PERFORMANCE WORK STATEMENT (PWS)

FOR

NORTH ATLANTIC TREATY ORGANIZATION (NATO) IMPROVED LINK ELEVEN (NILE) PROGRAM OFFICE

COMMAND AND CONTROL SYSTEMS (PMW 150)

IN-SERVICE SUPPORT (ISS) 6 ENGINEERING SERVICES

28 January 2026

Revision History

Version	Reason for Change	Date

Table of Contents

1 SCOPE

This Performance Work Statement (PWS) establishes the requirements for the continued modification, maintenance and configuration control of the NILE products. It is to provide Engineering, Project Management Services, Development and Testing of the System Network Controller (SNC) and NILE Reference System (NRS) as well as its associated test laboratory, test tools and documentation. These services to be acquired under this effort span the Sustainment cycle of the program and the tasks performed require collaboration and sharing of information within the Link 22 Community. The goal of Link 22 is to improve allied interoperability, complement other Tactical Data Link (TDL) capabilities and to enhance the warfighting capability. Link 11 sunset date was 31 December 2024, and the upcoming Block Cycle Release update is expected to be delivered in late 2026.

1.1 INTRODUCTION

The Program Executive Office Command, Control, Communications, Computers, and Intelligence (PEO C4I), Navy Command and Control Program Office (PMW 150) provide intuitive, innovative, resilient Command and Control and Tactical Communications solutions to the warfighter to enable better decisions faster. The North Atlantic Treaty Organization (NATO) Improved Link Eleven (NILE) Nations Program Management Office (PMO) is conducted collaboratively by seven nations under the guidance of a Memorandum of Understanding (MOU).

The Tactical Data Link (TDL) system provided by the NILE PMO has officially been designated Link 22. It is a secure radio system that provides Beyond Line-Of-Sight (BLOS) communications. It interconnects air, surface, subsurface, and ground-based tactical data systems, and it is used for the exchange of tactical data among the military units of the participating nations.

Link 22 is a new design developed to replace and overcome the known deficiencies of Link 11 showcasing Dynamic Time Division Multiple Access (DTDMA) capability and to compliment and interoperate easily with other TDL capabilities.

Development, Security, Operations (DevSecOps) principles shall be deployed to deliver all the work during the period of performance.

1.2 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 MOU. The original seven nations were Canada (CAN), France (FRA), Germany (DEU), Italy (ITA), the Netherlands (NLD), the United Kingdom (GBR) 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”.

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, provides better Real Time Tactical access compared to Satellite Communications and improves Allied Interoperability through Common Design. Link 22 offers a BLOS tactical data link that is designed to fully complement its Link 16 Line of Sight (LOS) counterpart, 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 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 Link 22 system is depicted by Figure 1 below. All NILE interface specifications (the orange and yellow 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.

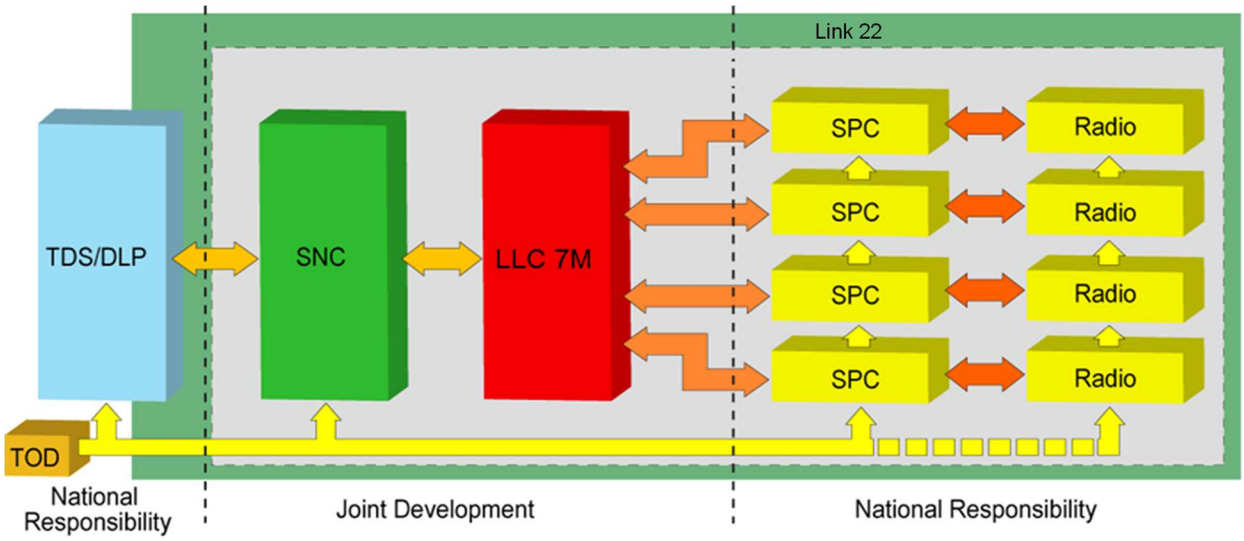

Figure 1- Link 22 System with NILE Communication Equipment

The SNC provides common operational software that is compatible among the 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 security 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".

2 APPLICABLE REFERENCE DIRECTIVES/DOCUMENTS

The Contractor shall adhere to the most current version of all documents listed. The Contractor shall comply with any changes to laws, regulations, policies and instructions during the performance of this contract.

2.1 Department of Defense (DoD)Specifications (Latest version)

Document Ref	Title
DoDI 5000.02	Operation of the Adaptive Acquisition Framework
DoDI 5000.64	Accountability and Management of DoD Equipment and Other Accountable Property
DoD I 5000.74	Defense Acquisition of Services
DoDI 5000.75	Business Systems Requirements and Acquisition
DoDI 5000.87	Operation of Software Acquisition Pathway
DoDI 5200.48	Controlled Unclassified Information (CUI)
DoDI 5220.22-M	National Industrial Security Program Operating Manual (now Part 117 of Title 32, Code of Federal Regulations)
DoDI 5230.11	Disclosure of Classified Military Information to Foreign Governments and International Organizations issued 7 Nov 23
DoDI 5230.24	Distribution Statements on DOD Technical Documents
DoD Manual 7000.14-R	DoD Financial Management Regulation, Volume 2B, Chapter 18 citation Department of Defense Financial Management Policy.
DoDD 8140.01	DoD Directive –Cyberspace Workforce Management dtd 05 Oct 20
DoDI 8320.02	Sharing Data, Information and Information Technology (IT) Services in the Department of Defense with change 1
DoD Manual 8400.01-M	Accessibility of Information and Communications Technology (ICT)
DoDI 8500.01	DoD Instruction – Cybersecurity
DoDI 8510.01	Risk Management Framework (RMF) for DoD Systems)
DoD 8570.01-M	Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change
DON CDO	DON Implementation Plan of the Department of Defense Data Strategy
DON CDO	Naval Data Management Concept of Employment
DON CIO Memo	Coding of DON Positions Performing Cybersecurity Functions
DON CIO Memo	Acceptable Use of Department of the Navy Information Technology (IT)
DOD Memo	Guidance Regarding Cyberspace Roles, Responsibilities, Functions, and Governance within the DOD
DON CIO Guidance	DON CIO Cybersecurity Strategy Guidance
DON CIO Memo	Guidance for Cybersecurity Workforce Operating System/Computing Environment Certification Compliance Process
Navy Telecoms Directive (NTD 10-11)	System Authorization Access Request (SAAR) – Navy
SECNAVINST 4440.34	IMPLEMENTATION OF ITEM UNIQUE IDENTIFICATION WITHIN THE DEPARTMENT OF THE NAVY
SECNAVINST 5239.25	Department of Navy Cyberspace Workforce Qualification and Management Program
SECNAVINST 5239.3C	DON Cybersecurity policy,
SECNAVINST M- 5239.3	Cyber Security Manual (published Apr 2022)
SECNAV M-5239.2	DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual
SECNAV M-5210.1	DON Records Management Program
NAVWARINST 5401.8	NAVWAR Information Superiority Governance Instruction
SECNAVINST 5510.36B	Department of the Navy Information Security Program

SECNAV M-5214.1	DON Information Requirements (Reports) Manual
SPAWARINST 12293.1	Civilian Employee Check-in/out Procedures
SPAWARINST 5270.5C	Information Technology Asset Registration and Management
Version 1.0	DoD Agile 101: An Agile Primer (version date: 18 Nov 2019)

2.2 Department of Defense Standards (Latest Version)

Document Ref	Title
MIL-HDBK-61A (SE)	Configuration Management Guidance,
MIL-STD-130N	Identification Marking of U.S. Military Property
MIL-STD-882E	DEPARTMENT OF DEFENSE Standard Practice for System Safety, 11 May 2012
ANSI/EIA 649B	Configuration Management Requirements for Defense Contracts, 20 November 2014
ISO 9001:2015	Quality Management Systems – Requirements, 23 September 2015
ISO 10007:2017	Quality Management Guidelines for Configuration Management 2017
ISO/IEC 8652	Information Technology, programming languages – Ada, 28 March 2013, with COR.1 1 February 2016
ISO/IEC/IEEE 12207:2017	Systems and Software Engineering – Software Lifecycle Process
MIL-PRF-49506	S/S by GEIA-STD-0007 Logistics Management Information

2.3 Other Government Documents

2.3.1 NATO Standards and Documents (latest edition)[1]

Document Ref	Title
STANAG 4107	Mutual Acceptance of Government Quality Assurance
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 4372	SATURN – A fast frequency hopping ECCM mode for UHF radio
STANAG 4430*[2]	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
STANAG 5616	STANDARDS FOR DATA FORWARDING BETWEEN TACTICAL DATA SYSTEMS EMPLOYING LINK 11/11B, LINK 16 AND LINK 22
STANAG 5522	Link 22 Tactical Message Standard
ATDLP-5.16	Allied Tactical Data Link Publication (ATDLP) 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)
APP–11	NATO MESSAGE CATALOGUE
AQAP-2110 Ed D, v1	NATO quality assurance requirements for design, development and production
AQAP 2210 Ed A, v2	NATO supplementary software quality assurance requirements to AQAP 2110 or AQAP 2310
NATO SDIP-29	Installation of Electrical Equipment for the Processing of Classified Information

[1] NATO SECRET (NS) for STANAG 4372, 4444. All other NATO documents listed are NATO Unclassified (NU)

[2] * Means these STANAG's have been withdrawn and mentioned for information purposes only due to being utilized a previous version of Link 22 BCR.

2.3.2 NILE Documents (Latest version)[3]

NILE PMP	NILE Program Management Plan
NILE CMP	NILE Configuration Management Plan
NILE PSI	NILE Project Security Instruction
NILE QMP	Quality Management Plan
NILE BCR	Block Cycle Release documents
NILE CPs	NILE Change Proposals
NILE WPs	NILE White Papers
NILE PCRs	NILE Problem Change Reports
NILE FRs	NILE Feedback Reports

2.3.3 COMSEC Documents (Latest edition)

CNSSI No. 4005	Safeguarding Communications Security (COMSEC) Facilities and Materials
CNSS Instruction 4003	Reporting and Evaluating Communications Security (COMSEC) Incidents
007-500028-001	LLC 7M Installation, Configuration, and Operations Instructions, Revision C, Apr 2016
PI-L22D-RM-03	LINK-22 Modernized Link Level COMSEC (MLLC) System/Subsystem Specification
PI-L22D-DP-10	Key and Certificate Management Plan (KCMP)
007-500028-001	LLC 7M Installation, Configuration and Operation Instruction (includes Outline and Mounting Drawings) LLC 7M Outline Solid Model (PDF/STEP format)
PI-L22D-TP-41	TEMPEST Test Evaluation Report
PI-L22D-TP-31	Environmental Test Report

2.4 BCR Documents

The table below constitutes the initial list of documents and version numbers. The Government will provide most current, applicable dates and version numbers of the documents at Task Order Contract award. This table may be updated throughout the lifetime of the contract. The CMIS Document Database will document the current baseline.

* Documents marked with an asterisk do not have to go through the formal CP process for revision. The documents without an asterisk will need to be updated if the SNC code changes.

Document Title	**Document Version**	**CDRL#**
*Software Test Description (STD) for the System Network Controller	As per latest BCR	B002
*Software Test Description (STD) for the System Network Controller	As per latest BCR	B002
*Software Version Description (SVD) for the System Network Controller	As per latest BCR	B002
Data Extraction and Reduction Document	As per latest BCR	B002
Interface Design Description for the DLP-SNC-IDD	As per latest BCR	B002
Interface Design Description for the NRS (IDD IRS)	As per latest BCR	B002

[3] Upon Contract award, all previously approved WPs will be provided and shall be utilized to deliver subsequent updates.

Document Title	Document Version	CDRL#
Interface Requirement Specification for the Link Level COMSEC Segment (LLC IRS)	As per latest BCR	B002
Media Simulation Software Requirement Specification	As per latest BCR	B002
*NILE Requirements Traceability Matrices	As per latest BCR	B002
Scenario Generator Software Requirement Specification	As per latest BCR	B002
Segment Specification for the Signal Processing Controller (SPC SS)	As per latest BCR	B002
Segment Specification for the System Network Controller (SNC SS)	As per latest BCR	B002
Software Design Description for the System Network Controller (SNC SDD)	As per latest BCR	B002
System Specification for the NILE Reference System	As per latest BCR	B002
System Technical Manual for the NILE Reference System	As per latest BCR	B002
System Technical Manual for the System Network Controller	As per latest BCR	B002
Glossary	As per latest BCR	B002
Software Test Description (STD) for the NILE Reference System*	As per latest BCR	B002
Software Version Description (SVD) for the NILE Reference System*	As per latest BCR	B002
Signal Processing Controller (SPC) Serial Splitter Segment Specification (SSS SS)	As per latest BCR	B002
*NRS Software Test Report (STR)	As per latest BCR	H001
*SNC Software Test Report (STR)	As per latest BCR	H001
Link 22 Guidebook	As per latest BCR	B00E
Configuration Management Information System (CMIS)*	As per latest	B00D

In the event of a conflict between the text of this Performance Work Statement and the references cited herein, the text of this document shall take precedence. The documents listed above may be invoked, for guidance only, on individual task orders. Additional applicable documents may be included in individual task/delivery orders. Nothing in this document, however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained.

3 PERFORMANCE REQUIREMENTS

3.1 General Requirements

The Contractor shall prepare and deliver products in accordance with the applicable directives stated in this PWS. The Contractor shall provide necessary resources with knowledge and experience as cited in the personal qualification requirement to support the listed tasks. The Contractor shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) that do not include performance of inherently Government functions.

