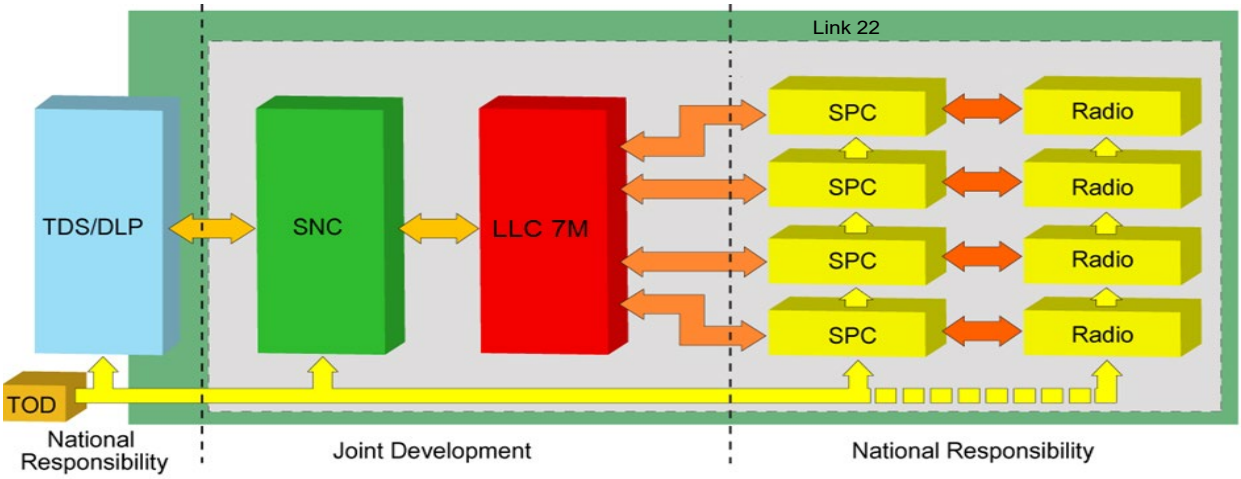

Figure 1- Link 22 System with NILE Communication Equipment

The SNC provides common operational software that is compatible among the Link 22 architectures of the seven current NILE Nations. The NRS is a test tool, which enables compatibility testing of Link 22 implementations by the participating nations.

The Link 22 system uses the Link-22 Modernized Link Level COMSEC (LLC 7M) device to provide communication encryption services at the link level. This cryptographic equipment also provides time-of-day (TOD) based encryption and decryption services for network messages sent over multiple NILE transmission networks.

The Link 22 products are sold through Foreign Military Sales (FMS), to other nations approved by the NILE nations. Those nations are hereinafter referred to as the "Link 22 Partner Nations".

3. REFERENCES

3.1. NILE Documents

NILE PMP	NILE Program Management Plan
NILE CMP	NILE Configuration Management Plan
SNC SDD	SNC Software Design Description
SNC SS	Segment Specification for the SNC
SNC STD	Software Test Description for the SNC
SNC STM	System Technical Manual for the SNC
SNC STR	Software Test Report for the SNC
SNC SVD	Software Version Description for the SNC
NRS SVD	Software Version Description for the NRS
	Media Simulation Software Requirements Specification
NRS IDD	Interface Design Description for the NRS
NRS SS	System Specification for the NRS
NRS STD	Software Test Description for the NRS
NRS STM	System Technical Manual for the NRS
NRS STR	Software Test Report for the NRS
	Scenario Generator Software Requirements Specifications
	Interface Design Description for the Data Link Processing Segment and the SNC
	Interface Requirement Specification for the Link-Level COMSEC Segment
	Configuration Management Information
SPC SS	Segment Specification for the SPC
	Segment Specification for the SPC Serial Splitter
DERD	Data Extraction and Reduction Document
	Glossary for the NILE in-Service Support Phase
	Help Files for NILE in-Service Support Document Navigation
	NILE Requirements Traceability Matrix
	Link 22 Guidebook
	Link 22 Familiarization v2

3.2. NATO Standards and Documents (latest edition)

STANAG 4203	Technical standards for single channel radio equipment
STANAG 4205	Technical standard for single channel UHF radio equipment
STANAG 4285	Characteristics of 1200/2400/3600 bits per second single tone modulators demodulators for HF radio links
STANAG 4430	Precise time and frequency interface and its management for military electronic systems
STANAG 4444	Technical standards for a slow hop HF EPM Communications system
STANAG 4539	Technical standards for non-hopping HF communication waveforms
ATDLP-5.16	TACTICAL DATA EXCHANGE - LINK 16
ATDLP-5.22	TACTICAL DATA EXCHANGE - LINK 22
ATDLP-6.02	STANDARD INTERFACE FOR MULTIPLE PLATFORM LINK EVALUATION (SIMPLE)
ATDLP-6.16	Tactical Data Forwarding
ATDLP-7.33	Multi-Link Standard Operating Procedures for Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS and Link 22
ADatP–3	NATO MESSAGE TEXT FORMATTING SYSTEM (FORMETS) – CONCEPT OF FORMETS (CONFORMETS)

