Office of Acquisition

Boulevard Léopold III
B-1110 Brussels, Belgium

NCIA/ACQ/2023/07301
22 September 2023

To : See Distribution List

Subject : **Request for Quotation RFQ-CO-115518-NPKI-M**
Provide NATO Public-Key Infrastructure Capability (NPKI), WP 2 - Data Centre Installation

Reference(s) :
A. AC/4-D(2019)0004 (INV) dated 04 Jul 2019
B. AC/4(PP)D/26904-ADD9 dated 19 Feb 2021
C. AC/4-DS(2021)0005 dated 13 Apr 2021
D. AC/4(PP)D/26904-ADD13 (INV) dated 30 Aug 2023

Dear Sir/Madam,

1 Your firm is hereby invited to participate in a Basic Ordering Agreement Plus (BOA+) competition for the design and installation of the underlying infrastructure, to be built in two data centres, which will provide a platform to host NATO's new PKI Services.

2 The contract award will be based on the quotation evaluated as the lowest price, technically compliant in accordance with the selection criteria set forth in the RFQ Instructions.

3 **THE CLOSING TIME FOR SUBMISSION OF QUOTATIONS IN RESPONSE TO THIS RFQ IS 13:00 HOURS (CENTRAL EUROPEAN TIME) ON FRIDAY, 3 NOVEMBER 2023.**

4 This RFQ consists of the following documents:

a) **Book I – The RFQ Instructions.** Book I provides the general solicitation information and includes the following annexes:

i. Annex A – Clarification Request Forms;
ii. Annex B – Administrative Certificates;
iii. Annex C – Pricing Sheets. (Note: The Pricing Sheets must be completed exactly as instructed);
iv. Annex D – Compliance Table.

b) **Book II – The Prospective Contract.** Book II contains the following sections:

i. Signature Page;
ii. Part I - Schedule of Supplies and Services (SSS);
iii. Part II - Contract Special Provisions;
iv. Part III - Contract General Provisions;
v. Part IV - Statement of Work.

5 The overall security classification of this RFQ is NATO UNCLASSIFIED.

NATO Communications and Information Agency
Boulevard Leopold III
1110 Brussels
Belgium
www.ncia.nato.int

NCIA/ACQ/2023/07301

6 This RFQ is the property of the NCI Agency and shall be protected in accordance with the applicable national security regulations.

7 In accordance with the NATO Management of Non-Classified NATO Information policy (C-M(2002)60), this RFQ shall NOT be published on the internet.

8 Your firm is requested to complete and return the enclosed acknowledgement of receipt within 5 days of receipt of this RFQ, informing NCI Agency of your firm's intention to quote/not to quote. Your firm is not bound by its initial decision, and if your firm decides to reverse your firm's stated intention at a later date, your firm is requested to advise the NCI Agency by a separate email.

9 The reference for this RFQ is **RFQ-CO-115518-NPKI-M**, and all correspondence concerning the RFQ should reference this number.

10 Prospective Offerors are advised that the NCI Agency reserves the right to cancel this RFQ at any time in its entirety and bears no liability for quotation preparation costs incurred by firms or any other collateral costs if solicitation cancellation occurs.

11 Your point of contact for all information concerning this RFQ is Ms Sumiko Duncan, Senior Contracting Officer, who can be reached at RFQ-CO-115518-NPKI-M@ncia.nato.int .

For the Chief of Acquisition:

Rebecca Benson

Digitally signed by Rebecca Benson
Date: 2023.09.22 09:58:54 +02'00'

Rebecca Benson
Principal Contracting Officer

Enclosure(s):

1. Attachment A - Acknowledgement of Receipt of Request for Quotation
2. Book I – The RFQ Instructions
3. Book II – The Prospective Contract

NCIA/ACQ/2023/07301

Attachment A

Acknowledgement of Receipt of Request for Quotation

RFQ-CO-115518-NPKI-M

Please complete and return within 5 days by e-mail: RFQ-CO-115518-NPKI-M@ncia.nato.int

for the attention of Ms. Sumiko Duncan.

We hereby advise that we have received Request for Quotation RFQ-CO-115518-NPKI-M

on ....., together with all enclosures listed in the Table of Contents.

CHECK ONE

{ } As of this date and without commitment on our part, we do intend to submit a quotation.

{ } We do not intend to submit a quotation.

{ } We are reviewing the requirements of the RFQ and will notify you of our decision as soon as possible.

Signature: _____

Printed Name: _____

Title: _____

Company: _____

Address: _____

NCIA/ACQ/2023/07301

Distribution List for RFQ-CO-115518-NPKI-M

External

- **Offerors** (sent separately in electronic version)

- **NATO Delegations** (Attn: Investment Adviser):

  Albania
  Belgium
  Bulgaria
  Canada
  Croatia
  Czech Republic
  Denmark
  Estonia
  France
  Germany
  Greece
  Hungary
  Iceland
  Italy
  Latvia
  Lithuania
  Luxembourg
  Montenegro
  The Netherlands
  North Macedonia
  Norway
  Poland
  Portugal
  Romania
  Slovakia
  Slovenia
  Spain
  Türkiye
  United Kingdom
  United States

  Belgium Ministry of Economic Affairs

- **Embassies in Brussels** (Attn: Commercial Attaché):

  Albania
  Belgium
  Bulgaria
  Canada
  Croatia
  Czech Republic
  Denmark
  Estonia
  France
  Germany
  Greece

NCIA/ACQ/2023/07301

Hungary
Iceland
Italy
Latvia
Lithuania
Luxembourg
Montenegro
The Netherlands
North Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Türkiye
United Kingdom
United States

- **NATO HQ**

NATO Office of Resources
Management and Implementation Branch – Attn: Deputy Branch Chief

Director, NATO HQ C3 Staff
Attn: Executive Co-ordinator

- **SACTREPEUR**
  Attn: Infrastructure Assistant

- **Strategic Commands**

ACO/DCOS CIS & Cyber Defence

ACT/DCOS Capability Development

- **NCI Agency –Internal Distribution**

ACQ Chief of Acquisition (Mrs Jennifer Upton)

ACQ Deputy Chief of Acquisition - Procurement & Policy (Mr Alexandre Vitry)

Administrator Contracts Award Board (Mr Nicolas Rego)

ACQ Principal Contracting Officer (Ms Rebecca Benson)

ACQ Principal IPS Officer (Mr Massimiliano Filippi)

NLO (Mr Bruno Modesto Melo)

NCSC Chief Cyber Security (Mr Ian West)

NCSC Head Capability Development (Ms Manisha Parmar)

NCIA/ACQ/2023/07301

NCSC Acting Head Cyber Security Programme Delivery Branch (Mr Tyson McWha)

NCSC Principal Project Manager (Mr Miles Knight)

Legal Office (Mr Kelby Kershner)

Chief Technology Office (Mr Jose Herrero)

Registry

- **NCI Agency – All NATEXs**

RFQ-CO-115518-NPKI-M

PROVIDE NATO PUBLIC-KEY INFRASTRUCTURE CAPABILITY (NPKI)

WP 2 - DATA CENTRE INSTALLATION

NATO Communications and Information Agency

NCI AGENCY

REQUEST FOR QUOTATION

AUTHORISATION/SERIAL NO.

AC/4-DS(2021)0005

CP 0A0155 - SERIAL 2005/0IS03072-20/28/29

GENERAL INDEX

RFQ-CO-115518-NPKI-M

PROVIDE NATO PUBLIC-KEY INFRASTRUCTURE CAPABILITY (NPKI)

WP 2 - DATA CENTRE INSTALLATION

NATO Communications and Information Agency

BOOK I

RFQ INSTRUCTIONS

Table of Contents

SECTION I - INTRODUCTION

1.1 PURPOSE

1.1.1 The purpose of this Request for Quotation (RFQ) is to award a Contract for the deployment, configuration and operation of NATO PKI Mitigation (NPKI-M) hosting capabilities in two Data Centres, located at NATO Headquarters (NHQ), Brussels (BEL) and in Mons (BEL).

1.2 SCOPE OF WORK

1.2.1 The NATO Public Key Infrastructure Mitigation (NPKI-M) project that is comprised of several Work Packages (WP) is to provide NATO with a set of security services enabling confidentiality, integrity, authentication, and non-repudiation. The principal aim of the project is to serve as a highly scalable network and user domain authentication, identification and security supporting framework as well as providing a confidentiality service to support community of interest separation. The NPKI-M project will provide the key and information management functions to other Communication and Information Systems (CIS) security services by means of lifecycle certificate management.

1.2.2 The primary objective of WP 2 – Data Centre Installation, which is the subject of this RFQ, relates to the design and installation of the underlying infrastructure, to be built in two data centres at NATO HQ and in Mons, that will provide a platform to host the new NPKI Services, which will enhance the security of NATO systems.