The Contractor shall provide necessary resources and knowledge to support the listed tasks and to analyze data and provide technical comments, questions and recommendations for the NILE PMO. The Contract Data Requirements Lists (CDRLs) are identified in Section 6.1.

The Contractor shall complete tasks while controlling and tracking performance and goals in terms of costs, schedules, resources and technical performance.

The Contractor shall provide personnel proficient in the use of tools, technologies and software applications for productivity, collaboration and systems architecture. Some examples include but not limited to:

- Collaboration/CM: SharePoint, JIRA, Jenkins
- Architecture: Visio
- Productivity: Microsoft 365, MS Project

Specific objectives will be dependent on the individual Task Orders issued against this contract. This will require the Contractor to provide engineering services to support NILE products, to include, but not be limited to:

a) Production of Block Cycle Releases (BCRs).
b) Production of BCR Engineering Releases (ER).
c) Design, development, implementation, test, and evaluation of potential engineering changes to NILE products and their interfaces as defined in the Task Order.
d) Establishment and maintenance of a NILE laboratory development and test environment for end-to-end Link 22 system to perform compatibility and interoperability testing with a focus on test automation.
e) Support of NILE Nations and Link 22 Partner Nations in their implementation of Link 22.
f) Maintenance and update of NILE documentation, to include maintenance and configuration management of NILE software, hardware and document repositories.
g) Providing Link 22 system expertise to the Link Level Communications Security 7M (LLC 7M) manufacturer, to support the integration of the LLC 7M into the Link 22 architecture.
h) Project management and government support services, also applying to Link 22-related international forums.
i) Support the deployment of the NILE PMO's Mobile Test Station at various field events.
j) Modification and delivery of existing software baselines to incorporate new incremental NILE capabilities; and,
k) Perform system-engineering analysis and evaluation associated with operational software baseline development, and requirements implementation.

3.2 Engineering Services

The Contractor shall provide technical/engineering services to the NILE PMO with respect to tasks in this PWS and defined in Task/Delivery Order.

3.2.1 System Network Controller (SNC) C++

The Contractor shall ensure that any modifications to the SNC application and Time of Day (TOD) Software is written in C++ as the modern software coding language.

The Contractor shall provide a management plan of how code language would be monitored, tested and validated in accordance with DevSecOps principles (where possible); and, test cases that will be performed on new code to ensure functionality, including regression tests. When the SNC is used on an X64 machine and the SNC is the only application running on the machine (TOD software is installed with the SNC), the SNC shall meet all minimum performance requirements listed below while in operation:

METRIC	OBJECTIVE	THRESHOLD
Processor	Processor: **2 GHz (dual core)** or **3 GHz (Single core)**. Shall not exceed **10%** of total available mean CPU resource, averaged over **10 minutes** in established state, using the **scenario 1**	Processor: **2 GHz (dual core)** or **3 GHz (Single core)**. Shall not exceed **25%** of total available mean CPU resource, averaged over **10 minute**s in established state, using the **scenario 1**
Memory usage	Maximum memory usage for software running **scenario 1**, averaged over **one day** in established state, shall not exceed **512 MByte**	Maximum memory usage for software running **scenario 1**, averaged over **10 minutes** in established state, shall not exceed **1 GByte**
Hard drive	SNC application shall not exceed **20 MByte**	SNC application shall not exceed **100 MByte**
Ethernet	**100 Mbytes** connection	
Boot time	OS has been booted and otherwise fully made ready for operations, the SNC software shall start to operational mode within a maximum time of **5 seconds**	OS has been booted and otherwise fully made ready for operations, the SNC software shall start operational within a maximum time of **30 seconds**
Shutdown time	SNC software shall stop operational mode and application be closed within a maximum time of **5 seconds**	SNC software shall stop operational mode and application be closed within a maximum time of **30 seconds**

List of Scenarios:

- Scenario 1: 1000 tactical data link objects with 20 NILE units on 4 NILE Networks
- Scenario 2: 200 tactical data link objects with 10 NILE units on 2 NILE Networks.

CDRL Deliverables:

A001 – Contractor's Progress, Status and Management Report
A00A – Technical and Management Work Plan
A00E– Integrated Master Schedule
B001 – Technical Report
B002 – BCR Documents
B003 – BCR Executable Software (SNC and NRS)
B004 – BCR Engineering Release Executables (SNC and NRS)
B005 – BCR Source Code (SNC and NRS)

3.2.2 NILE Reference System (NRS) Upgrade

The Contractor shall develop, build, test and modify the NRS Architecture and configuration. The Contractor shall complete the modernization of SNC Diamond(SNCD) to Multi Units Test Simulator (MUT Sim) in C++. The Contractor shall maintain updates on all relevant documentation post Critical Design Review (CDR) to reflect any implemented changes. The contractor shall collate up to five (5) discrepances identified during the NRS Upgrade into a single Feedback Report.

CDRL Deliverables:

B001 – Technical Report
A00E– Integrated Master Schedule

3.2.3 Modular, Open Design

The Contractor shall provide software products having an architecture that is layered and modular and uses standards-based commercial item/NDI software, operating systems, and middleware that shall utilize either non-proprietary or non-vendor-unique key module or component interfaces where available. Furthermore, and to support a wide range of operational environments (such as NILE and Link 22 Partner Nations utilizing unique Tactical Data System (TDS) and interfaces), the Contractor shall apply a modular open systems approach to its software products so that they are more robust, maintainable, and easier to update over time. The modular open systems approach should have common standard interfaces and shall divide "large software entities" into smaller modules to allow for ease of integration, delivery, and maintenance. Unless specified differently at the Task Order level, any software components, applications or software or interface data that are developed under the contract will be considered non-commercial software that is developed at Government expense. The Contractor's design approach shall be consistent throughout all subsystems and components.

Module Coupling – The Contractor's design approach shall result in modules that have minimal dependencies on other modules (loose coupling), as evidenced by simple, well-defined interfaces and by the absence of implicit data sharing. The purpose is to ensure that any changes to one module will not necessitate extensive changes to other modules and hence facilitate module replacement and system enhancement.

Module Cohesion – The Contractor's design shall result in modules that are characterized by the singular assignment of identifiable and discrete functionality (high cohesion). The purpose is to ensure that any changes to system behavioral requirements can be accomplished by changing a minimum number of modules within the system.

System Requirements Accountability – The Contractor shall ensure that all software requirements in this PWS are accounted for through a demonstrated ability to trace each requirement to one or more modules that consist of components that are self-contained elements with well-defined, open, and published interfaces implemented using open standards.

Inter-component Dependencies – The Contractor's design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh. The design shall be able to survive a change to the computing infrastructure with minimal or no changes required to the application logic. The interfaces between the layers shall be built to open standards or the technical data describing the interface shall be available to the Government with at least Government Purpose Rights. The software architecture shall minimize inter-component dependencies to allow components to be decoupled and reused, where appropriate, across various DoD or Service programs and platforms.

CDRL Deliverables:

B002 – BCR Documents
B003 – BCR Executable Software (SNC and NRS)
B004 – BCR Engineering Release Executables (SNC and NRS)
B005 – BCR Source Code (SNC and NRS)
B007 –CMIS Documents
B00D – Configuration Management Information System (CMIS)
B00E – Link 22 Guidebook
H001 – Software Test Plan (STP)
H002 – Software Test Report (STR)
H003 – System Acceptance Testing/Procedures

3.2.4 LLC 7M System Integration

As specified on a Task/Delivery Order, the Contractor shall be required to ensure continued compatibility between the LLC 7M and the NILE products (software, documentation and interfaces) to support the NILE PMO in assessing the system level aspects of the LLC 7M. This shall involve supporting future modifications to COMSEC requirements definition, analysis, integration, and testing. This may include but is not limited to providing continued System-Level Engineering support to the NILE PMO regarding the LLC 7M. The LLC 7M will be issued as Government Furnished Property (GFP), to the Request for Proposal, and the Contractor will not be required to perform any engineering work on the LLC 7M hardware, or internal algorithm.

The support may include:

a) Review of COMSEC updates proposed by the LLC 7M developer/manufacturer and provision of recommendations to the NILE PMO regarding the proposed updates.

b) Independent Verification and Validation (IV&V) of the LLC 7M to evaluate the adequacy and completeness of the LLC 7M, ensuring that it conforms to Link 22 system requirements (excluding requirements relating to the encryption/decryption algorithm)

c) Assessments and/or recommendations on the impact/viability of the Contractor or authority proposals that may affect the Link 22 System.

d) Answering specific technical questions from the NILE PMO relating to the review of system level CDRLs submitted to PEO C4I regarding the LLC 7M. Answers to such questions shall ensure engineering feasibility and compatibility to the Link 22 System

e) Test and analyze COMSEC units reported as ‘not faulty’

f) Remove and replace all three Renata batteries per LLC 7M located at the Contractor’s premises (i.e. 6 units) annually in accordance with the LLC 7M Installation, Configuration and Operation Instructions (Document 007-500028-001); and,

g) Update LLC Simulator (SIM) software when either the COMSEC and/or SNC is modified.

3.2.5 NILE Test Environment/Compatibility Laboratory

As specified in a Task/Delivery Order, the Contractor shall establish/provide and maintain a test environment/compatibility laboratory suitable for the development and maintenance of the NILE Products, and for compatibility and Independent Validation and Verification (IV&V) testing with Link 22 equipment, irrespective of the manufacturer.

The Contractor shall provide the NILE PMO, authorized NAVWAR/US Government personnel and authorized Cooperative Project Personnel (CPP) from all NILE Nations, access to Contractor facilities upon request.

The Contractor shall have an existing facility or be able to secure and establish a fully functional facility [4] within 6 months of award. For testing of some requirements, the Contractor shall identify and implement appropriate procedures necessary to test up to and including U.S. SECRET/NATO SECRET. General support, including NRS/SNC infrastructure and OS support, shall be part of the implementation of the Integrated Support Plan (ISP).

The Contractor shall set-up and maintain a NILE Compatibility Laboratory at the Contractor's site. The Contractor shall ensure availability of the following capabilities:

a) Two operational NRS environments (current and previous Block Cycle) shall be maintained for the duration of the contract. Software will be provided as Government Furnished Equipment (GFE).

b) An operational NILE Interoperability Test Tool (NITT) environment shall be acquired or developed and maintained for the duration of the contract; and

c) Availability of personnel trained in the operation of the NRS components, SNC, SNCd, interfaces, ancillary equipment (e.g. TOD card) and the NITT.

The goal of the NITT is to provide a test tool that supports the development, life cycle support, and performance validation of tactical data link systems (TDLs) employing Link 22, Link 16, JREAP (Joint Range Extension Application Protocol) as well as other communication interfaces. NITT provides capabilities to support the following test types:

i. Conformance tests
ii. Interoperability tests
iii. System integration tests

The NITT allows conformance and interoperability tests to be performed to verify the compliance of TDL implementation with the requirements set forth in the agreed standards. In addition, the Tool provides facilities for developmental testing activity to achieve integration of tactical data link system components (for example, Host/Data Link Processor (DLP), SNC, and communications equipment).

The Contractor shall propose an NITT for use in the NILE laboratory that meets the following requirements for the Government's consideration:

i. The NITT shall implement the most up to date BCR version.
ii. The NITT shall implement the STANAG 5522 Edition 6 or above
iii. The NITT shall be compatible with NRS and the Mobile Test Station (MTS)
iv. The NITT shall display the tactical situation in terms of TDL units, tracks and tactical messages, in human readable format.
v. The NITT shall have a recording function, and the logs must be in human readable format.
vi. The NITT software shall be compatible with Windows 11 (or later) or Linux Red Hat Enterprise Operative Systems (RHEL 9 or later).
vii. The NITT, when used in standalone mode (mainly as a training tool), shall not require any other Link 22 Hardware.

[4] A contractor (either US or foreign owned US) must have a Facility Security Clearance (FCL) commensurate with the highest level of classified access (Secret required for contract performance).

viii. The Contractor shall be an experienced, proficient user of the proposed NITT

The Contractor shall be able to physically transfer the NILE test environment/compatibility laboratory and NILE laboratory equipment to a Government-owned laboratory with appropriate Government clearance as directed by the Government. The Contractor shall be responsible for packaging and transporting the equipment to a location specified by the Government, within the continental United States, as directed by the Contracting Officer. The Contractor shall conduct an ongoing analysis of software and hardware obsolescence issues. These issues shall be reported to the Government as they arise.

CDRL Deliverables:

B006– RMF Package Deliverables
B00A– Information Assurance Test Plan
B00B–Information Assurance Test Report
A00D– Phase out Transition Plan
A003– Government Furnished Report

3.2.6 Assessment and Authorization

The Contractor shall design, develop, and produce the software products in accordance with DoDI Cyber Security 8500.01, the SECNAVINST DoN Cybersecurity Policy 5239.3C, SECNAVINST DoN Information Security Program 5510.36 (Series). While the USG will process the Risk Management Framework (RMF) package for approval, the Contractor shall assist in providing the necessary artifacts throughout the Assessment and Authorization process, to support acquisition of Authority to Operate (ATO). During the system integration event, the Contractor shall verify and document Security Technical Implementation Guideline (STIG) compliance of all system infrastructure components such as servers, clients, network devices, DoD Public Key Infrastructure (PKI) identity and access management systems and any other associated hardware and software products. The Contractor shall issue an Information Assurance Test Report and Plan (CDRL B00A and CDRL B00B). The Contractor shall support the NILE PMO in the development and maintenance of the Ports and Protocols Service Management, (CDRL B00F) that the Government will use to verify Information Assurance compliance.

The Contractor shall support the USG to complete Risk Management Framework (RMF) checklists in accordance with the DoDI 8510.01 RMF Process Guide for DoD Information Technology and deliver the RMF STIG Checklist in (.ckl) format in accordance with CDRL B006 to provide system RMF Accreditation readiness. As required, the Contractor shall provide cybersecurity SME support during the Government's RMF process.