3.3. Other Documents

DFARS Subpart 239.71	Security and Privacy for Computer Systems dtd 31 Oct 2019
DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14
DoDD 8140.01	DoD Directive –Cyberspace Workforce Management dtd 11 Aug 15
DoD 8570.01-M	Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 4 dtd 10 Nov 15
SECNAVINST 5239.20A	DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification dtd Jun 16
SECNAV M-5239.2	DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual dtd Jun 16
DON CIO Memo	Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16
Navy Telecoms Directive (NTD 10-11)	System Authorization Access Request (SAAR) – Navy
SECNAVINST 5239.3B	DON Information Assurance Policy, 17 Jun 09
007-500028-001	LLC 7M Installation, Configuration, and Operation Instructions, Revision C, Apr 2016
PI-L22D-RM-03	LINK-22 Modernized Link Level COMSEC (MLLC) System/Subsystem Specification
SPAWARINST 3058.1	Naval SYSCOM Risk Management Policy, 07 Apr 2008
SPAWARINST 5234.1A	Naval Warfare Systems Certification Policy, 24 Aug 2012
PI-L22D-DP-10	Key and Certificate Management Plan (KCMP)
007-500028-001	LLC 7M Installation, Configuration and Operation Instructions (includes Outline and Mounting Drawings) LLC 7M Outline Solid Model (PDF/STEP format)

DoD 5220.22-M	National Industrial Security Program Operating Manual dtd 18 May 16
DoDI 5230.24	Distribution Statements on Technical Documents
DoDI 5200.48	Controlled Unclassified Information
DoD Cloud Computing SRG v1r4	Department of Defense Cloud Computing Security Requirements Guide (version 1, release 4), dated14 Jan 2022
DoDI 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT), dated 29 Dec 2020
NIST SP 800-114	National Institute of Standards and Technology Special Publication, User's Guide to Telework and Bring Your Own Device (BYOD) Security, Published Jul 2016
NIST SP 800–88	National Institute of Standards and Technology Special Publication, Guidelines for Media Sanitization, Published Dec 2014
NIST SP 800-171	National Institute of Standards and Technology Special Publication, Protecting CUI in Nonfederal Systems and Organizations, Published Feb 2020
DFARS Clause 252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting
FIPS 140-2	Security Requirements for Cryptographic Modules

4. REQUIREMENTS

4.1. Learning objectives

4.1.1. The Contractor shall deliver technical and operator Link 22 training to personnel of NILE and Link 22 Partner Nations. The Contractor shall give an operational perspective to its presentations by giving application examples, context and/or operational anecdotes. At the end of the course the student should be able to set up, operate and manage a Link 22 network. The learning objectives for all Link 22 training courses (classroom-based, virtual instructor-led, virtual self-paced, and train the trainer) are as follows:

i. Link 22 familiarization
ii. SNC interfaces
iii. Planning & Network management overview
iv. Overview of the NILE Reference System (NRS)
v. Parse an Operational Tasking (OPTASK) Link Message to create a dynamic operational scenario, run the scenario, reduce data extraction (DX) file with NRS (students shall perform these activities). The dynamic operational scenario should start with a low track load for each unit and no congestion, but develop over time into a high track load congested landscape. The operator will need to adjust Network Parameters in order to reduce congestion.
vi. System initialization
vii. Order automation
viii. Congestion avoidance and Dynamic Time Division Multiple Access (DTDMA)
ix. Relay, routing and connectivity
x. Late Network Entry (LNE)
xi. Waveform overview
xii. Tactical messages

xiii. Troubleshooting
xiv. Monitor the alarms and alerts of the SNC, LLC, SPC and Radios and take the appropriate actions to fix the problem

4.1.2. The Contractor shall provide technical attendees with specialty training in the following additional areas:
i. Operational Network Cycle Structure (ONCS)
ii. Time of Day Overview
iii. Technical Messages
iv. Maintenance & Troubleshooting
v. Automated Testing with NRS
vi. Other Test Configuration with NRS