1.2.3 The Period of Performance (PoP) from the Effective Date of Contract (EDC) is EDC + 114 weeks, to include warranty.

1.3 GOVERNING RULES, ELIGIBILITY, AND EXCLUSION PROVISIONS

1.3.1 This solicitation is issued in accordance with the Procedure Governing the Use of Basic Ordering Agreements Concluded by the NATO Communications and Information Agency - 2019 Version set forth in document AC/4-D(2019)0004 (INV) dated 04 July 2019.

Pursuant to the BOA Plus procedures, the RFQ is open to companies from participating NATO member nations which are holders of an active NCI Agency Basic Ordering Agreement (BOA). Further, the BOA Plus procedures allow national authorities to nominate eligible bidders without an active BOA. Hence, qualified and certified companies that provide a Declaration of Eligibility (DoE), **sent** by their Delegation/Mission to NATO to the NCI Agency contracting authority will also be eligible.

1.4 LOWEST PRICE TECHNICALLY COMPLIANT (LPTC) EVALUATION METHOD

1.4.1 The evaluation method to be used in the selection of the successful Offeror under this solicitation is the Lowest Price Technical Compliant procedures set forth in AC/4-D(2019)0004 (INV).

1.4.2 The quotation evaluation criteria and the detailed evaluation procedures are described in Section 4.

1.4.3 This RFQ will not be subject to a public RFQ opening.

1.5 SECURITY

1.5.1 The overall security classification of this solicitation is NATO UNCLASSIFIED.

1.5.2 The selected Contractor will be required to handle and store classified material to the level of “NATO SECRET”. In addition, Contractor personnel will be required to work unescorted in Class II Security areas and therefore, access can only be permitted to cleared individuals. Only firms maintaining such cleared facilities and the appropriate personnel clearances will be able to perform the resulting Contract

1.5.3 Should the Contractor be unable to perform the Contract due to a lack of the proper facility/security clearances, this shall neither form the basis for a claim of adjustment or an extension of schedule nor can it be considered a mitigating circumstance in the case of an assessment of Liquidated Damages or a determination of Termination For Default by the Purchaser.

1.5.4 The selected Contractor’s personnel working at NATO sites as well as the Contractor’s personnel at the Contractor’s facility directly working on this project, shall possess a security clearance of “NATO SECRET”.

1.5.5 The Contractor personnel without such a clearance, confirmed by the appropriate national security authority and transmitted to the cognisant NATO security officer at least fourteen (14) days prior to the site visit, will be denied access to NATO site(s). Denial of such access by the Purchaser may not be used by the Contractor as the basis for a claim of adjustment or an extension of schedule nor can the denial of access be considered a mitigating circumstance in the case of an assessment of Liquidated Damages or a determination of Termination for Default by the Purchaser.

1.5.6 Offerors are advised that Contract signature will not be delayed in order to allow the processing of security clearances for personnel or facilities and, should the otherwise successful Offeror not be in a position to accept the offered Contract within a reasonable period of time, due to the fact that its personnel or facilities do not possess the appropriate security clearance(s), the Purchaser may determine the Offeror’s quotation to be non-compliant and offer the Contract to the next ranking Offeror.

1.5.7 All documentation, including the RFQ itself, all applicable documents and any reference documents provided by the Purchaser are solely to be used for the purpose of preparing a response to this RFQ. They are to be safeguarded at the appropriate level according to their classification. Any Reference Documents are provided “as is, without any warranty” as to quality or accuracy.

SECTION II – GENERAL RFQ INSTRUCTIONS

2.1 DEFINITIONS

2.1.1 The term “Assembly” as used herein means an item forming a portion of equipment that can be provisioned and replaced as an entity and which normally incorporates replaceable parts or groups of parts.

2.1.2 The term “Basic Ordering Agreement” (BOA) refers to the acquisition instruments negotiated between suppliers of products / services and the NCI Agency, on behalf of NATO.

2.1.3 The term "Compliance" as used herein means strict conformity to the requirements and standards specified in this Request for Quotation.

2.1.4 The term "Contractor" refers to a firm of a participating country which has signed a Contract under which he will perform a service, manufacture a product, or carry out works for NATO.

2.1.5 The term "Offeror" as used herein refers to a firm, consortium, or joint venture which submits an offer in response to this solicitation.

2.1.6 The term “Participating Country” as used herein means one of the contributory NATO nations in the project, namely, (in alphabetical order): BELGIUM, BULGARIA, CANADA, CZECH REPUBLIC, DENMARK, ESTONIA, FINLAND, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TÜRKIYE, UNITED KINGDOM, UNITED STATES OF AMERICA.

2.1.7 The term "Purchaser" refers to the authority issuing the RFQ and/or awarding the Contract (the NCI Agency).

2.1.8 In accordance with MIL-HDBK-505, the term “Sub-Assembly” as used herein refers to a portion of an assembly consisting of two or more parts that can be provisioned and replaced as an entity. The definition purposely excludes components and/or parts.

2.2 ELIGIBILITY

2.2.1 This RFQ is being conducted under Basic Ordering Agreement (BOA) Plus procedures, therefore, the solicitation will be issued to firms listed on the Offeror List and firms that have confirmed DoE(s) received by NCIA as described in Section I, Paragraph 1.3.2.

2.2.2 All Contractors, sub-Contractors and manufacturers, at any tier, must be from Participating Countries.

2.2.3 None of the work, including project design, labour and services shall be performed other than by firms from and within Participating Countries.

2.2.4 No materials or items of equipment down to and including identifiable sub-assemblies shall be manufactured or assembled by a firm other than from and within a Participating Country.

2.2.5 The intellectual property rights to all design documentation and related system operating software shall reside in NATO member countries, and no license fee, or royalty charges shall be paid by the Contractor to firms, individuals or governments other than within the NATO member countries.

2.3 QUOTATION SUBMITTAL AND RFQ CLOSING DATE

2.3.1 All Quotations shall be in the possession of the Purchaser at the address given below in Section II, Paragraph 2.3.2 before **13:00 hours (Central European Time) on Friday, 3 November 2023** at which time and date the RFQ shall be closed.

2.3.2 Quotations shall be delivered in electronic format only to the following email address:

RFQ-CO-115518-NPKI-M@ncia.nato.int

2.3.3 The Quotation shall consist of three (3) separate subject emails:

2.3.3.1 For the first e-mail the subject line shall read: "RFQ-CO-115518-NPKI-M - Official Quote for [company name] - Part I - Administrative Package". The e-mail content shall be as described in Paragraph 3.2.2 below, with no password protection to the file and shall be not larger than 20MB total.

2.3.3.2 For the second e-mail the subject line shall read: "RFQ-CO-115518-NPKI-M Official Quote for [company name] - Part II - Price Quotation". The e-mail content shall be as described in Paragraph 3.2.2 below, with no password protection to the file, and shall be not larger than 20MB total.

2.3.3.3 For the third e-mail the subject line shall read: "RFQ-CO-115518-NPKI-M - Official Quote for [company name] - Part III - Technical Proposal". The e-mail content shall be as described in Paragraph 3.2.2 below, with no password protection to the file, and shall be not larger than 20MB total per e-mail. For large Technical Proposals, multiple e-mails may be required to submit the entire package. In such case, Offerors shall clearly indicate the correct order in the e-mail subject line.

2.3.4 Quotations which are delivered to the Purchaser after the specified time and date set forth above for RFQ Closing are "Late Quotations" and shall not be considered for award. Consideration of Late Quotation - The Purchaser considers that it is the responsibility of the Offeror to ensure that the Quotation submission arrives by the specified RFQ Closing Date and Time. A late Quotation shall only be considered for award under the following circumstances:

2.3.4.1 A Contract has not already been awarded pursuant to the RFQ, and;

2.3.4.2 The Quotation was sent to the e-mail address specified in the RFQ and the delay was solely the fault of the Purchaser.

2.3.5 It is the responsibility of the Offeror to ensure that the quotation submission is duly completed by the specified RFQ Closing time and date. If a quotation received at the NCI Agency's facility by electronic data interchange is unreadable to the degree that conformance to the essential requirements of the solicitation cannot be ascertained, the Purchaser will immediately notify the Offeror that the quotation will be rejected unless the Offeror provides clear and convincing evidence:

(a) Of the content of the Quotation as originally submitted; and,

(b)That the unreadable condition of the quotation was caused by Purchaser software or hardware error, malfunction, or other Purchaser mishandling.

2.4 REQUESTS FOR EXTENSION OF RFQ CLOSING DATE

2.4.1 All questions and requests for extension of the RFQ Closing Date must be submitted by e-mail. Such questions shall be forwarded to the point of contact specified in paragraph 2.5 below and shall arrive not later than seven (7) calendar days prior to the stated "RFQ Closing Date". The Purchaser is under no obligation to answer

requests submitted after this time. Extensions to the RFQ Closing date are at the discretion of the Purchaser.