The Contractor shall develop and maintain the following CDRLs in accordance with DoD 8500 Series, RMF Process Guide v3:

a) The Government will provide the Contractor with a list of inherited security controls to be used as part of its accreditation boundary. The Contractor shall utilize the list of inherited security controls to produce and provide the final list of security controls of the NILE software system. The Contractor shall identify the applicability of the Government provided controls of the NILE software system and associated design.

b) The Contractor shall complete the RMF Check Point 2 checklist provided by the Government. Results of the Check Point 2 Checklist shall be provided to the Government 3 days prior to the scheduled RMF Checkpoint 2 date as provided by the Government. CDRL B006, RMF Checklist Report.

c) The Contractor shall complete the RMF Check Point 5 checklist provided by the Government. Results of the Check Point 5 Checklist shall be provided to the Government 3 days prior to the scheduled RMF Checkpoint 5 date as provided by the Government. CDRL B006, RMF Checklist Report.

d) The Contractor shall utilize the Government provided RMF Security Assessment Plan (SAP) template to complete the SAP for each system requiring an RMF Step 3 Collaboration. The SAP must be completed and provided to the Government 5 days prior to RMF Step 3.

e) The Contractor shall complete the Government provided document that serves as "compelling evidence" for RMF documentable control compliance. This includes but is not limited to vulnerability management plan, Continuity of Operations (COOP) plan, contingency planning, maintenance plan, access control plan, incidence response plan, audit and accountability plan.

CDRL Deliverables:

B006 – RMF Package Deliverables
B00A – Information Assurance Test Plan
B00B – Information Assurance Test Report
B00F– Ports and Protocols Service Management.

3.2.7 Backup Policy

The Contractor shall develop and implement data backup procedures based on the risk level of the system and in accordance with DoD policy (ASD STIG v-222638). For this purpose, the Contractor shall ensure that all data on individual workstations is backed up daily on a server equipped with a standard level RAID-5. The Contractor shall backup server data on another Network Attached Storage (NAS), which must be located in a different room, and equipped with a standard level RAID-5, backed up according to the following scheme:

a) Six daily incremental backups shall be maintained on the NAS, one for each of the past six days.

b) Three weekly full back-ups shall be maintained on the NAS, one for each of the past three months.

c) Three monthly full back-ups shall be maintained on the NAS, one for each of the past three months; and

d) For each intermediate delivery, or every quarter (whichever is first), the Contractor shall save the full backups of the last three months in two data sets on HD-BR discs. The Contractor shall deliver one to the NILE PMO, and the Contractor shall keep the other at their facilities in a fireproof safe.

The Contractor shall create and maintain a back-up strategy document explaining the architecture and processes used to comply with the above requirements.

CDRL Deliverables:

A004 –Project Management Plan

3.3 Software Development

The Contractor shall develop and integrate software products and updates to implement system requirements set out by the Government.

3.3.1 Software Repository

The Contractor shall ensure all software files, changes, updates, revisions, and upgrades are documented for traceability, audit and configuration management purposes. The Government retains the right to monitor and review, via the Integrated Product Team (IPT) process, all software information maintained

by the Contractor. The Contractor shall provide a final release at formal delivery for all software modified or purchased under this contract. The Contractor shall provide a final delivery every two years for Link 22 Partner Nations. Using DevSecOps, the contractor shall deliver an intermediate version (Engineering release) every six (6) months if there is a Link 22 improvement ready for national test centers of the NILE Nations. On demand, the contractor shall transform an intermediate version into a final version for delivery to Partner Nations.

CDRL Deliverables:
A001 – Contractor's Progress, Status and Management Report
B002 – BCR Documents
B003 – BCR Executable Software (SNC and NRS)
B004 – BCR Engineering Release Executables (SNC and NRS)
B005 – BCR Source Code (SNC and NRS)
B00D – Configuration Management Information System (CMIS)
B00E – Link 22 Guidebook

3.3.2 NILE Block Cycle Updates

The Contractor shall provide technical/engineering services to the NILE PMO with respect to tasks in this PWS and defined in Task/Delivery Order.

The Contractor shall produce a BCR of NILE products. To deliver BCRs, the Contractor shall (the following list is indicative and is not exhaustive):

a) Conduct technical and support analysis and design of the SNC and NRS modifications and issue resolution.
b) Analyze user stories, identify change requirements and recommend change proposals.
c) Code, integrate and test changes following Government approval through small sprints.
d) Maintain backward compatibility using modular architecture.
e) Update NILE documentation to reflect software changes.
f) Analyze deficiencies identified within the SNC and NRS software versions.
g) Investigate possible deficiencies in the NILE products as they are reported by the NILE Nations or Link 22 Partner Nations during their national Link 22 system integration (to the extent that such items or services do not adversely impact NILE products or compatibility or interoperability among the Link 22 systems of the Nations).
h) Track, mitigate, and report software/hardware obsolescence and maintain interoperability among all identified platforms.
i) Perform modification, automation, implementation and validation of test cases to demonstrate the modified functionality, the non-regression of the existing functionalities of the new BCR and the correct functioning of the interfaces (LLC 7M, SPCs, radios), making full use of existing SNC and NRS Computer Software Configuration Item (CSCI) and System Qualification Test (SQT) procedures and scenarios.
j) Deliver an updated Technical Data Package.
k) Perform a qualification testing phase for both new requirements and non-regression testing, with real and simulated equipment.
l) Schedule and conduct a Test Readiness Review (TRR) prior to the conduct of both formal CSCI and SQT acceptance tests.

CDRL Deliverables:
A001 – Contractor's Progress, Status and Management Report
A005 – Meeting Agenda
A006 – Meeting Minutes
A00A – Technical and Management Work Plan

A00E– Integrated Master Schedule
B001– Technical Report
B002 – BCR Documents
B003 – BCR Executable Software (SNC and NRS)
B004 – BCR Engineering Release Executables (SNC and NRS)
B005 – BCR Source Code (SNC and NRS)
B007 –CMIS Documents
B009– Software Quality Report and Code Quality Report
B00D– Configuration Management Information System (CMIS)
H002 – Software Test Report (STR)
H003 – System Acceptance Testing/Procedure

3.3.3 Engineering Release

The Contractor shall deliver intermediate releases (referred to Engineering Releases (ERs)) of the SNC to the Government as specified in the Task Order. These intermediate releases will include an updated and tested version of the SNC as specified in a Task Order. Intermediate deliveries must be delivered via a government-approved virtual method, as specified in the Task Order. The Contractor shall clearly mark intermediate releases as such, to avoid any confusion with the BCR release. The markings must appear in the name of the executable file and while launching and running the software, on the Human Machine Interface (HMI). Intermediate deliveries are part of the iterative process as explained in DevSecOps guidance.

CDRL Deliverables:

A001 – Contractor's Progress, Status and Management Report
B001– Technical Report
B004 – BCR Engineering Release Executables (SNC and NRS)
B005 – BCR Source Code (SNC and NRS)
B00D– Configuration Management Information System
H002 – Software Test Report (STR)
H003 – System Acceptance Test Plan/Procedure

3.3.4 Technology Insertion

The Contractor's architectural approach shall support the rapid and affordable insertion and refreshment of technology through modular design and the use of open standards and open industry-standard interfaces. The Government expects delivery of interfaces with sufficient intellectual property rights or data rights to allow the Government to maintain or have a third party maintain the interfaces on the Government's behalf.

The Contractor shall define the functional partitioning of the interfaces and the logical modularity of the system software subsystems and components with sufficient detail to facilitate future replacement of specific subsystems and components on either side of the interfaces without impacting other parts of the system and to encourage third-party vendor's participation.

The Contractor use of proprietary, vendor-unique or closed interfaces may be undesirable to the Government.

If applicable, the Contractor shall define its process for identifying and justifying proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software to be used. When interfaces, hardware, firmware, or modules that are proprietary or vendor-unique under this Task order are proposed for delivery, the Contractor shall demonstrate to the Government that those proprietary elements do not preclude or hinder the Government, other component or module developers performing on the Government's behalf from interfacing with or otherwise developing, replacing, or upgrading open parts of the system to accomplish the rapid and affordable insertion and refreshment of technology.

CDRL Deliverables:

B001 – Technical Report
B004 – BCR Engineering Release Executables (SNC and NRS)

3.3.5 Development Security and Operations (DevSecOps)

The Contractor shall propose a clear road map to developing a DevSecOps strategy and explanation of the continuous delivery pipeline (CDRL A004 – Project Management Plan).

In support of this effort, the Contractor will bring to bear industry and Government practices for elements of DevSecOps such as code repository management, configuration management, branching/merging code, building automation, test code coverage, and automated scanning tools. These practices and their manner of accomplishment are depicted by Figure 2 above and

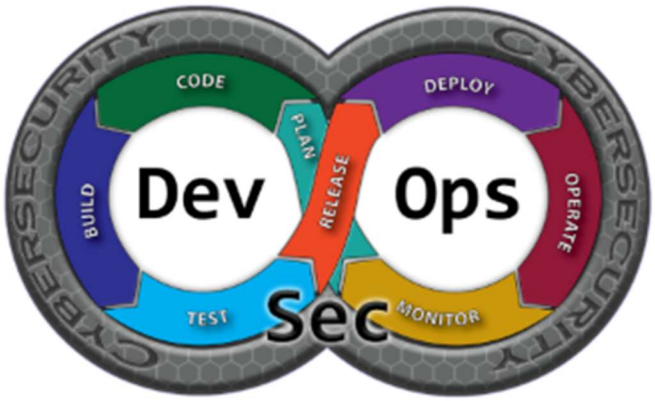

Figure 2 DevSecOps Principles

The DevSecOps support and environment shall include (at a minimum):

a. Installing and configuring application lifecycle management, continuous integration/continuous delivery, and continuous monitoring tools.
b. At a minimum, continuous integration shall implement the necessary toolsets (and platforms) and processes for software build change management, content / build scanning, software and unit testing, and packaging. Additionally, continuous integration shall include automation toolsets to implement version control for source code modification, changes, and repository.
c. Continuous delivery to the Product Owner shall implement the necessary toolsets and processes to automate software builds into production. At a minimum, continuous delivery shall implement software QA environment, integration and / or regression testing, production environment, and validation / stabilization of the software build prior to deployment.
d. The Contractor shall support the Government to implement a continuous deployment to properly and effectively manage the distribution and installation of the software builds. A mechanism, such as rolling deployment shall be implemented to allow for replacement of older software baselines that reside within the infrastructure. Additionally, to support Foreign Disclosure and proper releasability of software to Link 22 partner Nations, the contractor, through continuous deployment, shall manage the installation of software for each country and shall maintain a configuration of versions being delivered to each country.
e. Designing, implementing, and maintaining the DevSecOps continuous integration/continuous delivery pipeline and on-premises deployments.
f. Recommending and implementing industry-based practices for continuous monitoring.
g. Training and coaching development teams in utilizing application lifecycle management and continuous integration/continuous delivery tools.

h. Establishing and maintaining standards for use of the application lifecycle management and continuous integration/continuous delivery tools.
i. Recommending industry-based practices for incorporating testing, security, and operations representation early and continuously in the application lifecycle.
j. Recommending industry-based approaches, technologies and tools for instrumenting DevSecOps elements to provide greater visibility, transparency, and awareness related to pipeline bottlenecks, security, and operational issues.

The Contractor shall also look for practices to streamline and integrate security practices within the continuous integration/continuous delivery pipeline that is aligned with the DoD Enterprise DevSecOps initiative. The Contractor shall provide personnel proficient in the use of tools, technologies and software applications for productivity, collaboration and systems architecture. Some examples include but are not limited to: Jenkins, Kubernetes or Terraform.

The Contractor shall adhere to Governments current DevSecOps testing strategy as shown below in Figure 3.

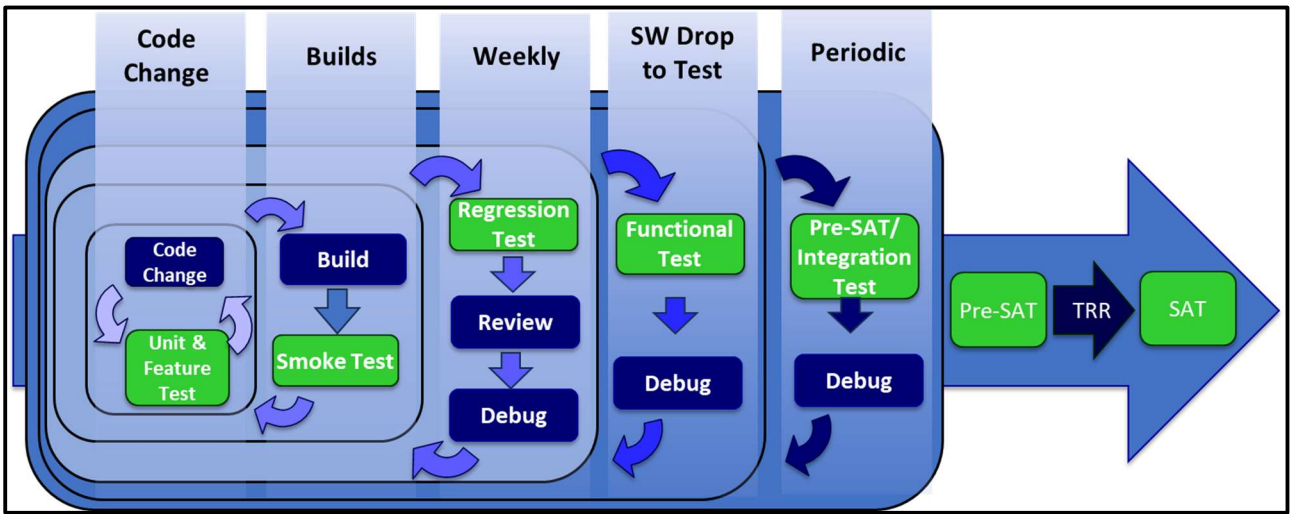

Figure 3 DevSecOps pipeline

For each Task Order (TO), the Government will specify the DevSecOps metrics relevant to that TO, consisting of the Lead Time, Deployment Frequency, the Mean Time to Recovery (MTTR) and the Change Fail rate. Metrics will be agreed bilaterally between the Contractor and the Government at TO level. The Minimum Viable Capability Release (MVCR) will also be specified for each TO and agreed bilaterally between the Government and the Contractor.

CDRL References:

A004 – Project Management Plan
A00E– Integrated Master Schedule
B004 – BCR Engineering Release Executables (SNC and NRS)
B008 – DevSecOps Report

3.4 Systems Engineering

The Contractor shall ensure engineering artifacts are updated to reflect new or revised capabilities. Examples of these artifacts include but are not limited to:

a) Data Link Processing Segment and SNC Interface Design Description (DLP-SNC-IDD)
b) Link 22 Guidebook
c) Software Version Description Document (SVDD)

d) SNC Software Design Description (SDD)
e) Configuration Management Plan (CMP)
f) BCR NILE Documents

The Contractor shall identify high level technical requirements and produce a product backlog with verifiable outcomes.