4.1.3. The Contractor shall provide operator attendees with specialty training in the following areas:
i. Planning & Network Management
ii. Operational Tasking (OPTASK) Link Message
iii. Plan a Link 22 Super Network from an Operational scenario and initialize each Network with NRS (students should conduct this activity)

4.1.4. The Operator training materials shall describe a generic Data Link Processor (DLP) and its operation in sufficient detail for the DLP operator to perform the following functions:
i. Parsing the OLM;
ii. Correcting errors in the OLM;
iii. Key Upload and Settings;
iv. Set the parameters for the SNC, LLC, SPC and the radios in order to be able to create a network/join a network with the different types of join;
v. SNC initialization;
vi. Network start entry with monitoring of incoming messages;
vii. Interpreting SNC statistics (error free messages, messages with decoded errors, messages with undecided errors, and messages not received; and,
viii. Verification of the ONCS
ix. Manage the network as Network Manager Unit or a Super Network Manager Unit;
x. Congestion Monitoring and Management.

4.1.5. The Contractor shall develop and maintain all required training materials, and should state whether the training materials will be delivered with a restrictive data rights or intellectual property rights posture. The Government expectation is that training materials developed under contract will be delivered with Unlimited Rights, as that term is defined in DFARS 252.227-7013, Rights in Non-Commercial Technical Data. The Contractor shall deliver all training materials (documents, HTML files, presentations, briefs, slides, exercises etc.) to the Government at the end of the Period of Performance. The course, and all materials must be in English, and there is no requirement to translate

any training materials into a language other than English. All documents provided by the NILE PMO as Government Furnished Information (GFI) for contract performance will be in English.

4.1.6. The Government may, at its discretion, add or remove training objectives to those stated in section 4 of this PWS.

4.2 The Contractor shall provide the following types of Link 22 training courses:

4.2.1 Classroom course requirements (CLIN 0001)

The Contractor shall design a classroom-based Link 22 course for Link 22 Operators and Technicians, with categories of information as provided in section 4.1. of this PWS. This includes designing all training materials (including slides, supporting documents, exercises, quizzes, tests, training handouts etc.).

The Contractor shall be required to provide classroom training facilities, equipped with all necessary hardware, software, and audiovisual equipment required to deliver the course. For parts of the training that require access to a PC or laptop, students should be able to access a PC/laptop at a ratio of a maximum of two students per PC/laptop. All PCs/laptops must be equipped with the latest version of Windows operating system compatible with the SNC per Government's direction. The Government will provide the NRS software as GFI for the Contractor to preload on to the PC/laptops in order to conduct the training. PCs/laptops will not be provided as GFI. The instructors shall be familiar with Windows 10 operating system (or latest version of Windows) and NRS software and capable of troubleshooting the systems.

The Contractor shall provide each student with a Feedback form, collect all the forms, analyze the feedback and provide the PMO with a summary of the feedback within 5 business days from the end of every training course. The Contractor shall provide the Government with recommendations for course improvements based on attendee feedback, and will implement changes following written approval from the COR and as issued on a Task Order.

The Contractor should identify a geographical location (country, city, and location) for the classroom-based training, which must be in one of the NILE Nations (CAN, DEU, ESP, FRA, ITA, UK and USA). The Government reserves the right to designate primary and alternative venues within the same NILE country.

The Contractor shall ensure that the venue for classroom-based courses conforms to the following requirements:

a. Sufficient desks for one per student with power at the desk;
b. Equipped with any audio visual equipment to allow the Contractor to deliver the training (e.g. projector, Wi-Fi or other connectivity, microphones if required);
c. Sufficient hardware (e.g. laptops) for the conduct of the training course at a maximum ratio of two students per PC/laptop; and
d. The room shall be separate from any public areas, have doors that shut properly and limit noise interference from outside, or those outside the room from listening to the course materials.

The Government reserves the right to inspect the training location, and should it not meet the requirements above, require selection of an alternative venue within the same NILE country.

The Contractor shall deliver up to five classroom-based Link 22 Operator and five Technician training courses per calendar year. If the Operator and Technical sessions are held in parallel, the Contractor shall provide at least two instructors per training event, at least one dedicated to the Operator session, and one dedicated to the Technical session. Each course will be able to accommodate up to 30 attendees from NILE Nations and eligible Partner Nations. Courses will be executed at Task Order level, at which time the Government will include a list of nations which are eligible to attend the specific course. As a minimum, the following nations will be included: AUS/BEL/CAN/CHL/DNK/ESP/FIN/FRA/ITA/JPN/MAR/MEX/NCIA/NLD/NOR/NZL/POL/PRT/ROK/SAU/SWE/TUR/UAE/UK/USA. The course, and all materials must be in English, and there is no requirement to translate any materials. The Contractor shall provide printed copies of all training materials for participants to take with them at the end of the course.