2.5 PURCHASER POINT OF CONTACT

2.5.1 The Purchaser point of contact for all information concerning this RFQ is:

NATO Communications and Information Agency

Acquisition

NATO HQ

Boulevard Leopold III

B-1110 Brussels, Belgium

Attention: Ms. Sumiko Duncan, Senior Contracting Officer

2.5.2 Emails:

2.5.2.1 Questions/Clarifications/Quotation: RFQ-CO-115518-NPKI-M@ncia.nato.int

2.6 REQUESTS FOR RFQ CLARIFICATIONS

2.6.1 Offerors, during the solicitation period, are encouraged to query and seek clarification of any matters of a contractual, administrative and technical nature pertaining to this RFQ.

2.6.2 All questions and requests for clarification must be submitted by e-mail and using the form in Annex A of Book I – RFQ Instructions. All questions and requests must reference the section(s) in the RFQ subject for clarifications. The questions and/or requests shall be forwarded to the email address specified in paragraph 2.5.2.1 above and shall arrive not later than seven (7) calendar days prior to the stated "RFQ Closing Date". The Purchaser is under no obligation to answer questions submitted after this time. Requests for clarification must address the totality of the concerns of the Offeror for any given area, as the Offeror will generally not be permitted to revisit areas of the RFQ for additional clarification as noted in 2.6.3 below.

2.6.3 Offerors are advised that subsequent questions and/or requests for clarification included in a quotation shall neither be answered nor considered for evaluation and may be grounds for a determination of non-compliance.

2.6.4 Except as provided above, all questions will be answered by the Purchaser and the questions and answers (deprived of any means of identification of the questioner) will be issued in writing to all prospective Offerors. Answers will be provided on a weekly basis.

2.6.5 The published answers issued by the Purchaser shall be regarded as the authoritative interpretation of the RFQ, and may lead to a formal amendment to the RFQ. Such amendment may also contain changes to the language, terms, conditions and/or specifications of the RFQ. Amendments to the language of the RFQ included in the answers, and/or the formal RFQ amendment, shall be incorporated by the Offeror in its offer.

2.7 REQUESTS FOR WAIVERS AND DEVIATIONS

2.7.1 Offerors are informed that requests for alteration to, waivers of, or deviations from the Schedule, the Special Contract Provisions, the Terms and Conditions in the NCI Agency's Basic Ordering Agreement, the Technical Specifications, the Statement of Work and any other Terms and Conditions of the Prospective Contract will not be considered after the Request for Clarification process.

2.7.2 Requests for alterations to the other requirements, terms or conditions of the RFQ or the Prospective Contract may only be considered as part of the clarification process set forth in Section II, Paragraph 2.6 above. Requests for alterations to the specifications, terms and conditions of the Contract which are included in a Quotation as submitted may be regarded by the Purchaser as a qualification or condition of the Quotation and may be grounds for a determination of non-compliance.

2.8 AMENDMENT OF THE RFQ

2.8.1 The Purchaser may revise, amend or correct the terms, conditions and/or specifications and provisions of the RFQ documents at any time prior to the date set for the RFQ Closing Date. Any and all modifications will be transmitted to all prospective Offerors by an official amendment designated as such and signed by the Contracting Authority. Such amendment shall be recorded in the Acknowledgement of Receipt which the Offeror shall complete and enclose as part of his quotation. This process may be part of the clarification procedures set forth in Section II, Paragraph 2.6 above or may be an independent action on the part of the Purchaser.

2.8.2 The Purchaser will consider the potential impact of amendments on the ability of prospective Offerors to prepare a proper quotation within the allotted time. The Purchaser may extend the "RFQ Closing Date" at his discretion and such extension will be set forth in the amendment document.

2.8.3 In no case, however, will the closing date for receipt of quotation be less than seven (7) days from the date of issuance of any amendment to the RFQ.

2.9 MODIFICATION AND WITHDRAWAL OF QUOTATION

2.9.1 Quotations, once submitted, may be modified by Offerors, but only to the extent that the modifications are in writing, conform to the requirements of the RFQ, and are received by the Purchaser prior to the exact time and date established for RFQ Closing. Such modifications shall be considered as an integral part of the submitted quotation.

2.9.2 Modifications to quotations which arrive after the RFQ Closing Date will be considered as "Late Modifications" and will be processed in accordance with the procedure set forth above concerning "Late Quotation", except that unlike a "Late Quotation", the Purchaser will retain the modification until a selection is made. A modification to a quotation which is determined to be late will not be considered in the evaluation and selection process. If the Offeror submitting the modification is determined to be the successful Offeror on the basis of the unmodified quotation, the modification may then be opened. If the modification makes the terms of the quotation more favourable to the Purchaser, the modified quotation may be used as the basis of Contract award. The Purchaser, however, reserves the right to award a Contract to the apparent successful Offeror on the basis of the quotation submitted and disregard the late modification.

2.9.3 An Offeror may withdraw his Quotation at any time prior to Quotation Opening without penalty. In order to do so, an authorised agent or employee of the Offeror must provide an original statement of the firm's decision to withdraw the Quotation and remove the Quotation from the Purchaser's premises.

2.10 QUOTATION VALIDITY

2.10.1 Offerors shall be bound by the term of their quotation in which the Offeror has provided a quotation for a period of 6 months starting from the RFQ Closing Date specified in Section II, Paragraph 2.3.1.

2.10.2 In order to comply with this requirement, the Offeror shall complete the Certificate of Quotation Validity set forth in Annex B-3. Quotations offering less than the period of time referred to above for acceptance by the Purchaser may be determined to be non-compliant.

2.10.3 The Purchaser will endeavour to complete the evaluation and make an award within the period referred to above. However, should that period of time prove insufficient to render an award, the Purchaser reserves the right to request an extension of the period of validity of all quotations which remain under consideration for award.

2.10.4 Upon notification by the Purchaser of such a request for a time extension, the Offerors shall have the right to:

2.10.4.1 accept this extension of time in which case Offerors shall be bound by the terms of their quotation for the extended period of time and the Certificate of Quotation Validity extended accordingly; or

2.10.4.2 refuse this extension of time and withdraw the quotation without penalty.

2.10.5 Offerors shall not have the right to modify their quotations due to a Purchaser request for extension of the quotation validity unless expressly stated in such request.

2.11 CANCELLATION OF REQUEST FOR QUOTATIONS

2.11.1 The Purchaser may cancel, suspend or withdraw for re-issue at a later date this RFQ at any time prior to Contract award. No legal liability on the part of the Purchaser for payment of any sort shall arise and in no event will any Offeror have cause for action against the Purchaser for the recovery of costs incurred in connection with preparation and submission of a quotation in response to this RFQ.

2.12 ELECTRONIC TRANSMISSION OF INFORMATION AND DATA

2.12.1 The Purchaser will endeavour to communicate answers to requests for clarification and amendments to this RFQ to the prospective Offerors by the fastest means possible, including the use of e-mail where the firms have forwarded the necessary address information. All Offerors are consequently strongly encouraged to provide accurate email addressing information and notify the Purchaser at the earliest practicable date should any changes occur.

2.12.2 Offerors are cautioned that the Purchaser will rely exclusively on electronic mail to manage all correspondence, amendments, etc., related to this RFQ.

SECTION III - QUOTATION PREPARATION INSTRUCTIONS

3.1 GENERAL

3.1.1 Quotations shall be prepared in accordance with the instructions set forth herein. Failure to comply with these instructions may result in the Offer being declared non-compliant.

3.1.2 Quotations and all related documentation shall be submitted in the English language.

3.1.3 Offerors shall prepare a complete quotation which comprehensively addresses all requirements stated herein. The quotation shall demonstrate the Offeror's understanding of the RFQ and his ability to provide all the deliverables and services listed in the Schedule of Supplies and Services (SSS). Quotations which are not complete will be declared non-compliant.

3.1.4 The Offeror shall not restate the RFQ requirements in confirmatory terms only. The Offeror must clearly describe what is being offered and how the Offeror will meet all RFQ requirements. Statements in confirmatory terms will only be sufficient for determining the quotation to be non-compliant.

3.1.5 Offerors shall classify their response in accordance with the classification of the RFQ.

3.1.6 Offerors are advised that the Purchaser reserves the right to incorporate the Offeror's Technical Proposal in whole or in part in the resulting Contract.

3.2 QUOTATION CONTENT

3.2.1 The complete Quotation shall consist of three distinct and separated parts each of which shall be delivered as an individual electronic submission as described in the following subparagraphs. Detailed requirements for the structure and content of each of these packages are contained in these RFQ Instructions.