CDRL Deliverables:

A008– Configuration Management Plan
B002– BCR Documents
B00E – Link 22 Guidebook

3.4.1 System Network Controller (SNC) and NILE Reference System (NRS) System/Segment Design Change

The Contractor shall perform engineering design studies to define the modified design, configuration, and performance characteristics of the SNC and NRS software, in accordance with the requirements of the current Segment Specifications and the list of specified functional modifications. The design shall be carried out to a level of detail such that the necessary modified segment components (including computer resources) and their functional characteristics are identified; the external and major internal hardware and software interfaces are characterized as to function; the physical layout of the segment is described, and feasibility, cost effectiveness, and reproducibility of the design are verified. If the documents specified in Section 2 (with exception of starred [*] documents) need to be modified, change pages shall be provided via a Change Proposal (CP). Design changes resulting from modifications shall be documented in accordance with the NILE Configuration Management Plan (CMP) and delivered as part of the Project Management Plan CDRL(A004). Updates to the current SNC Software Design Description (SDD) shall be provided upon modification of the SNC. The Contractor shall deliver Software Version Description (SVD) documents: one for the SNC and one for the NRS to control and track the software release.

When specified in a Task/Delivery Order, the Contractor shall deliver all the Source and Executable Software (CDRL B002, B003, B005 and B00E), including any batch files, command files, data files or other software files needed to regenerate the executable software and to install and operate the software on its target computer: one for the SNC and one for the NRS.

The Contractor shall embed cybersecurity in each new development. For each delivery, a Code Quality Report (CDRL B009) shall be issued by the Contractor, with the appropriate level of classification, assessing the potential vulnerabilities introduced by the latest developments.

In addition, an Interface Design Description (DLP-SNC-IDD) (CDRL B002) shall be maintained. This document shall identify all the interfaces of the SNC, briefly describe the purpose of each interface to another external system at a functional level and the data exchanged. The document shall also assess the potential threats and vulnerabilities on these interfaces and explain what measures have been put in place for each of them to ensure compliance with DODI 8500.01.

CDRL Deliverables:

B001– Technical Report
B002– BCR Documents
B009– Software Quality Report and Code Quality Report

3.4.2 Analysis of System Issues and Enhancement Proposals

The Contractor shall provide Subject Matter Expertise (SME) support services to assist the NILE PMO in the resolution of system issues and bug fixes, using the DevSecOps principles.

The Contractor shall ensure that cybersecurity requirements are continuously embedded and that potential threats are continuously assessed. These services shall include, but not be limited to:

a) Feedback Reports (FR) or Discrepancy Reports (DR) assessment and response. The Contractor shall record all incoming FRs and DRs, analyze them for technical feasibility, validity, including schedule and cost impacts as specified on a Task/Delivery Order. The Contractor shall recommend a resolution. Analysis of all priority 1 FRs shall be provided to the Government within 10 business days.

b) As directed by a Task Order, the Contractor shall deliver a resolution to FRs or at the request of the NILE PMO, in the form of Problem Change Reports (PCRs) or Change Proposals (CPs).

c) The Contractor shall support all issues and questions related to the three different media types of High Frequency Fixed Frequency (HF FF), Ultra High Frequency Fixed Frequency (UHF FF) and Ultra High Frequency Electronic Protection Measures (UHF EPM), including testing and documentation changes.

d) The Contractor shall conduct problem verification, reporting, tracking and resolution, using the NILE PMO designated tools and procedures.

e) The Contractor shall accomplish incorporation of documentation, interface, and software updates by retrofit.

CDRL Deliverables:

B001 – Technical Report – Study/Services

3.4.3 White Papers

The Contractor shall provide White Papers (WPs) whenever analysis and design proposals that are based on NILE Feedback Reports or at the NILE PMO's request are required. When tasked to deliver a WP via a Task Order/Delivery Order, the Contractor shall:

a) Maintain a history of the deleted and/or modified lines of code relative to the baseline software, where existing functionality is removed. The Contractor shall not proceed with changes to the baseline software without Government approval

b) Amend the software design documentation to describe the "sidelining" of existing functionality

c) Following Government approval, amend the specification documentation to reflect the modified baseline requirements, deleting existing functionality requirements as necessary

d) Ensure that the Configuration Management (CM) process maintains old versions of documentation.

e) Ensure that any proposed changes to the SNC which result in an updated version of the software are backwards compatible with the last SNC major version (e.g. 10.x) unless explicitly directed by the Government in a Task Order

f) Ensure that the development plan of any proposed change follows the DevSecOps guidance, using an iterative strategy; and,

g) Explain how cybersecurity is ensured for any proposed change.

The Contractor shall provide technical support, analysis, and design activities necessary to support current and evolving Link 22 interfaces and specifications including COMSEC, Signal Processing Controllers (SPC), and radios interfaces (see Figure 1). Hardware will be provided to the Contractor as Government Furnished Equipment (GFE). These activities shall be performed as specified on a Task/Delivery Order

and with reference to the waveforms presently used by the Link 22 system, as well as to potential new waveforms.

CDRL Deliverables:

B001 – Technical Report – Study/Services
B007 – CMIS Documents

3.4.4 BCR Documents

To maintain Configuration Management, the Contractor shall generate and/or maintain BCR Documents Technical Data Package (TDP) which details all information and requirements pertaining to the upgrade, testing, installation, training, and support for the SNC and NRS. As specified in a Task/Delivery Order, an updated TDP shall be delivered upon completion of each Block Cycle or Engineering Release. The TDP shall constitute a complete design disclosure of the SNC and NRS and shall be delivered with sufficient detail to allow the Government to build an identical system itself or via a third party. The TDP shall include all engineering design documentation baselines specifications, product drawings and associated lists, special tooling and test equipment drawings and associated lists, technical manuals, Commercial Off the Shelf (COTS) manuals, source and object code listings, software documentation, test plans and procedures, installation drawings, support documentation, System Technical Manuals (STMs), the Link 22 Guidebook, and configuration changes. COTS manuals shall consist of only the information that is normally supplied by the vendor. The TDP shall not include any classified COMSEC/TEMPEST information or requirements[5]. The TDP shall exactly represent the as-built configurations of the modified SNC and NRS that successfully completed Block Cycle Testing.

CDRL Deliverables:

B001– Technical Report
B002– BCR Documents

3.4.5 System Technical Manual

The Contractor shall deliver SNC and NRS System Technical Manual documents (STMs) that reference the executable software, source files, and software support information, including build design information and compilation, and modification procedures for a CSCI. The Contractor shall provide appropriate update pages to the SNC and NRS system level technical manuals according to SNC and NRS implemented changes.

B001 –Technical Report
B002– BCR Documents

3.4.6 Link 22 Guidebook

The Link 22 Guidebook includes both high-level and detailed descriptions of all components of the Link 22 system and their modes of operation and key features. This guidebook provides suitable information for Link 22 operators, planners, managers, developers, and testers. The intent of the document is to provide both an introduction for new users, as well as a detailed reference for established users. The Contractor shall be responsible for producing a modernized Link 22 Guidebook with updated layout, content and graphics following specific distribution procedures as directed by the NILE PM. The Contractor shall release the Guidebook in three different versions:

[5] If this occurs, that information requires an upgrade to classified, the government shall be appropriately notified of the higher level in writing and conduct a strategy meeting.

a) "Link 22 GUIDEBOOK" (COMPLETE GUIDEBOOK); for NILE Nations & Link 22 Partner Nations.

b) "Link 22 GUIDEBOOK - OVERVIEW AND OPERATIONS" (includes Chapters 1 & 2, Appendices A, E, F & G, and no Index); for NILE Nations, Link 22 Partner Nations and approved 3PS Nations only.

c) "Link 22 GUIDEBOOK - OVERVIEW" (includes Chapter 1 and Appendices A, E, F & G, no Index); for nations that have requested a copy and been approved by the NILE PM.

The Contractor shall provide configuration control of the Link 22 Guidebook in the same manner required for documents listed in Section 2.

CDRL Deliverables:
B00E– Link 22 Guidebook

3.5 Hardware Engineering

The Contractor shall recommend and provide any general purpose and special purpose electronic test equipment required for the operation and maintenance of the SNC, NRS and laboratory hardware, including GFP items specified in the contract.

When new hardware is procured under this contract, the Contractor shall recommend only hardware that can be maintained and repaired via service organizations with facilities located in a NILE Nation, to the extent such hardware is available. An exception to this applies to the procurement of a commercial development configuration. The Contractor shall deliver all information about procured or modified hardware to the Government IAW MIL-PFR 49506 (S/S by GEIA-STD-0007).

CDRL Deliverables:

A003– Government Furnished Report

3.5.1 Mobile Test Station (MTS)

The Contractor shall design, integrate, assemble and maintain a mobile test station.

The Contractor shall procure additional hardware and software as directed by the NILE PMO. The Contractor shall sustain and upgrade the mobile test station hardware and software in preparation for deployment for various field test events.

The Contractor shall maintain the supporting documentation including but not limited to the Configuration Management Plan (CMP) and Hardware/Software List (HW/SW list).

The Contractor shall assist the Government in providing the necessary artifacts throughout the Cybersecurity Assessment and Authorization process, to support acquisition and maintenance of the Authority to Operate (ATO) for the MTS. The Contractor shall provide subject matter expertise to deploy test events and post analysis of data collected. The Contractor shall ensure the MTS, and its components are included as part of GFP inventory.

CDRL Deliverables:

A003– Government Furnished Report
A008 – Configuration Management Plan
A00C– Integrated Support Plan
A00F– Contractor Acquired Property List

3.5.2 Firmware, Software Licenses and Warranties

The Contractor shall procure the software, hardware, and/or firmware specified on a Task/Delivery Order, in support of the NILE Laboratory.

The Contractor shall ensure that all products recommended and/or procured meet cybersecurity and computer requirements specified in PWS section 9.

The Contractor shall provide all support data and cost estimates necessary to justify a fair and reasonable price per item procured. The Contractor shall have an adequate accounting system to track all items ordered and its associated delivery status. After receipt, the Contractor shall have an adequate property management system to track each item location. All items procured by the Contractor shall be utilized or staged at the Contractor's facility, be transported by the Contractor to the installation, integrated or consumed in a system, or returned to the Government at the completion of the contract/task order.

CDRL Deliverables:

A003– Government Furnished Report
A00C– Integrated Support Plan
A00F– Contractor Acquired Property List
A00G– Contractor's Systems Security Plan

3.6 Test and Evaluation

The Contractor shall assist with the development and review of test documentation, procedures and reports for the NILE PMO.

The Contractor shall support Government Verification and Validation efforts to include test plan development, test procedure development, test schedule development, test execution and test reporting.

CDRL Deliverables:

H001– Software Test Plan
H002– Software Test Report
H003– System Acceptance Test Plan/Procedures

3.6.1 Planning and Execution of Integration and Field Testing

As specified on a Task/Delivery Order, the Contractor shall provide Subject Matter Expertise to assist the NILE PMO in the preparation and execution of testing of all the systems, which encompass the Link 22 architecture to be held either at the Contractor facility or Government sites.

These services shall include developing Test Plans and Test Procedures for assessing conformance and compatibility/interoperability of devices designed by Third Parties for the Link 22 System, including Radios, Signal Processing Controllers and Data Link Processors. Conformance means compliance to the relevant specification and suitability in the overall Link 22 system environment.

Compatibility/interoperability is the condition among communications-electronics systems or items of communications-electronics equipment where information or services can be exchanged directly and

satisfactorily between Link 22 systems with different SPC and radio configurations. At test completion the Contractor shall also provide detailed Test Reports of the activity performed, and the technical analysis and evaluation of the results.

CDRL Deliverables:
B001-Technical Reports
H001– Software Test Plan

3.6.2 Test Readiness Review (TRR)

The Contractor shall call for a TRR when confident that software that has been amended as part of code and documentation updates, test scenarios and test procedures are complete and ready to be conducted for formal acceptance. The purpose of the TRR is for the Contractor to present enough evidence to allow the Government to authorize to proceed to the next phase of testing.

The following TRR considerations shall be addressed:

- Previous Test results assessments e.g. Computer Software Configuration Item (CSCI) Qualification Testing, Hardware Configuration item (HWCI) Integration Test.
- Requirements, Issues and Changes.
- Acceptance (Block Cycle) Test Procedures, and Scenarios.
- Software Test Resources and Tools.
- Hardware and Support Environment.
- Configuration Management and Software Quality Assurance.
- Test Team.
- Recommended Tests to Conduct for Formal CSCI/System Testing.
- Known Software Problems.
- Test Schedule; and delivery of a Software Test Report detailing the results of all tests conducted during the qualification test phase.

CDRL Deliverables:

H001– Software Test Plan
H002– Software Test Report
H003 –System Acceptance Test Plan/Procedure

3.6.3 Contractor-conducted Test and Evaluation

3.6.3.1 Qualification Testing

The Contractor shall conduct software testing following the Quality Assurance program and the guidance of IEEE/EIA 12207 (Guide for Information Technology - Software life cycle processes – para 4.2).The Contractor shall deliver one Software Test Plan (STP) and two Software Test Description (STD) documents (one each for the SNC and NRS), at least one month before the start of the System Qualification Tests for Government approval. The STP and STDs shall encompass CSCI System Qualification Acceptance Testing. Existing CSCI and System Qualifications tests, which are reused, shall be incorporated into the revised STDs. The Contractor shall conduct a sequence of testing that follows the testing phases of Computer Software Unit (CSU) testing, CSCI Integration testing, System Integration testing, System Qualification, Acceptance testing and shall deliver two Software Test Report (STR) documents: one for the SNC and one for the NRS at the end of each of the test phases.

The STP shall specify test environments in which the test phases will take place and shall provide assurance that all the SNC and NRS requirements are 100% tested considering all the test phases. The SNC STP shall cover at least 50% of the requirements. The requirements coverage criteria shall be distributed between the Windows and Linux versions of the SNC. The NRS STP shall cover at least 20% of the requirements. Test environments shall include real equipment (as opposed to simulators), such as LLC 7Ms, SPCs and radios

to prove that a significant set of requirements has been met and successfully tested. By default, the minimum set of requirements to be tested under these conditions is set to 10%.

When both the NRS and SNC have been determined to be ready for formal acceptance testing, the Contractor shall schedule NRS and SNC Test Readiness Reviews (TRR) in agreement with the Government.