Reference
CDRL J001 – Classroom Training materials

4.2.2 Online virtual self-paced course requirements (CLIN 0001)

The Contractor shall provide an online platform to host the online Link 22 Operator and Technician training course. The online course must cover the same learning objectives as outlined in section 4.1.1. of this PWS, except for the practical activities with the NRS. The online platform proposed by the Contractor must be authorized by the Government for use with Controlled Unclassified Information (CUI) information, subcategories CTI, EXPT, and INTL (see DODI 5200.48). The platform must have the following functionality:

a. Individual log in required to access to training materials;
b. Training platform accessible 24/7 except during maintenance phases via web so that participants from all time zones can use it;
c. Function for students to submit questions directly on online training platform, and receive answers by email from Contractor within 5 business days;
d. Interactive exercises, quizzes and tests as mandatory elements to the training;
e. Mandatory assessment at the end of the course, with pre-defined percentage pass in order to receive emailed certificate of completion. Assessment should be the same as that in the classroom-based course;
f. Feedback form provided at the end of the course, in order to collect feedback from the attendees; and,
g. Support portal, accessible 24/7 via web with FAQ, knowledge base for the most common problems and capability to open individual support requests.

The Contractor help desk shall be capable of providing answers to users within 5 business days from the request.

The Contractor shall maintain and update the platform where training materials are available at all times, except during maintenance phases of the website. The planned maintenance phases of the website must be limited to 24 hours per month.

This distributed course will be only accessible following presentation and validation of user credentials provided after registration. **The platform shall be able to accommodate a minimum of 20 simultaneous connections without a decrease in performance. If the Contractor is able to offer more simultaneous connections, the Government will find this as a strength, and the resulting contract will be updated.** Each new registration must be validated by the NILE PMO. Each registration will only be valid for one year.

Reference
CDRL J003 – Online Self-paced Training materials

4.2.3 Online virtual instructor-led course requirements (CLIN 0001)

The Contractor shall design a distributed course session similar to the classroom session but performed online. This session will cover the same categories of information as the classroom based session for Link 22 Operators and Technicians, with categories 4.1. However, the practical activities with the NRS will be simulated and performed by the contractor online. The Contractor shall use the same training materials designed for the classroom session.

The Contractor shall perform this session via a platform previously agreed with the Government that meets the security requirements as per section 6 and 7 of this PWS. The software selected must allow the course to be interactive, meaning that the students shall be able to ask questions in real time and visualize the presentation as the teacher goes through them.

The Contractor shall deliver up to twelve distributed Link 22 Operator and twelve distributed Technician training courses per calendar year and each course will be limited to 30 attendees.

The Government will group attendees from nations in similar time zones where possible, and accordingly, the Contractor shall deliver the distributed course during business hours for the attendees (e.g. if the attendees are located in Japan, the Contractor shall deliver the distributed course between 0800 and 1700 JST (Japan Standard Time)). If attendees are from a mixture of nations, the NILE PMO will provide the Contractor with a preferred time zone for the distributed training.

Reference
CDRL J002 – Online Instructor-led Training materials

4.2.4 Train the Trainer course requirements (CLIN 0001)

The Contractor shall design a Train the Trainer (T3) Link 22 course, which teaches attendees how to deliver a classroom-based operator and technician Link 22 course, covering the learning objectives in section 4.1. of this PWS. Completion of the course should allow attendees to deliver the operator and technician Link 22 course in their respective nations.

The Contractor must design an examination which is mandatory for successful course completion, and for attendees to receive a trainer certificate.

The Contractor should be prepared to deliver the classroom based Link 22 T3 course up to 3 times per calendar year, with courses being executed at Task Order level, and each course will be limited to 20 attendees.

All of the requirements for the Link 22 classroom-based course shall apply to the classroom-based T3 course (see section 4.2.1. of this PWS).

Reference
CDRL J004 – Train the Trainer Training materials

4.3 In-country training (CLIN 0001)

The Contractor shall provide in-country training, by delivering the classroom-based Link 22 training course in-country for any NILE or Link 22 Partner Nation. These countries are as follows, but this list is not exhaustive and is subject to change:
AUS/BEL/CAN/CHL/DNK/ESP/FIN/FRA/ITA/JPN/MAR/MEX/NCAI/NLD/NOR/NZL/POL/PRT/ROK/SAU/SWE/TUR/UAE/UK/USA). Training facilities will be provided by the host country, and the Contractor shall provide all training materials and equipment including laptops as required for the delivery of the course.