3.2.2 All e-mails submitted shall be less than 20MB (per each e-mail) and shall not be password-protected.

Part	Format and Quantity Details
I: Quotation Administration Package	1 .zip File Submitted by Email not larger than 20MB total , which includes: • 1 Scanned PDF copies of the certificates with physical (non-digital) signatures of the prescribed certifications ✓ All of the required contents are outlined in Section III, Paragraph 3.3
II: Price Proposal	1 .zip File Submitted by Email not larger than 20MB total, which includes: • 1 Excel file, using the Pricing Sheets template provided with the RFQ • 1 PDF file of the Pricing Sheets "Offer Summary" tab ✓ All of the required contents are outlined in Section III, Paragraph 3.4
III: Technical Proposal	1 .zip File Submitted by Email not larger than 20MB total, which includes: • One file which addresses each evaluation criterion as described in Sections 3.2.5, 3.5, 4.4 and in accordance with the requirements of Section 3.5.2 ✓ If necessary, the technical volume may be separated into more than one email. Maximum email size per each email is 20MB. ✓ All of the required contents are outlined in Section III, Paragraph 3.5

3.2.3 The quotation volumes shall be sent via separate e-mails to the Quotation Delivery e-mail address as specified in Paragraph 2.3.2 and in accordance with Paragraph 3.2.2 above.

3.2.4 No information disclosing or contributing to disclose the quotation price shall be made part of the Technical Proposal. Failure to abide to this prescription shall result in the quotation being declared non-compliant.

3.2.5 As part of the Technical Proposal, the Offeror shall provide One (1) unpriced copy of the Pricing Sheets detailing the breakdown of labour, hours and equipment.

3.2.6 Documents submitted in accordance with paragraph 3.2.1 above shall be classified no higher than “NATO UNCLASSIFIED” material.

3.2.7 Partial Quotations on a Schedule and/or Quotations containing conditional statements will be declared non-compliant.

3.2.8 Where no specific format is mandated, electronic quotation documentation shall be delivered in PDF format without limitations of printing or “copy & paste”. The Purchaser reserves the right to request native formats electronic files of the proposal to facilitate the evaluation process.

3.3 PREPARATION OF THE ADMINISTRATIVE PACKAGE (VOLUME I)

3.3.1 Contents: Required documents submitted by email, containing one PDF file comprised of all of the required documents.

3.3.2 No information disclosing or contributing to disclose the quotation price shall be made part of the Administration Volume. Failure to abide to this prescription shall result in the quotation being declared non-compliant.

3.3.3 Volume I shall include the certificates set forth in Annex B to these RFQ Instructions, signed in the original by an authorised representative of the Offeror. The text of the certificates must not be altered in any way. The certificates are as follows:

B-1: Certificate of Legal Name of Offeror

B-2: Certificate of Independent Determination

B-3: Certificate of Quotation Validity

B-4: Certificate of Understanding

B-5: Certificate of Exclusion of Taxes, Duties and Charges

B-6: Acknowledgement of Receipt of RFQ Amendments (if applicable)

B-7: Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements

B-8: Certification of NATO Member Country of Origin of Delivered Equipment, Services, Materials and Intellectual Property Rights

B-9: Comprehension and Acceptance of Contract General and Special Provisions

B-10: List of Prospective Sub-Contractors / Consortium members

B-11: AQAP 2110 Compliance or ISO-9001:2015 Certification. The Offeror shall attach a copy of the company's AQAP 2110 compliance or ISO 9001:2015 certification.

B-12: List of Key Personnel

B-13: Disclosure of Involvement of Former NCI Agency Employment

B-14: Offeror Background IPR

B-15: List of Subcontractor IPR

B-16: Vendor Supply Chain Security Self-Attestation Statement

B-17: Compliance with Safeguarding NATO Information Controls

3.3.3.1 **Certificate B-7**, Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements, Offerors shall note especially the following:

3.3.3.1.1 If supplemental agreements, such as End-User Certificates or Technical Assistance Agreements, are required by national regulations, a draft version of these must be submitted with the Offeror's quote. Supplemental agreements submitted after the RFQ Closing Date shall not be considered.

3.3.3.1.2 The terms of supplemental agreements, if necessary, are the Offerors / Contractors responsibility and shall be totally consistent with the terms of the (Prospective) Contract, and shall not duplicate, negate, or further interpret any provisions of this Contract. The terms of the (Prospective) Contract shall take precedence over the Supplemental Agreement.

3.3.3.1.3 A problem with the supplemental agreement in any of the areas mentioned previously in this provision may result in a determination that the Quotation is not compliant with the terms of the RFQ, and in rejection of the Quotation, or termination for default of the Contract if the supplemental agreement is submitted after Contract award.

3.3.3.2 **Certificate B-10,** the Contractor shall identify by name, project role, and country of origin, all sub-contractors whose sub-contract value is expected to equal or exceed EUR 125,000, if any. A list of consortium members shall also be completed and included. If there are no sub-contractors/consortium members involved, the Offeror shall state this separately. The subcontractors listed in this certificate shall be traceable in the Pricing Sheets.

3.3.3.3 **Certificate B-11** Offerors shall provide documentary evidence that the Offeror possesses and maintains a current certification that is compliant with the requirements of Allied Quality Assurance Publication (AQAP) 2110, ISO 9001:2015, or an equivalent QA/QC regime.

3.3.3.3.1 If the Offeror is presenting a QA/QC regime that is claimed to be equivalent to AQAP 2110 or ISO 9001:2015, the burden of proof of such equivalency

shall be on the Offeror and such evidence of equivalency shall be submitted with the Certificate at Annex B-11 in the Administration Package.

3.3.3.3.2 Failure to execute this Certificate, or failure to provide documentary evidence of compliance with this requirement may result in a determination of a non-compliant quotation.

3.3.3.3.3 The Offeror will be required to maintain a valid certification throughout the duration of the contract.

3.3.3.3.4 If the Offeror provides a certification that is scheduled to expire during the solicitation phase or during the contract performance period, the Offeror will be required to provide evidence that a renewal process has begun and that a renewed certification will be obtained.

3.3.3.4 **Certificate B-16**, Offerors are required to read the CONSULTATION, COMMAND AND CONTROL BOARD (C3B) Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products. Offerors can request a copy of mentioned Directive through the email listed in Section II, Paragraph 2.5.2.1.

3.3.4 The Offeror shall send Volume I - Administrative Package via email to the Purchaser's email address specified in Section II, Paragraph 2.3.2 above. This shall consist of One (1) .zip file containing the Administrative Package.

3.3.4.1 The email shall be entitled: "RFQ-CO-115518-NPKI-M - Official Quote for [company name] – Volume I - Administrative Package" where the Administration Package .zip file shall be contained.

3.4 PREPARATION OF THE PRICE QUOTATION (VOLUME II)

3.4.1 Offerors shall prepare their Price Quotation by submitting one (1) email containing the completed Pricing Sheets provided with this RFQ under Book I - RFQ Instructions Annex C in both Excel and PDF formats. Offerors shall propose an accurate and complete Price Quotation in completing the Schedule of Supplies and Services (SSS) as defined in these RFQ Instructions in both Excel and PDF formats.

3.4.2 The prices provided shall reflect the comprehensive total price offered for the fulfilment of all requirements as expressed in the RFQ documentation.

3.4.3 Offerors shall furnish Firm Fixed Prices for all required items in accordance with the format set forth in these Instructions, as well as the Instructions contained within the Pricing Sheets itself.

3.4.4 Offerors are responsible for the accuracy of their Price Quotations. Price Quotations that have apparent computational errors may have such errors resolved in the Purchaser's favour or, in the case of gross omissions, inconsistencies or errors, may be cause for a determination of non-compliance by the Purchaser.

3.4.5 Offerors shall quote in their own national currency or in EUR, the host nation currency. Offerors may also submit Quotations in multiple currencies including other NATO member states' currencies under the following conditions:

3.4.5.1 The currency is of a "Participating Country" in the project, and

3.4.5.2 The Offeror can demonstrate, either through sub-contract arrangements or in its proposed work methodology, that it will have equivalent expenses in that

currency. In such case, all major sub-contracts and their approximate anticipated value shall be listed on a separate sheet and included with the Price Quotation.

3.4.6 The Purchaser, by virtue of its status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct taxes (incl. VAT) and all customs duties on merchandise imported or exported. The Offeror, therefore, shall certify that the prices stipulated in its Quotation do not include amounts to cover such direct taxes or customs duties.

3.4.7 The Offeror shall be responsible for ensuring that its prospective Sub-contractors are aware that the Purchaser is exempt from taxes and customs duties. The Offeror (and its prospective Sub-contractors) shall be responsible for complying with all applicable national and local legal and administrative procedures to ensure that authorities do not attempt to assess taxes and customs duties on goods and property imported or exported through NATO member nation frontiers under the prospective Contract nor assess direct taxation (VAT) on goods sold to the Purchaser under the prospective Contract. Offerors are reminded of the requirement to complete the certification to this effect in Annex B-5.

3.4.8 All prices quoted in the proposal shall be DDP (Delivered Duty Paid) to specified destination, in accordance with the International Chamber of Commerce INCOTERMS 2020 and shall also cover all packaging, packing, preservation, insurance and transportation charges. Prices quoted shall include all costs for items supplied and delivered to final destination.