3.6.3.2 Formal Acceptance Testing

A formal acceptance testing phase shall take place following the TRR and be witnessed by the NILE PMO designated personnel. A sample of test cases approved by the NILE PMO will be run. Upon completion, the NILE PMO designated personnel will sign an Acceptance Letter for the tested BCR. In the event of failed test cases, the NILE PMO may sign an Acceptance Letter with limitations or ask for revision testing to rectify the faults. Upon revision, the Contractor shall schedule an extra session of formal acceptance tests in agreement with the Government, and the Acceptance Letter signed by the NILE PMO designated personnel.

3.6.3.3 Intermediate Testing

The Contractor shall perform testing before each intermediate delivery. The Contractor shall deliver one Software Test Plan (STP) and two Software Test Description (STD) documents (one each for the SNC and NRS), at least two weeks before the start of the intermediate testing phase.

3.6.3.4 General Testing Rules

The Contractor shall ensure the following rules are adhered to when conducting formal verification activities (the following list is indicative and is not exhaustive):

- All Contractor conducted testing shall be performed following Government approved plans and procedures (STDs). Unlike CSCI and SQT phases, where the Government is witnessing all test activities, test witnessing by Government representatives is not required during Computer Software Unit (CSU) and Software Integration Test phases but shall be allowed and shall be at the discretion of the Government. The Government will notify the Contractor of intent to witness individual tests.
- The Contractor shall update and submit a traceability matrix along with the test plan, showing how the tests planned to be performed covers the different requirements.
- The Contractor shall prepare and submit Software Test Report (STRs) of testing activity results. Two documents shall be delivered after CSCI tests: one for the SNC and one for the NRS, noting that the Scenario Generator and Media Simulator CSCIs are incorporated into the NRS. The test reports shall include soft (electronic) copy versions of the completed Acceptance Test Procedures. They shall provide evidence that the tests were conducted, the results that were obtained, and bear the signatures of the personnel who conducted or witnessed the tests.
- The Contractor shall conduct retests of previously completed testing for which correction of a deficiency or any other modification affects the results of those previously completed tests. The selection of requirements for retesting is a joint Contractor and Government decision, with the Government having the final authority; and,
- The contractor shall continue to automate testing.

The Contractor shall perform all necessary testing phases including Computer Software Unit (CSU) testing, CSCI Integration testing, System Integration testing, System Qualification testing, Acceptance testing, and interface testing with real equipment (SPC, LLC 7M and radios) to demonstrate to the Government that each individual CSCI and the overall SNC and NRS Systems meet every single requirement derived from the requirements identified in the course of the contract.

Regarding the rest of the requirements of the SNC and NRS, the Contractor shall provide assurance that all of them remain met by the product to be delivered (BCR). This may involve testing each individual requirement of the SNC and NRS with real or simulated equipment if required by the Government. The scope of the testing activities will be defined in the STP.

CDRL Deliverables:

B002– BCR Documents
B009 – Software Quality Assurance Report and Code Quality Report
H001– Software Test Plan
H002– Software Test Report
H003 – System Acceptance Test Plan/Procedures

3.7 Operations and Sustainment

The Contractor shall support catastrophic maintenance of the BCR if required by deploying software and firmware updates, security patches and fixes according to the Configuration management plans and feedback received from Link 22 Partner Nations.

The Contractor shall support maintenance of lab infrastructure used for the development, integration and testing of software changes to ensure that it is operating as expected. Any deviation or deficient are to be reported according to applicable system engineering plans documents.

The Contractor shall provide intermediate software releases of the SNC to the Naval Undersea Warfare Command (NUWC) Security Assessment Team. The Contractor shall review the report provided by NUWC and address findings and recommendations. The frequency of the software releases to NUWC is to be agreed with the government. The implementation of recommended changes and the associated schedule will be agreed to with the government.

The Contractor may be tasked to mail classified and unclassified material to the NILE Nations from their facility for this effort, in accordance with §126.4 of the International Traffic in Arms Regulations, as amended by the U.S. Department of State's Directorate of Defense Trade Controls. Vendors should refer to the applicable Department of Defense Exemption guidelines: https://www.dtsa.mil/SitePages/about-dtsa/directorates/export-control/DoD-Exemption-Guidelines-Summary.aspx.

CDRL Deliverables:

A00C– Integrated Support Plan

3.8 Configuration Data Management

The term "Configuration Baseline" refers to all the initial baseline software, hardware and documentation and any evolution of these items through the life of this contract. Amendment of the current NILE baseline software, hardware and documentation shall be handled in accordance with the NILE approved Configuration Management (CM) process contained in the NILE Configuration Management Plan (CMP). The NILE CMP also integrates and expands CM terms and definitions mentioned in this PWS, in

accordance with NAVWARINST 5234, and provides approved format and template of NILE Feedback Reports (FRs).

CDRL Deliverables:

A004– Project Management Plan
A008– Configuration Management Plan

3.8.1 Configuration Management Plan (CMP)

The Contractor shall develop a CMP as part of the PMP, incorporating the requirements of the existing NILE CM procedures as contained in the NILE CMP. The Contractor shall be responsible for incorporating changes in the PMP and maintaining the configuration baseline, identified in CMIS documents listed in section 2.4 , to accurately document the evolving configuration. The Government will be responsible for approval of all updates to the configuration baselines. A new baseline shall be released by the Contractor after completion of each Block Cycle Update.

CDRL Deliverables:

A004– Project Management Plan
A008– Configuration Management Plan

3.8.2 Configuration Control Review Boards (CCRB)

The Contractor shall participate in the CCRB (a Government/Contractor forum co-chaired by both parties) to monitor the status of NILE software and hardware problems and pending Change Proposals (CPs). The CCRB will review and prioritize CPs, Problem Change Reports (PCRs), and FRs and support tasks, and establish consensus on feasible approaches to problem corrections(s), including the implementation of corrections and release of MVCRs. The Contractor shall generate a Change Proposal (CP) for any pending modification item or Problem Change Report (PCR) according to the decision taken during the CCRB. The location of CCRBs will be mutually agreed by the Contractor and the Government, and may be held via email or phone conference, as necessary and agreed upon with the Government on a case-by-case basis. Further details on CCRB structure and management of the processes are provided in the NILE CMP.

An agenda shall be developed by the Contractor prior to each CCRB meeting. The Contractor shall prepare and submit minutes of the CCRB meetings. A collection of all technical documentation such as PCRs, DRs, CPs, FRs and WPs should also be provided and submitted as CDRL B001.

CDRL Deliverables:

A005– Meeting Agenda
A006 –Meeting Minutes
A007– Briefing Materials
B001– Technical Report

3.8.3 Configuration Management Information System (CMIS)

The Contractor shall implement and maintain a CMIS to file project information, including all CDRLs. The CMIS shall be capable of producing Microsoft ACCESS or Excel compatible output and shall be continuously available to the Government upon request.

The Contractor will be provided with a copy of the existing CMIS at contract award. If the Contractor chooses to implement a new CMIS, the Contractor shall migrate all historical data to the new database. The Contractor shall deliver the CMIS database to the Government on a monthly basis.

CDRL Deliverables:

B007 –CMIS Documents
B00D– Configuration Management Information System (CMIS)

3.8.4 Configuration Control Board (CCB)

The CCB is a configuration control function for the NILE Nations. The Contractor shall support the CCB if clarifications on technical aspects are necessary, as detailed in a Task/Delivery Order.

CDRL Deliverables:

A007– Briefing Materials
B001– Technical Report

3.9 Integrated Support Plan (ISP)

The Contractor shall develop, implement and maintain an Integrated Support Plan. This effort shall be conducted as an integral part of the modification process, with the intent of minimizing product life cycle costs and enhancing supportability.

The ISP plan shall detail the maintenance concept for the NILE Compatibility Lab, hardware, and software, specifying items to be supported where organizational level (in-house) or depot level (suppliers) support shall be used. The ISP shall also document items to be disposed of, where necessary. Organizational level repairs shall be limited to replacement of hardware modules such as circuit cards, power supplies, keyboards or parts, etc., while depot level repairs shall consist of repairing piece parts of these modules.

The Contractor shall establish Packaging, Handling, Storage and Transportation (PHS&T) procedures that provide safe and efficient packaging, handling, storage, movement, and protection of the hardware and software items to include shipment of the MTS in support of operational training exercises. The ISP shall establish the production and delivery procedures for NILE BCR. All activities, milestones, and planning shall be addressed in the ISP portion of the PMP.

CDRL Deliverables:
A004– Project Management Plan
A00C– Integrated Support Plan

4 OTHER DIRECT COSTS (ODCs)

The Contractor may incur ODCs required to complete tasking as specified in individual task orders to support the performance of the requirements of the Link 22 system.

4.1 Materials

In addition to acquiring quantities in section 3.5, the contractor may procure additional materials such as Signal Processing Controller (SPC), radios, software licenses, replacement laptops, servers, etc. The contractor shall maintain a CAP list as directed by section 7.2 which shall be maintained in accordance with the GFP clauses in the contract.

The Contractor may be tasked to mail classified and unclassified material to the NILE Nations from its facility for this effort, in accordance with the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) amended text of §126.4 of the International Traffic in Arms Regulations. Vendors should refer to the applicable Department of Defense Exemption guidelines on https://www.dtsa.mil.

CDRL Deliverables:

A003– Government Furnished Report

4.2 Travel

To support contract activities, Contractor personnel may be required to travel to attend in-person meetings or to provide remote engineering support services on Link 22 related matters. Major meetings, which may require Contractor attendance, are scheduled twice a year for the average length of a business week (typically to be held abroad in May/June and November/December). However, additional travel might be required at short notice.

The Contractor may also be required to take local trips in support of one or more requirements described in this PWS. The costs for travel, subsistence, and lodging will be reimbursed to the Contractor in accordance with the Federal Acquisition Regulations (FAR). Specific travel requirements will be specified on Task/Delivery Orders.

Travel under this contract is only authorized under task/delivery orders issued by the COR.

The number of trips, travelers and locations are to be determined by the Government. The Government anticipates travel to be within Continental United States (CONUS) and Outside the Continental United States (OCONUS) locations.

4.2.1 Services to International Forums

As specified on a Task/Delivery Order, additionally, the Contractor may be required to travel internationally to support the NILE PMO at the following types of international forums, providing subject matter expertise and input on technical issues (including but not limited to NILE White Papers and Presentation Materials) of:

a) The NILE Steering Committee (SC).

b) The NILE Configuration Control Board (NILE CCB).

c) The Link 22 Communications and Interoperability Working Group (Link 22 C&IWG) and Link 22 Technical & Operational Working Group (Link 22 TOWG).

d) The Interoperability Testing being conducted between NILE Nations and/or Link 22 Partner Nations; and,

e) Other meetings, field events or workshops on Link 22 or TDL related matters providing material for easing the update of STANAG 5522/ATDLP-5.22 and other standards used for Link 22 System design.

CDRL Deliverables:

A001– Contractor's Progress, Status and Management Report
A007– Briefing Materials

4.2.2 Nation-specific Support

Nations can request support from the ISS Contractor in their national Link 22 planning and implementation. As specified on a Task/Delivery Order, the contractor may be asked to provide nation-

specific support. The Contractor shall provide technical/engineering services to any requiring NILE Nation, or any Link 22 Partner Nations (following approval from the NILE PMO) purchasing Link 22 services via FMS case, and their national contractors, with respect to any Link 22 system engineering matter. These services shall include:

a) Operation of NRS components, SNC, SNC Diamond (SNCd), interfaces and ancillary equipment (e.g. TOD card) on Intel based computer platforms from the nation requesting the support; and,
b) Analysis and evaluation of national SNC and NRS integration test results.

CDRL Deliverables:

B001– Technical Report
A007– Briefing Materials

4.3 Reimbursement of Travel Costs

All Travel requirements (including itineraries, travel costs, estimates, and dates) estimates shall require prior approval by the Government. Any travel under the contract must be specifically identified by the Contractor in a written quotation submitted to the COR for approval prior to incurring any travel costs. Travel is on a strictly cost reimbursable basis. Costs for travel shall be billed in accordance with the regulatory implementation of Public Law 99-234 and FAR 31.205-46 Travel Costs. The Contractor is responsible for ensuring all travel costs billed to the contract at the task/delivery order level are itemized and allowable as defined in the FAR.

CDRL Deliverables:
A00B– Contracts Funds Status Report

5 MANAGEMENT REQUIREMENTS

5.1 Program Management Services

The Contractor shall appoint a Program Manager (PM) who shall have overall responsibility for the management, control and coordination of all work performed in this contract. The Contractor shall designate a single, full-time (defined as 1,920 hours per contract year) The Contractor Program Manager shall document, in a tailored Program Management Plan (PMP CDRL A004), management (and associated organizational chart), cost, engineering, logistics, cyber and software development plans. This single document shall include an Integrated Management Plan, Contract Work Breakdown Structure (CWBS), which represents how the Contractor plans to accomplish the entire contract work scope, consistent with the Contractor's internal organizations and processes. CWBS will serve as the framework for contract planning, budgeting, and reporting of cost and schedule status to the Government. The first iteration of the PMP shall be delivered to the NILE PMO within 90 days of Contract award and then update annually.

The Contractor shall establish and maintain management operations that shall include the following areas:

- Program Planning and Control
- Subcontractor Control
- Financial Management
- Data Management
- Management and Accountability for Government Furnished Property/Information/ Equipment, Material or Information
- Risk Assessment and Management

The Contractor shall provide an open channel of communication, via phone, Video Teleconference (or equivalent, which shall support sharing CUI CTI data) and email, during the NILE PMO's working hours. The Contractor shall maintain current knowledge to support the system engineering tasks. The Contractor shall provide identification of issues and problems with the specifications, implementations and overall Link 22 system to enable the Government to achieve efficient, effective and interoperable Link 22 systems.

The Contractor shall manage data generated as part of the contract in databases or with specific data management tools. All data shall be deliverable to the Government, upon request.

The Contractor's Program Manager shall be the primary authority who will interface with the NILE PMO and, as directed by the NILE PMO and in accordance with the PWS, with the other entities participating in the NILE ISS phase including:

a) The Governmental Configuration Management forums (CCB, etc.).

b) NATO and NILE working groups; and

c) National Link 22 segment integrators, as contracted by the NILE Nations and Link 22 Partner Nations, when required.

CDRL Deliverables:

A001 – Contractor's Progress, Status and Management Report
A003 – Government Furnished Report
A004 – Project Management Plan
A005– Meeting Agenda
A006– Meeting Minutes
A007– Briefing Materials
A009 – Contract Work Breakdown Structure
A00B –Contract Funds Status Report
A00A –Technical Work and Management Plan
A00D– Phase In/Out Transition Plan
A00E– Integrated Master Schedule

5.1.1 Integrated Master Schedule

The Integrated Master Schedule (IMS) serves as the authoritative program schedule baseline. It provides a time-phased, networked representation of all major tasks, milestones, deliverables, and dependencies required to execute the contract. The IMS ensures alignment between technical, cost, and schedule objectives, and enables effective monitoring of program performance.