Reference
CDRL J001 – Classroom Training materials

4.4 Examination and practical work (CLIN 0001)

The Contractor shall ensure that the classroom-based course, online self-paced, online instructor-led, train the trainer, and in-country classroom-based courses all include the following:

a. Daily quizzes, interactive exercises, and informal tests and/or assessments to consolidate student learning, and objectively validate the efficacy of the instruction;
b. Examination at the conclusion of the course to be completed by each student, with a pass mark set in advance. The Contractor shall design the examinations to validate learning over the entirety of the course, administer the examination, mark the examination papers and provide students with their result (pass/fail) and a pass certificate (where applicable). The Contractor shall provide each student with the results of their examination, and a pass certificate for successful students within 3 business days of the completion of the examination.

The Contractor shall ensure that the classroom-based course and train the trainer course all include the following:

a. Practical experience of launching the SNC application and setting up the correct parameters to start, initiate, and operate a network as a simple NU, a SNU or a SNMU;
b. Monitor and understand potential SNC alerts; and,
c. Resolve a connectivity issue generated by the instructor.

The course must include interactive exercises to consolidate learning and enable participants to get practical experience of Link 22. Practical experience shall include use of the NRS on a PC/laptop. In addition, the training shall require participants to take an assessment on the final day of the course and pass with a pre-defined percentage in order to receive a certificate of completion.

The Contractor shall provide a post-training course report following each classroom-based (including in-country), online instructor-led, and train the trainer course.

References
CDRL A006 – Post Training Report

4.5 Updates to training materials requirements (CLIN 0002)

The Contractor shall update training materials in alignment with the release of new NILE Block Cycle Releases and any other significant capability updates (e.g. as a result of intermediate deliveries). For the purposes of this contract, the Contractor should plan to implement updates to the training materials in 2024, and 2026. The Government may request updates outside these time periods, within the period of performance of the contract limited to 1 per year.

5. ADMINISTRATION

5.1 Training Course Administration

The Government will be responsible for registering attendees to attend all types of training courses under this contract, and ensuring that they are approved to receive Link 22 information. The Government will provide the Contractor with a list of attendees for all courses 12 weeks ahead of the first day of each course.

The Contractor shall send all delegates a Course Conduct Information Package no later than 10 weeks prior to the start date of each classroom-based, online instructor-led, and train the trainer course, which shall include at a minimum the following information:

a. Specific location of the training, including directions from the closest international airport;
b. Recommended travel options, including the name of the closest international airport and recommended travel route and method from the airport to the training location;
c. Local accommodation recommendations;
d. Planned agenda including daily start and finish times, and the content for each day of the training;
e. Information about refreshments available on site or nearby;
f. Dress code;
g. Access and security requirements for attending the training site;
h. Pre-reading or pre-course activities that need to be completed before the student attends the course; and,
i. Training system credentials, information, user guides etc., as required for the successful completion of the course.

References

CDRL J005 – Course Conduct Information Packet DI-PSSS-81522

5.2 Contractor's Progress, Status and Management Report

The Contractor shall provide a Contractor's Progress, Status and Management Report on a monthly basis. The report shall detail the schedule of events and the integrated cost and schedule status of work progress on the contract, as well as reporting on the quality metrics set out in the Quality Assurance Surveillance Plan. The schedule shall reflect the tasks, dates (baseline, forecast, and actual), external and internal dependences and relationships necessary to support accurate forecasts of contract milestone delivery dates by both the Contractor and the Government. The report shall be prepared for planning work, controlling costs, and generating timely, reliable and valuable information for the Government. Supporting schedules detailing the sub-events required to achieve milestones in the schedule shall also be prepared and maintained. Changes to the schedule shall be highlighted, with reasons for the changes. The Contractor shall address the effect of the changes on interrelated milestones. The Contractor shall also relate technical accomplishments with cost and schedule accomplishments, as well as highlighting any risks that the Contractor has identified with details on the nature of the risk, and planned and/or implemented mitigation steps. When delivering the Contractor's Progress, Status and Management Report, the Contractor shall alert the NILE Project Manager in writing to any open risks, with a status summary. The Contractor shall include a status of their own performance relative to the QASP within the report.

References
CDRL A001 – Contractor's Progress, Status and Management Report
CDRL A002 – Government Furnished Equipment (GFE) Report

5.3 Post-Award Conference

The Contractor shall host an in-person Post-Award Conference (PAC) no later than ten (10) business days after contract award, unless the Government agrees to a later date. The Government will establish specific dates in coordination with the Contractor. The agenda shall be developed by the Contractor and shall include the following:

a) Introduction and identification of key Government and Contractor management and engineering personnel;
b) The Contractor's management organization, plans, procedures, and schedules;
c) The Government's management organization, plans, procedures, and schedules;
d) Government concerns;
e) Contractor concerns;
f) Status of GFE/GFI;
g) Status of submittals and approvals of regulatory issues, i.e. export, security;
h) Status of subcontracts, if any; and
i) Other tasks established by the Government in conjunction with the Contractor.