3.4.9 Except as provided in paragraph 3.4.5 (b) above, Price Quotations shall contain no document and/or information other than the completed Pricing Sheets and SSS. Any other document of a contractual or technical nature will not be considered for evaluation and may be cause for a determination of non-compliance by the Purchaser.

3.4.10 When completing the Pricing Sheets, a unit price and total fixed price for each specified element needs to be supplied on each CLIN line item. Offerors are required to insert price information in all cells marked in yellow and to complete all required tabs contained in the Pricing Sheets. Prices should not be grouped. The prices and quantities entered on the document shall reflect the total items required to meet the contractual requirements. The total price shall be indicated in the appropriate columns and in the currency quoted. If the price of a line item is expressed in different currencies, these shall be identified, and there shall be as many totals on that line item as there are currencies. In preparing the Price Quotation, Offerors shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part. The accuracy of the inputs of the Pricing Sheets is the responsibility of the Offeror. The Purchaser in its favour may resolve ambiguous computation of prices.

3.4.11 The Offeror shall furnish Firm Fixed Price quotations, for all proposed items. Partial Quotations shall be rejected.

3.4.12 The Offeror shall be liable for all other taxes, assessments, fees, licences, administrative charges or other Government assessments or charges which are applicable to the performance of the prospective Contract. It is the Offeror's responsibility to inform itself of its liability in each country where such liability may arise.

3.4.13 Price Proposals exceeding the deadlines for delivery and completion of works indicated in the Schedule of Supplies and Services may be declared non-compliant.

3.4.14 The Offeror shall identify for each CLIN all significant sub-contractors and provide required information about their prospective sub-contractors whose estimated value of the subcontract is expected to equal or exceed EUR 125,000 using the "List of Prospective Sub-Contractors" form attached to Book I Annex B-10.

3.4.15 The Offeror shall separately price the cost of Warranty. Zero values or the statement that the Quotation price includes the cost of warranty shall not be allowed.

3.4.16 The Offeror shall send Package II - Pricing Package via email to the Purchaser's email address specified in Section II, Paragraph 2.3.2 above. This shall consist of One (1) zip file containing the Pricing Package.

3.4.16.1 The email provided shall be entitled: "RFQ-CO-115518-NPKI-M Official Quote for [company name] - Part II - Price Quotation" where the Pricing Package .zip file shall be contained.

3.5 PREPARATION OF THE TECHNICAL PROPOSAL (VOLUME III)

3.5.1 The Technical Proposal package shall include the following:

3.5.1.1 Table of Contents. The Offeror shall compile a detailed Table of Contents which lists not only section headings but also major sub-sections, and topic headings required set forth in these Instructions or implicit in the organisation of the Technical Proposal.

3.5.1.2 Cross-Reference/Compliance Table. The Offeror shall include the completed Technical Proposal Cross-Reference Table at Annex D of Book I. The Offeror shall complete the Column marked "QUOTATION REFERENCE" of the Table, citing the appropriate section of the Technical Proposal that corresponds to each paragraph of these Instructions for the Preparation of the Technical Proposal. The completed table serves as an index for the Purchaser's Technical Evaluation Panel and also as an aide memoire to the Offeror to ensure that all the required information has been provided in the Technical Proposal.

3.5.1.3 Corporate Experience: At not more than two (2) pages in length, the Offeror shall provide at least one (1) executive summary describing the successful delivery a project including a Data Centre installation during the last five (5) years. For each project, the Contractor shall describe:

3.5.1.3.1 The domain or area (ideally the customer name), the size (contract value range), duration and challenges encountered with remediation;

3.5.1.3.2 The scope of work, demonstrating the Offeror's capability to successfully implement Data Centre Installation and meeting requirements of a comparable or greater complexity to those defined in Book II Part IV SOW Annex A.

3.5.1.4 Project Implementation Plan (PIP): At not less than thirty (30) pages in length, the Offeror shall submit a preliminary Project Implementation Plan in accordance with the requirements of the Statement of Work (Book II Part IV SOW Section 3.2) for the NATO Public-Key Infrastructure Capability (NPKI) WP 2 - Data Centre Installation, which clearly describes how the Offeror intends to implement the totality of the project in compliance with the contractual requirements.

3.5.1.4.1 The PIP shall comprise of all project implementation aspects, which include management provisions, facilities, schedules, personnel assignments, external relationships and project control.

3.5.1.4.2 The PIP shall include sections on Project Overview and Applicable Documents, as well as the following sections:

3.5.1.4.3 Project Management Plan (PMP): At not more than ten (10) pages in length, the Offeror shall submit a preliminary Project Management Plan in accordance with the requirements of the Statement of Work (Book II Part IV SOW Section 3.3) for the NATO Public-Key Infrastructure Capability (NPKI) WP 2 - Data Centre Installation.

3.5.1.4.3.1 The PMP shall include a Project Breakdown Structure (PBS) that shall contain the critical work elements (tasks) of the project and illustrate their relationship to each other and to the project as a whole.

3.5.1.4.3.2 The PMP shall include a Project Master Schedule (PMS): The Offeror shall submit a preliminary Project Master Schedule that shall contain all contract events and milestones for the Project. As described in the SOW Section 4.1, the PMS shall show all contractual deliverables, their delivery dates, and the tasks associated with them, including the Purchaser's review stages. The PMS shall for each task identify the start and finish dates, duration, predecessors, constraints, and resources. The PMS shall provide network, milestone, and Gantt views, and identify the critical path for the overall project. Any PMS which does not align with the dates provided in the SSS may be determined to be non-compliant.

3.5.1.4.4 System Design, Integration and Implementation: At not less than ten (10) pages in length, the Offeror shall describe how the NATO Public-Key Infrastructure Capability (NPKI) WP2 - Data Centre Installation will be implemented with sufficient technical detail for the Purchaser to determine compliance with the SOW. For this purpose the Offeror shall demonstrate compliance with the Requirements as specified under SOW Sections 4.4 and 4.5, and indicate how the components and quantities of equipment and licenses are to be deployed.

3.5.1.4.5 Integrated Product Support (IPS): At not less than ten (10) pages the Offeror shall describe the Integrated Product Support (IPS) aspects of the Quotation. This description shall address, with an adequate level of detail, the following: Offeror's IPS Organisation, Roles, Responsibilities and Procedures; Maintenance Concept; Logistic Support Analysis (LSA) & Reliability, Maintainability, Availability, Testability (RAMT); Technical Documentation and Data, Supply Support, Support and Test Equipment Lists; Training, including Manpower and Personnel Requirements; Planning and execution of Handling and Storage; Warranty; and Planning of Supply Chain Security as set forth in the SOW Section 5 and in accordance with the applicable Standards and Specifications required in SOW Section 2. The description shall provide sufficient evidence to confirm that the Offeror will be able to meet the timelines in accordance with the requirements of the Schedule of Supplies and Services and the SOW.

3.5.1.4.6 Testing and Acceptance: At not more than ten (10) pages in length, the Offeror shall describe how it can meet the NPKI WP 2 testing requirements

and its methodology for conducting all related activities as detailed in SOW Section 6. This includes the development of all test documentation required under the prospective Contract, the conduct of all testing, the evaluation and documentation of the tests results by an Independent Verification and Validation (IV&V) as specified in SOW Section 6.

3.5.1.4.7 Quality Assurance (QA): At not less than three (3) pages and not more than ten (10) pages in length, the Offeror shall describe how it can meet the Quality Assurance and Quality Control aspects of the Project, as specified in SOW Section 7. The Offeror shall submit a preliminary QA Plan (QAP), with details of how the Offeror shall establish, execute, document and maintain an effective Quality Assurance (QA) programme, throughout the Contract lifetime.

3.5.1.4.8 Configuration Management: At not less than three (3) pages and not more than ten (10) pages in length, the Offeror shall describe how it can meet the Configuration Management requirements as specified in SOW Section 8. In conformance with the required Standards and Specifications required in SOW Sections 2 and 8, this shall include a description of the unique Configuration Management framework, Baselines, the Product Lifecycle Management (PLM) tool, and the Configuration Management Database (CMDB).

3.5.1.5 Key Personnel CVs: At not more than two (2) pages in length for each Key Personnel team member, the Offeror shall provide curriculum vitae (CV) of the proposed Project Manager, Technical Lead, Subject Matter Experts (Test Director, Integrated Product Support Manager, Security Accreditation Manager) and Quality Assurance Representative (QAR).

3.5.1.5.1 For the Project Manager, the Offeror shall provide details about qualifications, evidence of six (6) years' experience as the Project Manager for an effort of similar scope, duration, complexity and cost, including the application of a formal project management methodology such as PRINCE2 as defined in SOW Section 3.1.3.