The Contractor shall develop a comprehensive IMS that integrates all contractually required tasks, subcontractor schedules, and government-furnished inputs. The Contractor shall generate an Integrated Master Schedule for each Performance and Management Requirement on the Task/Delivery Order.

The IMS must be logically linked, resource-loaded where applicable, and reflect the critical path to contract completion.

The IMS shall be submitted to the Government 60 days after contract award. Updates shall be provided on a recurring basis (e.g., monthly) to reflect progress, changes, and risk mitigation activities.

The IMS shall conform to industry-standard scheduling tools (e.g., Microsoft Project, Primavera).

The schedule must include Work Breakdown Structure (WBS) alignment and milestone tracking,

The prime contractor shall ensure any subcontractor schedules are fully integrated into the IMS.

Dependencies between prime and subcontractor tasks must be clearly defined to provide visibility into potential schedule risks.

The Government will review the IMS for adequacy, realism, and compliance with contractual requirements, and the Contractor shall address Government comments and resubmit the IMS until approval is obtained.

CDRL Deliverables:

A00E– Integrated Master Schedule

5.1.2 Contract Work Breakdown Structure

For all Cost-Plus-Fixed-Fee CLINS, the Contractor shall generate a one-page summary for each task on the Task/Delivery Order. The summary shall include, but not be limited to:

- Any changes required to external interfaces, whether implementation of a task would result in a non-backwards compatible version of the SNC
- A basic schedule showing analysis and implementation (separately); and the estimated effort for analysis and implementation (separately)
- For each task, the Contractor shall obtain approval via e-mail from the Contracting Officer's Representative (COR) before implementing any solutions. Throughout the Period of Performance of the CLIN, if it becomes apparent that the details contained within any of the one-page summaries require updating, the Contractor shall immediately notify the NILE PMO and provide an updated summary.

CDRL Deliverables:

A004 – Project Management Plan
A009 – Contract Work Breakdown Structure
A00E– Technical and Work Management Plan

5.1.3 Project Planning and Control

The Contractor shall identify, plan, organize, direct, coordinate, and control activities necessary to accomplish overall contract requirements in accordance with the DevSecOps principles. The Contractor shall establish a formal organization responsible for accomplishing the tasks outlined in this PWS. The Contractor shall ensure that all plans and procedures required by this PWS and CDRLs approved by the Government, are adhered to by the Contractor and all sub-contractors, if any. A clear line of project authority shall exist between all organizational elements and the PM. Any changes to the line of project authority shall be communicated to the COR within 7 days of any updates or changes.

CDRL Deliverables:

A005– Meeting Agenda
A006– Meeting Minutes
A007– Briefing Materials

5.1.4 Contractor Progress, Status and Management Report

The Contractor shall provide, on a monthly basis, a report detailing the schedule of events and the integrated cost and schedule status of work progress on the contract as well as reporting on the

DevSecOps metrics set out in the respective Task Order(s). The schedule will consist of a logically networked schedule in Microsoft Project 2010 (or later). 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, in accordance with the risk management plan within the PMP (CDRL A004). Additionally, the Contractor shall identify and provide any technical status and risks associated with software development activities, DevSecOps and sprints, and recommendations to the PMO. The metrics consist of presenting the Lead time, the Deployment Frequency and the Change Fail rate. 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. The report shall be also briefed and discussed at the following NILE In Process Reviews (IPRs).

CDRL Deliverables:

A001 – Contractor's Progress, Status and Management Report
A004 – Project Management Plan
A00B – Contract Funds Status Report

5.1.5 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/GFP (including Classified items)

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 within 30 days of the meeting.

CDRL Deliverables:

A005– Meeting Agenda

A006– Meeting Minutes
A007– Briefing Materials

5.1.6 In- Process Reviews (IPR)

Commencing with the Post Award Conference, the Contractor shall conduct IPRs, which should be available both in person and virtually. The purpose of these reviews is to provide status updates related to the contractor's cost, schedule and performance during TO execution. Examples of topics to be presented include but are not limited to the following:

a. Outstanding Action items from previous meeting
b. Budget execution against current spend plan(s)
c. Staffing, including a summary of proposed, approved and completed staffing changes since the last review
d. Highlights from monthly work accomplishments
e. Upcoming work efforts and milestones
f. Estimates at completion, and
g. Risks, issues and opportunities.

The Contractor shall present and administratively support IPRs. 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 CWBS, 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.

CDRL Deliverables:

A005– Meeting Agenda
A006– Meeting Minutes
A00E– Integrated Master Schedule

5.1.7 Integrated Product Team (IPT)

The Contractor shall track program progress by participating in designated Integrated Product Teams (IPT), working groups, program review, design review, readiness reviews. The Contractor shall coordinate and conduct meetings to promote effective and efficient management of this TO for the Government, including monthly MSR's with NILE PMO.

The Contractor shall coordinate and participate in joint and regularly scheduled Contractor/Government IPT meetings to resolve problems and issues. IPTs should be available in person or virtually. To maintain the agile nature of the project, the government requires the meetings to run every six (6) weeks. IPT responsibilities shall include:

a) Monitoring of the accomplishment of project work and progress using information from all available sources, including cost and schedule data

b) Identification of technical and project risks, and formulation of risk mitigation recommendations; and

c) Expediting resolution of problems and clarifying issues

The location of all IPTs shall be agreed mutually between the Contractor and the Government, and meetings shall be organized on a case-by-case basis according to the volume of items to be performed and problems to resolve. The Contractor shall prepare and submit minutes of the IPT meeting within 10 business days after the IPT.

CDRL Deliverables:

A005 – Meeting Agenda
A006 – Meeting Minutes
A007– Briefing Materials
A00E– Integrated Master Schedule

5.1.8 Risk Management

The Contractor shall establish a risk management program conforming to the guidelines of NAVWARINST 3058.1 that identifies and controls performance, cost, and schedule risks likely to occur in this effort. Planning for risk management shall be documented in the PMP.

CDRL Deliverables:

A004– Project Management Plan

6 REPORTS, DATA, DELIVERABLES AND COMMUNICATION

Reports, technical data and computer software deliverables shall be provided in accordance with the Contract Data Requirements List, as specified in individual Task/Delivery Orders. The Contractor shall provide draft deliverables as specified in individual Task/Delivery Orders. All classified deliverables shall be protected and handled in accordance with the contract DD Form 254 Contract Security Classification Specification. The Contractor shall provide deliverables in accordance with the frequency and timelines as described in each CDRL, DD Form 1423-1. The requirement specifies that all documents should be prepared in Microsoft Office Suite product line, specifically Microsoft Word compatible format unless a different format is explicitly stated in the CDRLs. Additionally, any other electronic documents that are part of the contract must be created using Microsoft Office Suite Product Line.

6.1 Product Deliverables

All requirements are set forth in each CDRL Exhibit A and this document. All non-classified CDRL deliverable documents and copies will be submitted electronically via an upload by the Contractor into the Acquisition Management System (AMS) CDRL Tool: https://ams.navair.navy.mil/CDRL/Pages/Default.aspx. CDRL tool training is found on this link: https://myteam.navair.navy.mil/communitites/ams/Pages/Courses.aspx

The Contractor shall be responsible for delivering all data.

Exhibit	CDRL	Deliverables
A: Program Mgt	A001	Contractor's Progress, Status and Management Report
	A002	Cyber Security Workforce Report
	A003	GFP Report (quarterly)
	A004	Project Management Plan
	A005	Meeting Agenda
	A006	Meeting Minutes

	A007	Briefing Materials
	A008	Configuration Management Plan
	A009	Contract Work Breakdown Structure
	A00A	Technical and Management Work Plan
	A00B	Contract Funds Status Report
	A00C	Integrated Support Plan
	A00D	Transition Plan
	A00E	Integrated Master schedule (IMS)
	A00F	Contractor Acquired Property List (CAP)
	A00G	Contractor's Systems Security Plan and Associated Plans of Action to Implement NIST SP 800-171 on a Contractor's Internal Unclassified Information System
B: Systems Engineering	B001	Technical Report
	B002	BCR Documents
	B003	BCR Executable Software (SNC/NRS)
	B004	BCR Engineering Release Executable (SNC/NRS)
	B005	BCR Source Code (SNC and NRS)
	B006	Risk Management Framework (RMF) Package Deliverables
	B007	CMIS Documents (WP, PCR, CP, FR, DR)
	B008	DevSecOps Report (linked to Jenkins)
	B009	Software Quality Report and Code Quality Report
	B00A	Information Assurance Test Plan
	B00B	Information Assurance Test Report
	B00C	Configuration Audit Summary Report and Certification
	B00D	Configuration Management Information System (CMIS)
	B00E	Link 22 Guidebook Manual
	B00F	Ports and Protocols Service Management
H: Test & Evaluation	H001	Software Test Plan
	H002	Software Test Report
	H003	System Acceptance Test Plan/Procedure

6.2 Performance Standards

The Task Order Quality Assurance Surveillance Plan (QASP) will be used to monitor performance. The Government reserves the right to unilaterally change the performance standards if it is in the best interest of the Government. If the government changes performance standards, the contractor shall be notified.

6.2.1 Quality Assurance (QA)

The Contractor shall implement a QA program, to include Software Quality Assurance (SQA) following the guidance of ISO 9001/IEC 25010 and AQAP standards referenced in Section 3. The Contractor shall implement the QA program through their quality procedures such as (the following list is indicative and is not exhaustive):

a) Internal management processes.

b) Ensuring that best commercial practices and policies are in place and there is capability to audit that these practices and policies are being followed.

c) SNC and NRS baseline specifications compliance and requests for waivers or deviations.

d) SNC and NRS software upgrade.

e) Analysis and design documentation.

f) Block Cycle test plans, procedures and reports; and

g) Process improvement.

At project reviews (IPRs and IPTs), the Contractor shall demonstrate in detail how benchmarks and metrics are established and controlled to ensure repeatable results and internal QA processes meet all applicable Government requirements.

The QA program shall be documented, and all records associated with the establishment, implementation, and operation of the quality system made available for review and retention. The Contractor shall monitor the preparation, maintenance and compliance with work and inspection instructions as a function of the quality program. The Government may perform any necessary inspections, verifications, and evaluations to ascertain conformance to requirements and the adequacy of the implementing procedures. Inspection and test records shall indicate the nature of the observations, number of observations made and the number and type of deficiencies found. Data included in inspection and test records shall be complete and accurate and shall be used for trend analysis and to assess effectiveness of corrective action. Additionally, Contractor performance will also be measured in accordance with a Government Quality Assurance and Surveillance Plan (QASP).

CDRL Deliverables:

A004– Project Management Plan

6.2.2 Acceptable Quality Level

All requested analysis and reports provided by the Contractor shall be in accordance with CDRL criteria and must be technically accurate, incorporate Government comments and be grammatically correct. Drafts for review do not count as deliverables. Scheduled performance requirements may vary based on milestones and acquisition requirements. The Contractor shall provide necessary timely assistance to meet program emergent requirements as requested by the Government.

6.2.3 Quality Assurance Audits (QAA)

QAAs will be performed to verify implementation of the Contractor's QA program. The Contractor shall conduct QAAs of Contractor compliance to the Government's requirements. The Contractor shall ensure that a full audit of all quality assurance requirements has been conducted before each BCR delivery. The Contractor shall design an audit schedule. The Contractor shall provide pertinent managerial and technical skills necessary to support QAAs and CSCI surveillance. QAAs shall be conducted by the Contractor in accordance with a Government approved company standard audit plan. The Contractor shall correct any deficiencies discovered during the audit(s). For each QAA conducted, the Contractor shall submit an Audit Summary Report to the Government.

CDRL Deliverables:

B00C - Configuration Audit Summary Report and Certification

6.2.4 External Quality Assurance Audits

The Contractor shall coordinate an additional QAA which will be performed by an external, independent entity to verify implementation of the Contractor's QA program. This external QAA will occur annually, not to exceed five business days, and will verify QA requirements as directed by the NILE PMO.

6.3 Progress and Management Reports

The Contractor shall prepare and provide a Contractor Monthly Status Report, (CDRL A001) which indicates the progress of work, status of the program(s), DevSecOps metrics set out in the respective Task Order(s) and existing or potential problem areas for all assigned tasks.

The Contractor shall submit the Contract Status Report for the same timeframe as each invoice submitted in the Wide Area Workflow (WAWF) Module of the Procurement Integrated Enterprise Environment (PIEE). The Contractor shall provide, monthly, a report detailing the schedule of events and the integrated cost and schedule status of work progress on the contract as well as reporting on the DevSecOps metrics set out in the respective Task Order(s).

The schedule will consist of a logically networked schedule in the most updated software tools such as Microsoft Project 2010, Primavera (or later). 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 should 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, in accordance with the risk management plan within the PMP (CDRL A004).

Additionally, the Contractor shall identify and provide any technical status and risks associated with software development activities, DevSecOps and sprints, and recommendations to the PMO. The metrics

consist of presenting the Lead time, the Deployment Frequency and the Change Fail rate. When delivering the Contractor's Progress, Status and Management Report, the Contractor shall alert the NILE Program 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. The report shall be also briefed and discussed at the following NILE In Process Reviews (IPRs).

CDRL Deliverables:

A001–Contractors Progress and Management Reports
A00B– Contract Funds Status Report
A00E –Integrated Master Schedule
B008 – DevSecOps Report

7 GOVERNMENT FURNISHED PROPERTY/ INFORMATION/ EQUIPMENT (GFP/GFI/GFE)

This section applies to all the Performance Requirements on this Contract. Government Furnished Equipment (GFE), Government Furnished Information (GFI) or Government Furnished Property (GFP) may be used by the Contractor to perform Engineering Services development and testing activities.

7.1 Government Furnished Property (GFP)- Attachment 5

a) The Contractor shall record, track, and maintain accountability for all Government Furnished Property (GFP), including Government Furnished Equipment (GFE) and GFI (Government Furnished Information) in accordance with DoDI 5000.64: Accountability and Management of DoD Equipment and Other Accountable Property, and NAVWAR Instruction 4440.12A: Management of Operating Materials and Supplies, Government Furnished Property, and Inventory. All GFP and GFI items provided shall only be used for performance of this contract.

b) If, for any reason, the performance under this contract ends, the Contractor shall return all GFP and GFI to the Government within forty- five (45) calendar days after performance ends, unless disposal has been authorized by the Government. The Contractor shall not modify or reproduce any GFI without prior written approval from the Government. The Contractor shall return any modified GFE to the original condition in which it was furnished to the Contractor unless a letter is sent by Contracting Officer to the Contractor allowing the return of modified GFI.

c) The Contractor shall provide a Status of GFE Report (CDRL A003), including an Inventory Listing containing the mandatory data elements specified in NAVWAR Instruction 4440.12A. At contract completion, the Contractor shall coordinate with the COR to receive GFP disposition instructions or return GFP to the Government Program Office.