The Contractor shall prepare and submit minutes of the Post Award Conference.

Reference

CDRL A003 – Conference Agenda
CDRL A004 - Conference Minutes
CDRL A005 – Briefing Materials

5.4 In-Process Review (IPR)

Commencing with the Post Award Conference, the Contractor shall conduct IPRs, which should be available both in-person and virtually. The Contractor shall present and administratively support IPRs. The location of all IPRs shall be agreed mutually between the Contractor and the Government. An IPR shall be performed quarterly or as required by the Government. The Contractor shall develop agendas and minutes for the IPR for Government approval. The Government will have the right to modify or add items to the IPR agenda. At the IPR, the Contractor shall determine and report detailed project status information, keyed to the CDRLs, and CLINs, including proposed sub-contractor work. The Contractor shall prepare and submit minutes for each IPR within 10 business days after the IPR.

Reference
CDRL A003 – Conference Agenda
CDRL A004 - Conference Minutes
CDRL A005 – Briefing Materials

6. SECURITY

6.1 Physical Security

The Contractor's classroom-based Link 22 course design shall meet the following physical security requirements for protecting the confidentiality of CUI in classroom training facilities including all hardware, software, and audiovisual equipment. The Contractor shall ensure that the location of any classroom-based training courses conforms to the following physical security requirements:

a. Limit physical access to Link 22 systems, equipment and information to authorized individuals only. Premises shall have access controls in place to limit unauthorized access;
b. Classroom shall not have any public access points (e.g. doors or windows that open to a public area);
c. Protect and monitor they physical facility and infrastructure (e.g. employment of guards, use of sensor devices, use of video surveillance);
d. Link 22 materials, equipment, data and any Government Furnished Information or Equipment left on-site shall be secured in accordance with its classification markings;
e. Visitors must be escorted, and their activity monitored (e.g. use audit logs of physical access); and,
f. Enforce safeguarding measures for CUI at alternate work sites. Contractor will ensure that all employees accessing CUI from an alternative site/remote site are following the proper security guidelines. Alternative work sites may include government facilities or private residence. (Enterprise and user security guidance when teleworking is provided in the National Institute of Standards and Technology publication (NIST SP 800-114).

6.2 Information Security

The Contractor shall ensure the following security requirements are followed when handling digital and non-digital information. It is the responsibility of the Contractor to ensure the confidentiality of CUI material is maintained when accessing information from local or via remote means:

a. Protect project information containing CUI both paper and digital. If digital media is to be used to transfer information (e.g. removable hard disk drives), it is the responsibility of the Contractor to implement cryptographic mechanisms for example using encrypted removable hard drive to ensure security of CUI data;
b. Limit access to CUI data on systems to only authorized individuals;
c. Sanitize or destroy media containing CUI data before disposal or release for reuse. The Contractor shall use their organization's discretion on the employment of sanitization techniques and procedures for media containing information. (For more information regarding proper sanitization of media follow NIST SP 800-88);
d. Information, storage, and removable media should be marked with necessary CUI markings and distribution limitations;
e. Prohibit the use of portable devices when such devices are not owned and managed by the Contractor; and,
f. Protect the confidentiality of backup software that stores Link 22 and CUI data.

6.3 Cloud Platform Security

The Contractor shall ensure that any cloud-based platform used to access Link 22 information complies with Impact Level 5 (IL-5): Controlled Unclassified Information and Unclassified National Security Information of the DoD Cloud Computing Security Requirements Guide (SRG) (latest version). The Contractor shall submit the Body of evidence (BoE)/security artifact documentation to the Government for review on an annual basis and must show that the cloud platform complies with all IL-5 SRG latest version requirements.

The Contractor shall use an established cloud platform that meets IL-5 SRG requirements which will allow the trainers and students to access the information remotely. If the Contractor plans to use a third-party to manage the cloud platform, the Contractor shall provide BoE of IL-5 requirements to the Government on an annual basis for review.

If the Contractor plans to use third-party cloud computing service, the Contractor shall ensure the software is registered on the DoD Cloud Service Catalog (https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/cloud-service-support), in accordance with DFARS Procedures, Guidance and Instructions (PGI) 239.7603-1.