3.5.1.5.2 For the Technical Team and the Subject Matter Experts, the Offeror shall provide details about qualifications and evidence that the proposed team possesses the necessary knowledge, capability and experience required in SOW Sections 3.1.4, 3.1.5, 3.1.7, 3.1.8, 3.1.9, and in particular demonstrate that the team meets each of the requirements described in [SOW 20] a. through p.

3.5.1.5.3 For the Quality Assurance Representative (QAR), the Offeror shall provide details about the qualifications, evidence of four (4) years' experience in working with quality control methods and tools and have a broad knowledge of NATO Standards (e.g. STANAG 4107 Ed. 11), processes and procedures applicable to Quality Assurance (QA) and Quality Control (QC) in the industry, as defined in SOW Section 3.1.6

3.5.2 The Offeror shall send Volume III – Technical Package via email to the Purchaser's email address specified in Section II, Paragraph 2.3.2 above. This shall consist of One (1) .zip file containing the Technical Package and One (1) unpriced copy of the

Pricing Sheets as per Section III, Paragraph 3.2.3 above. Maximum email size is 20MB.

3.5.2.1 The email provided shall be entitled: “RFQ-CO-115518-NPKI-M - Official Quote for [company name] - Part III - Technical Proposal” where the Technical Package .zip file shall be contained.

3.5.2.2 If necessary, e.g. where the Technical Package exceeds the maximum e-mail size of 20MB, the Technical Package may be separated into more than one email. In such case, Offerors shall clearly indicate the correct order in the e-mail subject line (e.g. “…Technical Proposal, Part 1 of 2, …”) . Maximum email size per each email is 20MB.

SECTION IV - QUOTATION EVALUATION

4.1 GENERAL

4.1.1 The evaluation of Quotations will be made by the Purchaser solely on the basis of the requirements in this RFQ.

4.1.2 The evaluation of Quotations and the determination as to the compliance or technical adequacy of the supplies and services offered will be based only on that information furnished by the Offeror and contained in its Quotation. The Purchaser shall not be responsible for locating or securing any information which is not included in the Quotation.

4.1.3 To ensure that sufficient information is available, the Offeror shall furnish with its Quotation all information appropriate to provide a complete description of the work which will be performed and/or the supplies to be delivered. The information provided shall be to a level of detail necessary for the Purchaser to determine exactly what the Offeror proposes to furnish and whether the offer meets the technical, administrative and contractual requirements of this RFQ. Significant omissions and/or cursory submissions may result in a determination of non-compliance without recourse to further clarification.

4.1.4 During the evaluation, the Purchaser may request clarification of the Quotation from the Offeror, and the Offeror shall provide sufficient detailed information in connection with such requests as to permit the Purchaser to make a final determination based upon the facts. The purpose of such clarifications will be to resolve ambiguities in the Quotation and to permit the Offeror to state its intentions regarding certain statements contained therein. The Offeror is not permitted any cardinal alteration of the Quotation regarding technical matters and shall not make any change to its price quotation at any time nor restate the Statement of Work (SOW).

4.1.5 The Offeror's prompt response to the Purchaser's RFQ clarification requests is important and therefore failure to provide the requested clarifications within the time-limits set forth in the specific Clarification Requests may cause the Quotation to be deemed non-compliant.

4.1.6 The evaluation will be conducted in accordance with the Use of Basic Ordering Agreements (BOAs) by the NATO Communications and Information Agency (NCI Agency) set forth in the NATO document AC/4-D(2019)0004 (INV).

4.1.7 The administrative compliance of the Quotations will be evaluated first. Quotations that are declared administratively non-compliant may be rejected without further evaluation. Following evaluation for administrative compliance, evaluation will be carried out in the following two areas: Volume II - Price, Volume III- Technical. Should areas of Administrative non-compliance be identified in the Pricing or Technical evaluation this shall be treated in accordance with Section IV, Paragraph 4.2 below.

4.1.8 All administrative compliant Quotations will be reviewed for price compliancy and the identified lowest offer will be reviewed for technical compliance. Any Contract resulting from this RFQ will be awarded to the Offeror whose offer, as evaluated by the Purchaser, is the lowest priced, technically compliant quotation and in compliance with the requirements of this RFQ.

4.2 ADMINISTRATIVE CRITERIA

4.2.1 Prior to commencement of the Price and Technical evaluation, Quotations will be reviewed for compliance with the Quotation Submission Requirements of this RFQ. These are as follows:

4.2.1.1 RFQ Closing Date and Time

4.2.1.1.1 The Quotation was received by the RFQ Closing Date and Time.

4.2.1.2 Delivery and marking of the Quotation

4.2.1.2.1 The Quotation consists of three distinct and separated parts each of which has been delivered as an individual electronic submission as described in Section III, Paragraph 3.2.2 of the Book I – RFQ Instructions;

4.2.1.2.2 The Quotation submission e-mails were marked properly in accordance with Section III, Paragraphs 3.3.4.1, 3.4.17.1 and 3.5.2.1 of the Book I – RFQ Instructions;

4.2.1.2.3 The Quotation and all related documentation is classified no higher than "NATO UNCLASSIFIED" material;

4.2.1.2.4 No information disclosing or contributing to disclose the quotation price has been made part of the Administration Volume.

4.2.1.3 Language

4.2.1.3.1 The Quotation and all related documentation has been provided in the English language.

4.2.1.4 Certificates

4.2.1.4.1 The Administrative Package contains all the certificates B-1 thru B-17 set forth in Annex B to the Book I – RFQ Instructions, signed in the original by an authorised representative of the Offeror;

4.2.1.4.2 The text of the certificates set forth in Annex B to the Book I – RFQ Instructions has not been altered in any way.

4.2.2 A Quotation that fails to conform to the above requirements may be declared non-compliant and may not be evaluated further by the Purchaser.

4.2.3 If it is discovered, during either the Price or Technical evaluation, that the Offeror has taken exception to the Terms and Conditions of the Prospective Contract, or has qualified and/or otherwise conditioned its Quotation on a modification or alteration of the Terms and Conditions or the language of the Statement of Work, the Offeror may be determined to have submitted a non-compliant Quotation.

4.3 PRICE CRITERIA

4.3.1 The Offeror's Price Quotation will be first assessed for compliance against the following standards:

4.3.1.1 The Price Quotation meets the requirements for preparation and submission of the Price Quotation set forth in the Price Quotation Preparation Section III, Paragraph 3.4 of the Book I – RFQ Instructions and the Instructions contained in the Pricing Sheets (Annex C to the Book I – RFQ Instructions) in particular.

4.3.1.2 Adequacy, accuracy, traceability and completeness of detailed pricing information:

4.3.1.2.1 The Offeror has furnished Firm Fixed Prices for all items listed. Not having provided a price for all items as required per the Pricing Sheets, i.e. to fill out **all** yellow fields and/or complete all required tabs contained in the Pricing Sheets, may render the Quotation non-compliant. Prices cannot be embedded/included in other prices.

4.3.1.2.2 All pricing data, i.e., quantities, unit prices, has been provided as reflected in the Pricing Sheets.

4.3.1.2.3 Quotation prices include all costs for items supplied, delivered, and supported.

4.3.1.2.4 All prices have been accurately entered into appropriate columns and accurately totalled.

4.3.1.2.5 The Offeror has provided accurate unit prices (where required) and a total price for each line item.

4.3.1.2.6 The Offeror has provided accurate unit prices and a total price of each of the sub-items it added (if any).

4.3.1.2.7 The currency of all line items has been clearly indicated.

4.3.1.2.8 The Offeror has quoted in its own national currency or in the Host Nation currency, Euros. Where multiple currencies including other NATO member states' currencies are quoted, the conditions of Section III, Paragraph 3.4.5 of the Book I – RFQ Instructions shall be met.

4.3.1.2.9 The Offeror has indicated that in accordance with the treaties governing the terms of business with NATO, it excluded from its prices all taxes, duties and customs charges from which the Purchaser has been exempted.

4.3.1.2.10 Price quotes for each individual item(s), and totalled prices are accurate and realistic (based on historic data, and/or market and competitive trends in the specified industrial sector(s)).

4.3.1.2.11 Detailed pricing information has been provided and is adequate, accurate, traceable, and complete.

4.3.1.2.12 The Price Quotation meets requirements for price realism as described in Section IV, Paragraph 4.3.5 of the Book I – RFQ Instructions.

4.3.2 A Quotation which fails to meet the compliance standards defined in this section may be declared non-compliant and may not be evaluated further by the Purchaser.

4.3.3 Basis of Price Comparison to determine lowest compliant Quotation

4.3.3.1 The Purchaser will convert all prices quoted into EURO for purposes of comparison and computation of price scores. The exchange rate to be utilised by the Purchaser will be the average of the official buying and selling rates of the European Central Bank at close of business on the last working day preceding the RFQ Closing Date.

4.3.3.2 The price comparison will be based on the Offered Grand Total Firm Fixed Price which includes all **CLINs** in the Pricing Sheets.