The Contractor shall maintain the Status of Government Furnished Property Report in accordance with CDRL A003 and deliver at the end of the period of performance of this Task Order. The Contractor shall ensure inventory of all classified and unclassified GFE are maintained and dispositioned.
The Contractor shall ensure that any Mobile Test Station equipment is included to the Government Furnished Property inventory upon procurement and will be returned to the Government at the end of its use. The Contractor shall ensure they have a suitable transportation plan in place to ensure the inventory is securely returned to the Government.

The Government shall provide the GFE/GFI or a GFP list to the Contractor upon commencement of the performance period. The Contractor shall track GFE/GFI/GFP to include the specific make and model under CDRL A003.

The Government will provide the following GFI/GFE:

a) Information Packets for all TOWG and CCB meetings.
b) NILE PMO brief templates for TOWG and CCB meetings; and,
c) BCR 12 System Requirements Specification.
d) Link Monitoring and Management Tool (LMMT) Software v2.2
e) LMMT Software User's Manual (SUM)
f) Mobile Test Station

CDRL Deliverables:

A003–Government Furnished Property Report

7.2 Contractor Acquired Property

The Contractor shall be responsible for identifying monthly and cumulative Contractor Acquired Property (CAP) procurements in the Contractor's Progress, Status and Management Report (CDRL A001). At any time outside the monthly reporting cycle, the Contractor shall be capable of generating and providing a CAP inventory tracking report(s) (CDRL A003) of items procured, received, and delivered as applicable.

Any contractor acquired property under this contract must be either:

a. Specifically requested in writing by the Contractor at least two weeks prior to incurring any costs. Written Government authorization will be provided by the COR.
b. Acquired or procured as directed by the Government. Documentation of the analysis determining prices to be fair and reasonable should be retained and provided upon request.

The Contractor shall recommend and procure items that conform to the following applicable product validation, identification, and tracking requirements:

7.2.1 Product Validation

The Contractor shall certify that it purchases supplies from authorized resellers and/or distributers. The Contractor shall warrant that the products are new, in their original box. The Contractor shall obtain all manufacturer products submitted in contract/task order offers from authentic manufacturers or through legal distribution channels only, in accordance with all applicable laws and policies at the time of purchase. The Contractor shall provide the Government with a copy of the End User license agreement (the contractor must provide the license to the Procurement Contracting Officer (PCO) prior to purchase for review and the PCO must approve the license prior to purchase) and shall warrant that all manufacturer software is licensed originally to Government as the original licensee authorized to use the manufacturer software. The Contractor shall track the licensing information and have it available for Government review. As per section 10.3, the Contractor shall coordinate with the Contracting Officer at the Task Order level to determine if the proposed software is available under the DoD Enterprise Software Initiative (ESI) program.

7.2.2 Electronic Parts

To mitigate the use of counterfeit and/or defective electronic parts, the Contractor shall ensure all acquired electronic parts comply with the notification, inspection, testing, and authentication requirements in accordance with DFARS 252.246-7007 and DFARS 252.246-7008 specific to electronic parts.

7.2.3 IT Security Requirements

The Contractor shall ensure that all products recommended and/or procured meet cybersecurity and computer requirements.

7.2.4 Item Unique Identification (IUID)

In accordance with SECNAVINST 4440.34, the Contractor shall ensure that certain delivered items manufactured, integrated, or purchased (depending on if item meets a unit cost threshold, is serially managed, or if Government specifies identification required) have an item unique identification or Unique Item Identifier (UII). If specified by the Government, prior to delivery, the Contractor shall clearly mark and identify each applicable item based on the guidance provided in DoD MIL-STD-130N for those items not already marked. With Government concurrence, the Contractor shall specify the construct, syntax, marking methodology, and quality methodology chosen to mark the required parts and any corresponding technical justification. All IUID information shall be recorded and shall be subject to Government review. The Contractor shall track IUID items and maintain information being recorded. Prior to delivery of applicable CAP item, the Contractor shall register items with Unique Item Identifier (UII) in the IUID Registry.

CDRL Deliverables:

A001–Contractor Progress and Management Report
A003–Government Furnished Property Report
A00F–Contractor Acquired Property List

7.3 GFE COMSEC Requirements for Non-US Contractor

a) In accordance with Paragraph 3.1 (g)[6] of the In-Service Support (ISS) 6 Performance Work Statement (PWS), the Contractor shall be required to conduct Link 22 system testing and integration utilizing the Link 22 COMSEC device (LLC 7M). The United States (US) Government will provide as Government Furnished Equipment (GFE) six (6) LLC 7M units to the Government of the successful Offeror (Contractor).
b) If the proposal contains a teaming arrangement and the Subcontractor is a non-US company, the Subcontractor's Government will receive, transfer, and permit Contractor use of the LLC 7M units in accordance with the requirements of para 3.2.4[7] of the ISS6 PWS. The US Government will retain legal title over the LLC 7M units and retains the right to possess the articles as needed.
c) In accordance with the relevant requirements of the NILE ISS Memorandum of Understanding (MoU) as amended, the Subcontractor's Government will legally bind the Subcontractor to a requirement that the Subcontractor will not retransfer or otherwise use the LLC 7Ms or any related export-controlled information furnished by the Subcontractor's Government for any purpose other than the purposes authorized under either the ISS MoU or the ISS6 PWS. The Subcontractor must also be legally bound not to retransfer either the LLC 7Ms or any related export-controlled information to another contractor or subcontractor unless that contractor or subcontractor has been legally bound by its government to limit use of the LLC 7Ms or related information to the purposes authorized under either the ISS MOU or the ISS6 PWS**.**
d) Prior to transfer of the LLC 7Ms from the US Government to the Subcontractor's Government, the Subcontractor's Government will be requested to sign a Country Over Private Entity (COPE) Agreement for Third Party Transfer with the US Government for the purpose of authorizing the LLC 7M transfer (see Appendix B. A sample COPE Agreement will be provided separately to the Subcontractor's Government for the purpose of carrying out this agreement.
e) Following signature of a COPE Agreement, and prior to transfer of the LLC 7Ms from the Subcontractor's Government to the Subcontractor, the Subcontractor shall execute a Private Company Assurance Form for Third Party Transfer with the Subcontractor's Government for the purpose of authorizing the LLC 7M transfer and acknowledging the

[6] Paragraph 3.1 (g) states that the Contractor will provide "Link 22 system expertise to the Link Level Communications Security 7M (LLC 7M) manufacturer, to support the integration of the LLC 7M into the Link 22 architecture".

[7] Paragraph 3.2.4 states "the Contractor shall be required to ensure continued compatibility between the LLC 7M and the NILE Products to support the NILE PMO in assessing the system level aspects of the LLC 7M".

f) Subcontractor's responsibilities under the transfer of the LLC 7Ms. The Private Company Assurance form will be provided by the US Government as an attachment to the ISS6 Contract.

8 Place and Period of Performance

8.1 Place of Performance

The place of performance for efforts under this PWS shall be at Government site and Contractor site facilities as designated by the Contracting Officer Representative (COR). Telework is authorized on a case-by-case basis upon approval by COR.

Accomplishment of the requirements in this PWS requires work at the following locations: San Diego, CA. Task performance will be at Contractor facilities, on site at Government facilities and at locations during travel in support of the NILE Technical Meetings.

The Contractor shall provide services from its site located within a 60-minute commute time of the Government on-site locations. Response time availability is essential for responding to ad-hoc inquiries and data calls. There may also be instances where the Contractor shall be required to provide work at another Government location or Contractor location.

8.2 On-site and Off-site Support

The primary place of performance for efforts under this PWS shall be at the Contractor facilities. The Contractor shall ensure personnel and subject matter experts are able to successfully support task requirements. Regardless of on-site or off-site designation of contractor personnel, all tasks may require daily and/or ad hoc access to classified spaces, Government labs, networks and/or platforms. All classified work shall be performed at the approved locations in accordance with DD Form 254.

8.3 Period of Performance

The period of performance will have a five-year base ordering period and an option to extend services to six months under FAR 52.217-8. In certain situations, the Task Order may be extended for the past five years for up to six months, pursuant to FAR 52.217-8, Option to Extend Services, and FAR 52.217-9, Option to Extend the Term of the Contract, as applicable.

9 SECURITY

The Contractor shall take all measures necessary to ensure access up to SECRET data, information, and spaces. The Contractor shall have adequate facilities to perform all tasks and functions of this contract, including a Facility Security Clearance and a COMSEC Account/Custodianship up to the SECRET level. The Contractor shall ensure SECRET security clearance level for Contractor personnel. The Contractor shall be required to host and attend meetings classified up to the SECRET level. The Contractor will need to be NATO Read-on as noted in the DD254.

To fully support a secured facility with COMSEC, the Contractor shall adhere to the Committee on National Security Systems (CNSS) reference No. 4005 for 'Safeguarding COMSEC Facilities and Materials'. Additionally, the Contractor must ensure that the facility and associated space requirements (such as physical playout, barriers, windows, manpower, etc.) have been approved utilizing CNSSI 4005 prior to Contractor approval. For COMSEC security incidents and reporting, the Contractor must adhere to CNSSI reference 4003 for "Reporting and Evaluating COMSEC Incidents". Any individual handling and processing COMSEC material must attain proper approval; the Contractor must have an established COMSEC Account number and COMSEC Manager to process the clearances for individuals handling COMSEC materials and associated key management infrastructure.

OPSEC REQUIREMENTS: All work shall be performed in accordance with DoD and Navy Operations Security (OPSEC) requirements and in accordance with the OPSEC Attachment to the DD254.

Software, hardware and firmware used for maintenance or diagnostics shall be maintained within the secure computing facility and even if unclassified, shall be separately controlled.

The Contractor shall work with the NILE PMO to facilitate access of appropriate information to Link 22 stakeholders. This may typically include ITAR regulations, Technical Assistance Agreements and/or export licenses.

9.1 System Security Plan and Plans of Action and Milestones (SSP/POAM) reviews

a) Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.
b) If the Government determines that the SSP(s) 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 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 action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.
c) Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) 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(s).
d) The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

9.2 Compliance to NIST 800-171

a) The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171) or establish an SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012 and DFARS clause 252.204.7021, for all covered contractor information systems affecting this contract.
b) 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:
   (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 protection acceptable to the Government may be substituted.
   (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.

(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.
(4) Audit user privileges on at least an annual basis.
(5) Implement:
    i. 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 a SSP and POAM); and,
    ii. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program).
(6) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.
(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.

9.3 Cyber Incident Response

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.

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.

If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the 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 contracting officer will approve or disapprove the request after coordination with DC3.

9.4 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.

9.5 NCIS/Industry Monitoring

In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (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.

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.

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-US law.

9.6 Cyber IT and Cybersecurity Personnel

The Cyberspace workforce elements addressed include Contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, Contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed Contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

The Contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the Task/Delivery Order can require additional updates at any time.

Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR).

Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

9.7 Design, Integration, Configuration or Installation of Hardware/Software

The Contractor shall ensure any equipment/system installed or integrated into a Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The Contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16. 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 ELA's that are in effect can be found at www.esi.mil.

9.8 Product Recommendations

The Contractor shall ensure that all products recommended and/or procured that impact cybersecurity or Information Assurance (IA) shall be selected from the NIAP Validated Products List. The Contractor shall ensure the products chosen are based on the appropriate Evaluated Assurance Level (EAL) for the network involved and utilized in accordance with latest Defense Information Systems Agency (DISA)

policy at time of order. The Contractor shall store all product information and have it available for Government review as needed.

9.9 Security Management

All work performed under this PWS shall be performed in accordance with DD Form 254. Performance of this task by the Contractor shall require access up to, and including, SECRET and NATO SECRET (NS). The Contractor shall attend meetings classified up to the SECRET and NS level.

This effort requests access to NATO information: This means information/documents belonging to and circulated by NATO. Access to NATO information requires final Government clearance at the appropriate level. Prior approval from NAVWAR's NATO Control Officer (NCO)/Alternate (CODE 83310, 619-553-3005/3191) is required before the Contractor or a Subcontractor shall be granted access to NATO material. Additionally, a special briefing shall be provided by the Contractor's Facility Security Officer (FSO).

The Contractor shall be required to access the Secret Internet Protocol Router Network (SIPRNet). SIPRNet is not authorized to process or transmit NATO Restricted, NATO Confidential or NATO Secret data.

Note: If the Contractor is a United States entity, if foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC SD foreign travel team, OTC2, Room 1656 for action. A Request for Foreign Travel form shall be submitted for each traveler to initiate the release of a clearance message at least 35 days in advance of departure. Each traveler shall also submit a Personal Protection Plan (PPP) and shall attend a Level 1 Antiterrorism/Force Protection briefing within one year of departure, and a country specific briefing within 90 days of departure.

9.10 Classified Technical Data

The Contractor shall identify and implement the appropriate organizational procedures necessary to maintain U.S. SECRET and NATO SECRET classification level during modification and testing of particular system requirements. These procedures shall be established and submitted to the designated security authorities for approval. Coding, integration, and testing activities shall be organized in a way to minimize the use of classified parameters.

9.11 Security Training

Regardless of the contract security level required, the Contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the Contractor's designated Security Officer shall track the following information: security clearance information; dates possessing Common Access Cards; issuance and expiration dates for SPAWAR/SSC Atlantic/SSC Pacific Badge; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; CSWF certifications; etc. The Contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

9.12 Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFAR's PGI 239.7102-3 have promulgated that Contractor personnel shall have documented current cybersecurity certification status within their contract. The Contractor shall develop, maintain, and submit a monthly CSWF Report. IAW clause DFARS 252.239-7001, the Contractor shall provide a CSWF list that identifies those individuals who are IA trained and certified. The prime Contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. The Contractor

shall verify with the COR or other Government representative the proper labor category cybersecurity designation and certification requirements.

The Contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on contract, the Contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the contract, and if applicable, are certified/credentialed for the CSWF. A favorable background determination is determined by either a National Agency Check with Inquiries (NACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI) and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or SPAWAR/SSC Atlantic/SSC Pacific information. Cost to meet these security requirements is not directly chargeable to contract.