6.4 Hardware and Software

The Contractor shall ensure any equipment/system being used to deliver the training will meet the cybersecurity requirements as specified under DoDI 8500.01. The Contractor shall ensure that any configuration change, change of hardware or software is in accordance with established DoD/DON/Navy cyber directives. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used. Procurement and installation of software

governed by DON Enterprise License Agreements (ELAs) shall be in accordance with DON CIO Policy and DON ELAs awarded. A list of ELAs that are in effect can be found at www.esi.mil. The Contractor shall store all product/system information and have it available for government review as needed.

References
CDRL A009 – Cloud Platform Body of Evidence

7. CYBERSECURITY

7.1 System Security Plan

Within thirty (30) days of contract award, the Contractor shall make its System Security Plan (SSP) for its covered contractor information system(s) available for review by the Government at the Contractor's facility. The SSP shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012. The Contractor shall fully cooperate in the Government's review of the SSP at the Contractor's facility.

If the Government determines that the SSP does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The Procurement Contracting Officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a Plan of Actions and Milestones (POA&M) for the correction of the identified deficiencies. The Contractor shall immediately notify the Procurement Contracting Officer of any failure to meet a milestone in such a POA&M.

Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP.

The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP. The Government will conduct such reviews at least once per year and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

Compliance to the NIST 800-171

7.1. The Contractor shall fully implement the CUI security requirements and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (rev. 1) *NISP SP 800-171), or establish an SSP and POA&M that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

7.2. Notwithstanding the allowance for such variation, the Contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

7.2.1. Implement Control 3.5.3 (multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a

network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

7.2.2. Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the Contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

7.2.3. Implement Control 3.1.12 (monitoring and control remote access sessions) – require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods;

7.2.4. Audit user privileges on at least an annual basis;

7.2.5. Implement:

7.2.5.1. Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in an SSP and POA&M); and,

7.2.5.2. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

7.2.6. Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POA&M for implementation which shall be evaluated by the Navy for risk acceptance; and,

7.2.7. Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

7.2 Cyber Incident Response

a. The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

b. Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/instructions_for_submitting_media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

c. If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the Procurement Contracting Officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The Procurement Contracting Officer will approve or disapprove the request after coordination with DC3.

7.3 Naval Criminal Investigative Service (NCIS) Outreach

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

7.4 NCIS/Industry Monitoring

a. In the event of a cyber-incident or at any time the Government has the indication of a vulnerability of potential vulnerability, the Contractor shall cooperate with the NCIS, which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the Contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.
b. If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.
c. In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-U.S. law.

References
CDRL A007 – Information Security (IS) Plan of Action & Milestones (POA&M)
CDRL A008 – reserved
CDRL A00A – Physical Asset Body of Evidence

8. PERSONNEL QUALIFICATIONS

Personnel assigned to or utilized by the Contractor in the performance of this contract should, at a minimum, meet the desired experience, skills, and qualifications set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner. If the Offeror does not identify the labor categories listed below by the same specific title, then a cross-reference list should be provided in the Offeror's proposal identifying the difference.

The Government may review resumes of contractor personnel proposed to be assigned at the Task Order level. If personnel are not currently employed by the Contractor, a written agreement from potential employee to work will be part of the technical proposal.

If the Ordering Officer questions the qualifications or competence of any persons performing under the contract, the burden of proof to sustain that the person(s) are qualified as prescribed herein shall be upon the Contractor.

The Contractor must have personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in task orders. The work history of each Contractor employee shall contain experience directly related to the tasks and functions to be assigned. The Ordering Officer reserves the right to determine if a given work history contains necessary and

sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance.

Labor Category	Desirable skills, experience and qualifications
Junior training and development specialist	International English Language Testing Systems (IELTS) band 8 (or equivalent) at a minimum, unless the Offeror's first language is English, in which case no language skills certification is required. Operational TDL (ideally Link 22) experience and expertise, including in DTDMA. 2 years' experience (gained in the last 3 years) delivering technical training (preferably in the TDL field) to international Government/military personnel Proficient user of MS Office suite, including MS Teams, and proposed online training platform.
Mid training and development specialist	International English Language Testing Systems (IELTS) band 8 (or equivalent) at a minimum, unless the Offeror's first language is English, in which case no language skills certification is required. Operational TDL (ideally Link 22) experience and expertise, including in DTDMA. 4 years' experience (gained in the last 6 six years) delivering technical training (preferably in the TDL field) to international Government/military personnel. Expert user of MS Office suite, including MS Teams, and proposed online training platform.
Senior training and development specialist	International English Language Testing Systems (IELTS) band 8 (or equivalent) at a minimum, unless the Offeror's first language is English, in which case no language skills certification is required. Operational TDL (ideally Link 22) experience and expertise, including in DTDMA. 5 years' experience (gained in the last 7 years) delivering technical training (preferably in the