4.3.4 **Inconsistencies and discrepancies in Quotation price quotation**. In case of inconsistencies, discrepancies and/or contradictory pricing information in the different parts of the Quotation price submission and notwithstanding the possibility for the Purchaser, at its sole discretion to obtain clarification from the Offeror, for the purpose of determining the total price of the Quotation, the following order of precedence shall apply:

4.3.4.1 PDF copy of the completed Pricing Sheets

4.3.4.1.1 Schedule of Supplies and Services Total to be Evaluated Quotation Price as indicated by the Offeror

4.3.4.1.2 Total of the Quotation calculated from the indicated Total Prices(s) indicated per CLIN(s)

4.3.4.2 Microsoft Excel copy of the completed Pricing Sheets

4.3.4.2.1 Schedule of Supplies and Services Total to be Evaluated Quotation Price as indicated by the Offeror

4.3.4.2.2 Total of the Quotation calculated from the indicated Total Prices(s) indicated per CLIN(s)

4.3.5 Price Realism

4.3.5.1 Should an Offeror submit a price quotation so low that it is not a realistic reflection of the objective cost of performance of the associated technical proposal, this may be considered by the Purchaser to be an unrealistic offer and may be determined to be non-compliant.

4.3.5.2 Indicators of an unrealistically low Quotation may include, but are not limited to, the following:

4.3.5.2.1 Labour Costs that, when amortised over the expected or proposed direct labour hours, indicate average labour rates far below those prevailing in the Offeror locality for the types of labour proposed.

4.3.5.2.2 Direct Material costs that are considered to be too low for the amounts and types of material proposed, based on prevailing market prices for such material.

4.3.5.2.3 Numerous Line Item prices for supplies and services that are provided at no cost or at nominal prices.

4.3.5.3 If the Purchaser has reason to suspect that a Offeror has artificially debased its prices in order to secure contract award, the Purchaser will request clarification of

the Quotation in this regard and the Offeror shall provide explanation on one of the following basis:

4.3.5.3.1 An error was made in the preparation of the Price Quotation. In such a case, the Offeror must document the nature of the error and show background documentation concerning the preparation of the Price Quotation that makes a convincing case that a mistake was made by the Offeror. In such a case, the Offeror shall petition the Purchaser to both remain in the competition and accept the Contract at the offered price, or to withdraw from the competition.

4.3.5.3.2 The Offeror has a competitive advantage due to prior experience or industrial/technological processes that demonstrably reduce the costs of Offeror performance and therefore the price offered is realistic. Such an argument must support the technical proposal offered and convincingly and objectively describe the competitive advantage and the net savings achieved by this advantage over standard market practices and technology.

4.3.5.3.3 The Offeror recognises that the submitted Price Quotation is unrealistically low compared to its cost of performance and, for business reasons, the Offeror is willing to absorb such a loss. Such a statement can only be made by the head of the business unit submitting the Quotation and will normally be made at the level of Chief Operating Officer or Chief Executive Officer. In such a case, the Offeror shall estimate the potential loss and show that the financial resources of the Offeror are adequate to withstand such reduction in revenue.

4.3.5.4 If an Offeror fails to submit a comprehensive and compelling response on one of the basis above, the Purchaser may determine the Quotation submitted as non-compliant. If the Offeror responds on the basis of the above and requests to withdraw from the competition, the Purchaser may, depending on the nature and gravity of the mistake, allow the Offeror to withdraw.

4.3.5.5 If the Purchaser accepts the Offeror's explanation of mistake in Section IV, Paragraph 4.3.5.3.1 and allows the Offeror to accept the Contract at the offered price, or the Purchaser accepts the Offeror's explanation pursuant to Section IV, Paragraph 4.3.5.3.3 above, the Offeror shall agree that the supporting pricing data submitted with its Quotation will be incorporated by reference in the resultant Contract. The Offeror shall agree as a condition of Contract signature, that the pricing data will be the basis of determining fair and reasonable pricing for all subsequent negotiations for modifications of or additions to the Contract and that no revisions of proposed prices will be made.

4.3.5.6 If the Offeror presents a convincing rationale pursuant to Section IV, Paragraph 4.3.5.3.2 above, no additional action will be warranted. The Purchaser, however, reserves its right to reject such an argument if the rationale is not compelling or capable of objective analysis. In such a case the Quotation may be determined to be non-compliant.

4.4 TECHNICAL CRITERIA

4.4.1 Upon determination of the lowest-priced Quotation as described above, the Quotation shall be evaluated to confirm compliance with the following technical criteria associated with the respective sections of the Technical Proposal.

4.4.2 Table of Contents

4.4.2.1 **Aim** – The purpose of this criterion is to ensure the Offeror has provided a Technical Proposal addressing each element of Section III, Paragraph 3.5.1.1 (Table of Contents) of the Book I – RFQ Instructions.

4.4.2.2 **Criterion** – The Offeror shall ensure that its Technical Proposal includes and addresses each element of Section III, Paragraph 3.5.1.1 (Table of Contents) of the Book I – RFQ Instructions.

4.4.2.3 Document References

4.4.2.3.1 RFQ Instructions. Section III, Paragraph 3.5.1.1

4.4.2.4 Pass/Fail Criteria

4.4.2.4.1 Pass – The Offeror has included a Table of Contents addressing each element from Section III, Paragraph 3.5.1.1 of the Book I – RFQ Instructions in its Technical Proposal.

4.4.2.4.2 Fail – The Offeror has not included a Table of Contents addressing each element from Section III, Paragraph 3.5.1.1 of the Book I – RFQ Instructions in its Technical Proposal.

4.4.3 Cross Reference Compliance Table

4.4.3.1 **Aim** – The purpose of this criterion is to ensure the Offeror has provided a Technical Proposal addressing each element of Section III, Paragraph 3.5.1.2 (Cross Reference/Compliance Table) of the Book I – RFQ Instructions.

4.4.3.2 **Criterion** – The Offeror shall ensure that its Technical Proposal includes and addresses each element of Section III, Paragraph 3.5.1.2 (Cross Reference/Compliance Table) of the Book I – RFQ Instructions.

4.4.3.3 Document References

4.4.3.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.2

4.4.3.3.2 RFQ Instructions ANNEX D – COMPLIANCE TABLE

4.4.3.4 Pass/Fail Criteria

4.4.3.4.1 Pass – The Offeror has included a Cross Reference/Compliance Table addressing each element from Section III, Paragraph 3.5.1.2 of the Book I – RFQ Instructions in its Technical Proposal.

4.4.3.4.2 Fail – The Offeror has not included a Cross Reference/Compliance Table addressing each element from Section III, Paragraph 3.5.1.2 of the Book I – RFQ Instructions in its Technical Proposal.

4.4.4 Corporate Experience

4.4.4.1 **Aim** – The purpose of this criterion is to provide confidence to the Purchaser that the Offeror has the necessary corporate experience of successfully delivering

projects including a Data Centre installation meeting requirements of a comparable or greater complexity to those in the Statement of Work (SOW).

4.4.4.2 **Criterion** – At not more than two (2) pages in length, the Offeror shall detail its corporate experience of successfully delivering a project including a Data Centre installation, meeting requirements of a comparable or greater complexity to those in the Statement of Work (SOW) in the last five (5) years.

4.4.4.3 **Document References**

4.4.4.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.3 (including 3.5.1.3.1, 3.5.1.3.2).

4.4.4.4 Pass/Fail Criteria

4.4.4.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.3 (including 3.5.1.3.1, 3.5.1.3.2) of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal contains at least one (1) example of successfully delivering a project including a Data Centre installation, meeting requirements of a comparable or greater complexity to those in the Statement of Work (SOW) in the last five (5) years.

4.4.4.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.3 (including 3.5.1.3.1, 3.5.1.3.2) of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not demonstrate any previous experience in delivering a project including a Data Centre installation, meeting requirements of a comparable or greater complexity to those in the Statement of Work (SOW) in the last five (5) years.

4.4.5 <u>Project Implementation Plan (PIP)</u>

4.4.5.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to implement the project and perform contract administration, including details of the controls that shall be applied to manage Sub-Contractor performance and deliverables as detailed in the Statement of Work (SOW) Section 3.2.

4.4.5.2 **Criterion** – At not less than thirty (30) pages in length, the Offeror shall detail the Project Implementation Plan (PIP), which shall include management provisions, facilities, schedules, personnel assignments, external relationships and project control. The PIP shall be in sufficient detail to allow the Purchaser to assess the Contractor's plans and approach in implementing the entire project in conformance with the specified requirements. The PIP shall include as a minimum the following sections:

4.4.5.2.1 Project Overview

4.4.5.2.2 Applicable Documents

4.4.5.2.3 Project Management Plan

4.4.5.2.4 System Design and Implementation

4.4.5.2.5 Integrated Product Support

4.4.5.2.6 Quality Assurance and Quality Control

4.4.5.2.7 Configuration Management

4.4.5.2.8 Testing and Acceptance

4.4.5.2.9 Documentation

4.4.5.3 Document References

4.4.5.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.4 (including 3.5.1.4.1, 3.5.1.4.2)

4.4.5.4 Pass/Fail Criteria

4.4.5.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.4 (including 3.5.1.4.1, 3.5.1.4.2) of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has provided a preliminary Project Implementation Plan in accordance with the requirements of the Statement of Work Section 3.2, which clearly describes how the Offeror intends to implement the totality of the project in compliance with the contractual requirements.