When a Contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) are required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, Contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each Contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, Contractors shall seek latest guidance from their appointed company Security Officer and the NAVWAR/SSC Atlantic/SSC Pacific Information Assurance Management (IAM) office:

a) For annual DoD Cybersecurity/IA Awareness training, Contractors shall use this site: https://twms.nmci.navy.mil/. For those Contractors requiring initial training and do not have a CAC, contact the NAVWAR/SSC Atlantic/SSC Pacific IAM office at phone number (843) 218-6152 or e-mail questions to ssc_lant_iam_office.fcm@navy.mil for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.
b) For SAAR-N form, the Contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NAVWAR/SSC Atlantic/SSC Pacific IAM office at or from the website: https://navalforms.documentservices.dla.mil/. Digitally signed forms will be routed to the IAM office via encrypted e-mail to ssclant_it_secmtg@navy.mil.

9.13 COMSEC Equipment

The Contractor shall manage the use and storage of the Link 22 COMSEC devices, fill devices, and key materials in accordance with established procedures for handling COMSEC material. Non-US Contractors' use and storage of this equipment shall be in accordance with an approved INFOSEC Equipment Agreement (IEA). Facilities used for modification and testing of the SNC and NRS shall possess the proper accreditation prior to storage and processing of classified data. Installation of COMSEC equipment shall be performed in accordance with the requirements of SDIP-29.

9.13.1 Offshore Procurement of COMSEC Equipment

Due to the unique sensitivity of Communications Security and to maintain rigid control over the integrity of COMSEC equipment, no subcontracts or purchase orders which involve design, manufacture, production, assembly or test in a location not in the United States, of equipment, assemblies, accessories or parts performing cryptographic functions shall be made under this contract without prior specific

approval of the Contracting Officer. The Contractor further agrees to include this text in any and all subcontracts to this contract for equipment, assemblies, accessories or parts.

9.14 NILE Products Security

The Contractor shall ensure that the NILE laboratory is not connected to the Internet or any Contractor intranet. The Contractor shall ensure that the NILE products are isolated from Internet/intranet connections when stored and shall be encrypted should they be sent over an Internet connection for the purposes of fulfilling the requirements of this contract. Contractor shall ensure that any hardware or processes to facilitate homeworking, or working with subcontractors, conform to the requirements of the DD254.

10 TASK ORDER PROGRAM MANAGEMENT AND ADMINISTRATION

All work to be performed under this PWS shall be defined and implemented via the issuance of Task Orders/Delivery Orders (TOs/DOs) that will specify the type of effort, the level of effort, data requirements, funding authorization, and the period of performance. As specified in individual task orders, the Contractor shall submit cost proposals for Engineering Services and other CLINs that are not pre-priced. The contractor's cost proposals shall be in accordance with its approved Disclosure Statement and Federal Acquisition Regulation (FAR) 15.403-4, as applicable. The Contractor's proposals shall provide information to substantiate all proposed costs including a Basis of Estimate (BoE) for each CLIN and a proposed schedule with detail commensurate with the value of the prospective order.

10.1 Contract Kick-Off

A Kick-Off Meeting will be coordinated by the Contractor with the Government and conducted no later than 10 business days after task order award. At Contract Kick-Off the Contractor shall provide a detailed transition plan to include introducing the Prime and Subcontractor team, the staffing plan and timeline, and steps the company will take to ensure a smooth transition for continued Program Office support. Participation by all Key and non-Key Personnel in the Contract Kick-Off is required.

All Key and non-Key Personnel shall provide on-site support to the Program Office no later than ten business days after task order award.

10.2 Services Contract Reporting

Services Contract Reporting (SCR) requirements apply to this contract. The Contractor shall report required SCR data fields using the SCR section of the System for Award Management (SAM) at following web address: https://sam.gov/SAM/.

Reporting inputs will be for the labor executed during the period of performance during each U.S. Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://sam.gov/SAM/.

10.3 Commercial/Commercial Off-the-shelf (COTS) License Management and Support

At the Task Order level, the Contractor shall inform the Government what pre-existing commercial/COTS software products are planned for delivery prior to award. The Contractor shall further provide copies of

the licenses associated with the proposed commercial/COTS deliverables and shall review such licenses for consistency with federal procurement law, and to ensure such licenses meet the Government end user needs. The Contractor shall coordinate with the Contracting Officer at the Task Order level to determine if the proposed software is available under the DoD Enterprise Software Initiative (ESI) program, and to resolve any duplicative licenses with Navy ESI software or PaaS/IaaS solutions. The Contractor shall identify any additional COTS licensing costs in the Contract Funds Status Report (CFSR) (CDRL A00B). The Contractor shall retain digital copies of end user license agreements for additional required commercial/COTS licenses that are not available under the DoD ESI program.

10.4 Labor Category

The Contractor shall provide qualified Key Personnel and non-Key Personnel that meet the Standard Labor Categories Descriptions, throughout contract performance. The Contractor shall ensure its employees satisfy the additional requirements specific to Key Personnel in this Task Order. For non-Key Personnel, at any time from start of award to the expiration of the period of performance, the Government reserves the right to request, and review resumes to ensure the Contractor is providing qualified personnel for each labor category. Upon request from the Contracting Officer or COR, the Contractor shall submit proof of qualifications to the COR for review for non-key personnel performing under this PWS. Such qualifications must be provided within 48 hours of the Government's request.

10.5 Task Order Transition

It is the desire of the Government to maintain continuity during the transition periods between prime contractors. In the event there is a follow-on award, and the incumbent is not the new contractor, the contractor of this task shall provide status update on transitional efforts and the progress for being fully transitioned within 30 days after Task Order award.

Incoming) Transition Strategy Brief and Execution Plan detailing how the contractor will work with the incumbent to understand current/open issues to ensure a seamless transition to support NILE PMO, how the contractor intends to manage personnel placement through the organization and negotiated contracts.	30 Days prior to transition & updates as required
(Outgoing) Transition Strategy Brief & Execution Plan	90 days prior to the end of period of performance for the contract and updates/revisions as required

The incumbent contractor shall provide a transition strategy that addresses these and other specific concerns and present their execution strategy 90 days prior to the execution of the transition which will be 60 days in duration (30 days before termination of current prime contractor service support contract to 30 days after new prime contractor is in place.)

Appendix A: Acronyms

ATDLP	Allied Tactical Data Link Publication
BCR	Block Cycle Release
BLOS	Beyond Line of Sight
BoE	Basis of Estimate
CCB	Configuration Control Board
CCRB	Configuration Control Review Board
CDRL	Contract Data Requirements List
CMP	Configuration Management Plan
COTS	Commercial Off the Shelf
CP	Change Proposal
CUI	Controlled Unclassified Information
DCMA	Defense Contract Management Agency
DEVSECOPS	Development, Security and Operations
DFARS	Defense Federal Acquisition Regulation Supplement
DLP	Data Link Processing
DR	Discrepancy Report
DTDMA	Dynamic Time Division Multiple Access
ER	Engineering Release
FAR	Federal Acquisition Regulation
FMS	Foreign Military Sales
FR	Feedback Report
GFE/GFI/GFP	Government Furnished Equipment, Information or Property
HW	Hardware
HF	High Frequency
IPR	In Process Review
IPT	Integrated Product Team
ISS	In-Service Support
LLC 7M	Link 22 Modernized Link Level COMSEC
MOU	Memorandum of Understanding
MSR	Monthly Status Report
MTS	Mobile Test Station
MUT Sim	Multi Units Test Simulator
NAS	Network Attached Storage
NAVWAR	Naval Information Warfare Systems Command
NCIS	Naval Criminal Investigative Service
NDI	Network Device Interface
NILE	NATO Improved Link Eleven

NITT	NILE Interoperability Test Tool
NRS	NILE Reference System
NS	NATO Secret
NSA	National Security Agency
NU	NATO Unclassified
ODCs	Other Direct Costs
PCO	Procuring Contracting Officer
PCR	Problem Change Report
PM	Program Manager
PR	Program Review
PWS	Performance Work Statement
RF	Radio Frequency
RFP	Request for Proposal
RMP	Risk Management Plan
SNC	System Network Controller
SNC-IDD	SNC Interface Design Description
SDD	SNC Software Design Description
SSP	System Security Plan
STANAG	Standardization Agreement
STM	System Technical Manuals
SVDD	Software Version Description Document
TDL	Tactical Data Link
TDP	Technical Data Package
TDS	Tactical Data System
TOD	Time of Day
TRR	Test Readiness Review
TOWG	Technical and Operational Working Group
UHF	Ultra-High Frequency
WBS	Work Breakdown Structure
WP	White Paper

Appendix B: Template Country Over Private Equity (COPE) Agreement

Blanket Country Over Private Entity (COPE) Standard Template

The Embassy of the United States of America presents its compliments to the Ministry of Foreign Affairs of (Host Country) and has the honor to refer to recent discussions regarding the potential transfer of defense articles and/or defense services from a third government to a private entity that is physically located within the jurisdiction of the Government of (Host Country) ("Private Entity").

The Government of the United States of America considers consenting to a transfer of defense articles and services from a third country to a Private Entity only upon being furnished with assurances from the Government of (Host Country).

In accordance with the foregoing, the Government of (Host Country) hereby gives its assurances that unless the prior written consent of the Government of the United States of America has been first obtained:

(A) It will not permit a private entity, which has received defense articles and/or services into the jurisdiction of the government of (Host Country), to retransfer said defense Articles and/or services,

or any component thereof, by sale, lease, release, assignment, loan conveyance or any other means to any Government, entity, international organization, or person not an officer, employee or agent of the private entity or the Government of (Host Country).

(B) It will not permit a private entity, which has received defense articles and/or services into the jurisdiction of the government of (Host Country), to use said defense articles and/or services, or any component thereof, for any purpose other than those for which provided.

(C) It will ensure that a private entity, which has received defense articles and/or services into the jurisdiction of the government of (Host Country), maintains the security of said defense articles and/or equipment, or any component thereof, and will provide substantially the same degree of security protection afforded to such articles and information by the Government of the United States of America; and

(D) It will retain ultimate responsibility for ensuring that any technical information retained by a private entity, which has received defense articles and/or services into the jurisdiction of the government of (Host Country), remains in the territorial boundaries of (Host Country) and under the legal jurisdiction of the Government of (Host Country).

The Embassy proposes that if the foregoing is acceptable to the Government of (Host Country), this note, together with the Ministry's reply, shall constitute an agreement between the two governments (a Country Over Private Entity Blanket Assurance agreement) which shall enter into force on the date of the Ministry's reply. The Embassy of the United States of America avails itself of this opportunity to renew to the Ministry of Foreign Affairs of the (Host Country) the assurances of its highest consideration.

Appendix C: Configuration Management Document Definitions

Document Type	Definition
Block Cycle Release	A Block Cycle Release (BCR) contains, among other things: • SNC software that is fully tested and is intended for Operational use. • NRS software is a suite of tools used for DLP or SNC testing purposes. • Core Documentation (e.g. SNC SS, NRS SS, LLC IRS, SPC SS, etc.) fully reviewed.
Engineering Release	A BCR Engineering Release (ER) contains, among other things: • SNC software that is partially tested and is intended for Testing purposes only, NOT for Operational use. • Core Documentation in Draft status.
Feedback Report	A Feedback Report (FR) is the mechanism available to the Nations/Organizations/Link 22 Partner Nations to provide feedback on problems, suggestions, and questions about Link 22. FRs are initially analyzed by the Government and forwarded to the ISS Contractor (when required) for analysis and in parallel to all NILE and Link 22 Partner Nations/Organizations for review.
White Papers	White Papers (WP) are technical papers produced by the ISS Contractor containing studies that address contractual PWS items and/or topics of specific subjects requiring investigation/analysis. WPs may be generated by activities related to PWS items and FRs, which usually contain a recommendation and a way-ahead. White Paper may be categorized into either White Paper Major or White Paper Minor.
Problem Change Report	A Problem Change Report (PCR) documents the analysis describing the solution of a software problem or of a potential software change from the existing baseline. The PCR is the method used by the ISS contractor to trace the software problems, generated as a result of PWS items (via WPs), FRs or internal testing. Most PCRs are approved by the CCRB when the analysis/design of the solution is agreed upon. The implementation of an agreed PCR always results in software changes after approvals. A Problem Change Report (PCR) may be categorized into PCR Major or PCR Minor.
Change Proposal	Change Proposals (CP) document modifications to baseline Link 22 documentation. CPs may be generated by the activities related to a PWS items, FRs, internal testing and/or PCRs. CPs are delivered to the CCRB for action. At a minimum the CP should detail which Configuration Items are affected and provide high-level information to enable decisions to be made.

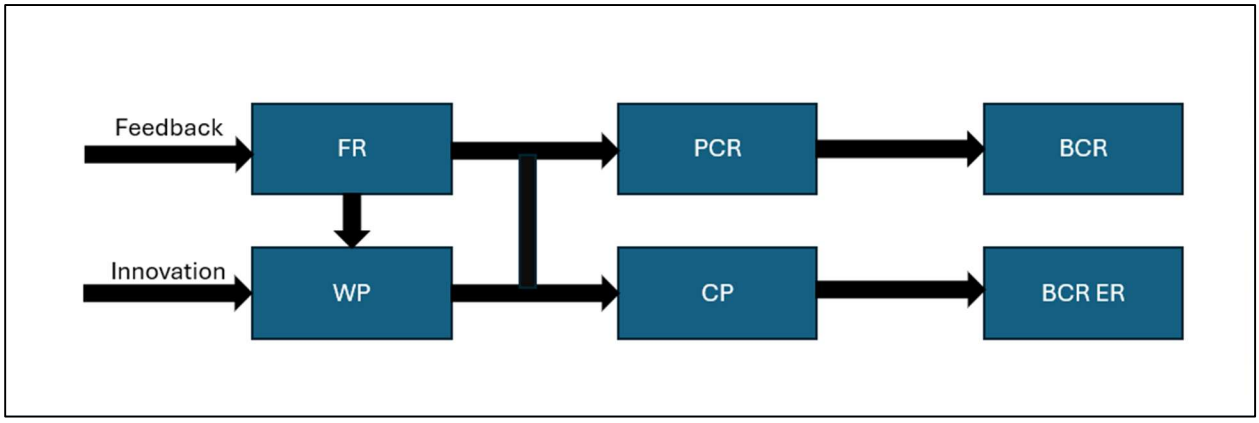

Figure 3: Configuration Management Document Flow