	TDL field) to international Government/military personnel. Expert user of MS Office suite, including MS Teams, and proposed online training platform.
Junior Admin assistant	2 years' experience in a similar role, supporting a Navy program with administrative tasks Proficient user of MS Office suite, including MS Teams. Experience with Task Orders, and financial administration of CPFF and FFP contracts.
Task Order PM	International English Language Testing Systems (IELTS) band 8 (or equivalent) at a minimum, unless the Offeror's first language is English, in which case no language skills certification is required Expert user of MS Office suite, including MS Teams
Mid IT specialist	Expert user of proposed online training platform
Mid software engineer	Expert user of proposed online training platform.
Mid instructional systems designer	Expert user of MS Office suite, and proposed online training platform. 5 years' experience (gained in the last 7 years) designing technical training courses, including Train the Trainer, and preferably in TDL field. Experience desired to include producing training materials, designing examinations, tests, interactive exercises etc.

9. PATENT MATTERS

The Point of Contact regarding Patent Matters for this contract is:

For HQ or NIWC-PAC
Office of Patent Counsel / Code 36000
NIWC Pacific
53560 HULL STREET
San Diego, CA 92152-5001

(619) 553-3001

For NIWC-Atlantic use:

Legal Office - Patent Counsel
NIWC-Atlantic Code 36000
PO Box 190022
N. Charleston, SC 29419-9022
(843) 218-5569

Do not submit interim final invention reports to this address.

10. REIMBURSEMENT OF TRAVEL COSTS

Any travel under the contract must be specifically identified by the contractor in a written quotation to the Ordering Officer prior to incurring any travel costs. Travel under this contract is only authorized under task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order.

11. REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION

As used in this text, “sensitive information” includes:

a) All types and forms of confidential business information, including financial information relating to a contractor’s pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
b) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 2101-2107);
c) Information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;
d) Other information designated as sensitive by the Naval Information Warfare Systems Command (NAVWARSYSCOM).

In the performance of the contract, the Contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements. Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The Contractor shall:

a) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;

b) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation; Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure;
c) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment; and,
d) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

In the event that the Contractor inadvertently accesses or receives any information marked as proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the Contractor may not be authorized to access such information, the Contractor shall:

a) Notify the Contracting Officer; and,
b) Refrain from any further access until authorized in writing by the Contracting Officer.

The requirements of this text are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government Information Systems. Subcontracts. The Contractor shall insert the above paragraphs in all subcontracts that may require access to sensitive information in the performance of the contract. Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the Contractor's plan to implement the requirements of the above language and shall include the use of a firewall to separate Contractor personnel requiring access to information in the performance of the contract from other Contractor personnel to ensure that the Contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The Contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

12. REPRESENTATION OF COMPLIANCE WITH THE ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) ACCESSIBILITY STANDARDS

The Offeror represents that it will / will not deliver Electronic and Information Technology (EIT) that complies with the EIT Accessibility Standards at 36 C.F.R. § 1194.

If the Offeror represents that it will not deliver EIT that complies with the EIT Accessibility Standards at 36 C.F.R. § 1194, it shall complete the following table:

Item	Rationale for Not Providing Compliant EIT

13. TRADEMARK LANGUAGE

The Contractor shall not assert any claim, in any jurisdiction, based on trademark or other name or design-based causes of action that are based on rights the Contractor believes it has in the term(s) NILE, Link 22, NRS, SNC, NAVWAR and NAVWAR geometric triangle mark (the "Designation(s)"), against the Government or others authorized by the Government to use the Designation(s) (including the word(s), name, symbol, or design) acting within the scope of such authorization (i.e. claims for trademark infringement, dilution, trade dress infringement, unfair competition, false advertising, palming off, passing off, or counterfeiting). Such authorization shall be implied by the award of a Government contract to any party for the manufacture, production, distribution, use, modification, maintenance, sustainment, or packaging of the products and services identified under this contract, and the scope of such implied authorization is defined as the use of the Designation(s) in performance under such contract by the prime Contractor and its subcontractors and suppliers at any tier. In all other cases, the scope of the authorization will be defined by the Government in writing.

The Contractor shall notify the contracting officer at least 30 days before asserting rights in, or filing an application to register, any one of the Designation(s) in any jurisdiction within the United States. Any such notification shall be in writing and shall identify the Designation(s) (including the word(s), name, symbol, or design), provide a statement as to its intended use(s) in commerce, and list the particular classes of goods or services in which registration will be sought.