4.4.5.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.4 (including 3.5.1.4.1, 3.5.1.4.2) of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not answered the question or the Offeror has not met the requirements.

4.4.5.5 <u>Project Management Plan (PMP)</u>

4.4.5.5.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the Project Management requirements of the Project Management Plan (PMP) detailed in the Statement of Work (SOW) Section 4.2.

4.4.5.5.2 **Criterion** – At not more than ten (10) pages in length, the Offeror shall detail the Project Management Plan (PMP), meeting the requirements specified in the Statement of Work (SOW) Section 3.3.

4.4.5.5.3 Document References

4.4.5.5.4 RFQ Instructions, Section III, Paragraph 3.5.1.4.3 (including 3.5.1.4.3.1)

4.4.5.5.5 SOW Section 3.3

4.4.5.5.6 Pass/Fail Criteria

4.4.5.5.6.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.4 (including 3.5.1.4.3.1) of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has provided a preliminary Project Management Plan in accordance with the requirements of the Statement of Work Section 3.3, which clearly describes how the Offeror intends to implement the totality of the project in compliance with the contractual requirements.

4.4.5.5.6.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.4 (including 3.5.1.4.3.1,) of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not answered the question or the Offeror has not met the requirements specified in the SOW Section 3.3.

4.4.5.6 <u>Project Master Schedule (PMS)</u>

4.4.5.6.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the PMS requirements detailed in the Statement of Work (SOW) Section 3.4 by the dates provided in the Schedule of Supplies and Services (SSS).

4.4.5.6.2 **Criterion** – The Offeror shall provide a PMS containing a preliminary Schedule and explain how the requirements and deadlines specified in the Statement of Work (SOW) and the Schedule of Supplies and Services (SSS) shall be met.

4.4.5.6.3 Document References

4.4.5.6.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.4.3.2

4.4.5.6.3.2 SOW Section 3.4.

4.4.5.6.4 Pass/Fail Criteria

4.4.5.6.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.5 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal includes a PMS in accordance with SOW Section 3.4 which provides a preliminary Schedule clearly explaining how the requirements specified in the Statement of Work (SOW) shall be met and delivered by the Offeror by the dates provided in the Schedule of Supplies and Services (SSS).

4.4.5.6.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.5 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not include a preliminary PMS clearly explaining how the requirements specified in the Statement of Work (SOW) shall be met and delivered by the Offeror by the dates provided in the Schedule of Supplies and Services (SSS).

4.4.5.7 <u>System Design, Integration and Implementation</u>

4.4.5.7.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the System Design, Integration and Implementation requirements detailed in the Statement of Work (SOW) Sections 44 and 4.5.

4.4.5.7.2 **Criterion** – At not less than ten (10) pages in length, the Offeror shall describe how the NATO Public-Key Infrastructure Capability (NPKI) WP2 - Data Centre Installation will be implemented with sufficient technical detail for the Purchaser to determine compliance with the SOW Sections 4.4 and 4.5.

4.4.5.7.3 **Document References**

4.4.5.7.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.4.4.

4.4.5.7.3.2 SOW Sections 4.4 and 4.5

4.4.5.7.4 Pass/Fail Criteria

4.4.5.7.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.6 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal clearly explains how the requirements specified in the SOW Sections 4.10 and 4.11 shall be met by the Offeror. The Offeror's technical proposal clearly

demonstrates how the work shall be delivered; indicating how the components and quantities of equipment and licences are deployed in the Offeror's proposal and plans.

4.4.5.7.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.6 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not explain how the requirements specified in the SOW Sections 4.10 and 4.11 shall be met by the Offeror.

4.4.5.8 Integrated Product Support (IPS)

4.4.5.8.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the IPS requirements of the Project as detailed in the Statement of Work (SOW) Sections 2 and 5.

4.4.5.8.2 **Criterion** – At not less than ten (10) pages in length, the Offeror shall explain how the IPS requirements specified in the SOW Sections 2 and 5 shall be met.

4.4.5.8.3 Document References

4.4.5.8.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.4.5

4.4.5.8.3.2 SOW Sections 2 and 5

4.4.5.8.4 Pass/Fail Criteria

4.4.5.8.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.7 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal clearly explains how the IPS requirements specified in the SOW Sections 2 and 5 shall be met by the Offeror.

4.4.5.8.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.7 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not explain how the IPS requirements specified in the SOW Sections 2 and 5 shall be met by the Offeror.

4.4.5.9 Testing and Acceptance

4.4.5.9.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the Testing requirements detailed in the Statement of Work (SOW) Section 6.

4.4.5.9.2 **Criterion** – At not more than ten (10) pages in length, the Offeror shall explain how the Testing requirements specified in the SOW Section 6 shall be met.

4.4.5.9.3 Document References

4.4.5.9.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.6

4.4.5.9.3.2 SOW Section 6

4.4.5.9.4 Pass/Fail Criteria

4.4.5.9.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.8 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal clearly explains how the Testing requirements specified in the SOW Section 6 shall be met by the Offeror.

4.4.5.9.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.8 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not explain how the Testing requirements specified in the SOW Section 6 shall be met by the Offeror.

4.4.5.10 Quality Assurance (QA)

4.4.5.10.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the Quality Assurance (QA) requirements detailed in the Statement of Work (SOW) Section 7.

4.4.5.10.2 **Criterion** – At not less than three (3) pages and not more than ten (10) pages in length, the Offeror shall explain how the Quality Assurance requirements specified in the SOW Section 7 shall be met.

4.4.5.10.3 Document References

4.4.5.10.3.1
RFQ Instructions, Section III, Paragraph 7

4.4.5.10.3.2
SOW Section 7

4.4.5.10.4 Pass/Fail Criteria

4.4.5.10.4.1
Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.9 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal clearly explains how the Quality Assurance requirements specified in the SOW Section 7 shall be met by the Offeror.

4.4.5.10.4.2
Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.9 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not explain how the Quality Assurance requirements specified in the SOW Section 7 shall be met by the Offeror.

4.4.5.11 Configuration Management

4.4.5.11.1 **Aim** – The purpose of this criterion is for the Purchaser to understand the Offeror's approach to delivering the Configuration Management requirements detailed in the SOW Sections 2 and 8.

4.4.5.11.2 **Criterion** – At not less than three (3) pages and not more than ten (10) pages in length, the Offeror shall explain how the Configuration Management requirements specified in the SOW Sections 2 and 8 shall be met.

4.4.5.11.3 Document References

4.4.5.11.3.1
RFQ Instructions, Section III, Paragraph 3.5.1.4.8.

4.4.5.11.3.2
SOW Sections 2 and 8

4.4.5.11.4 Pass/Fail Criteria

4.4.5.11.4.1
Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.10 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal clearly explains how the Configuration Management requirements specified in the SOW Sections 2 and 8 shall be met by the Offeror.

4.4.5.11.4.2
Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.10 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not explain how the Configuration Management requirements specified in the SOW Sections 2 and 8 shall be met by the Offeror.

4.4.6 Key Personnel – Project Manager

4.4.6.1 **Aim** – The purpose of this criterion is to provide confidence to the Purchaser that the Offeror's Project Manager has the necessary experience required in SOW Section 3.1.3.

4.4.6.2 **Criterion** – At not more than two (2) pages in length, the Offeror shall provide a CV for its offered Project Manager detailing their individual experience in accordance with the requirements specified in the SOW Section 3.1.3.

4.4.6.3 Document Reference

4.4.6.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.5.1

4.4.6.3.2 SOW Section 3.1.3

4.4.6.4 Pass/Fail Criteria

4.4.6.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.11.1 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal contains a CV for the Project Manager which clearly explains how the requirements specified in the SOW Section 3.1.3 shall be met by the Offeror.

4.4.6.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.11.1 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not contain a CV for the Project Manager which clearly explains how the requirements specified in the SOW Section 3.1.3 shall be met by the Offeror.

4.4.7 Key Personnel - Technical Lead/ Subject Matter Experts

4.4.7.1 **Aim** – The purpose of this criterion is to provide confidence to the Purchaser that the Offeror's Technical Lead and Subject Matter Experts have the necessary experience required in SOW Sections 3.1.4, 3.1.5, 3.1.7, 3.1.8, 3.1.9,4.4, in

particular demonstrate that the team meets each of the requirements described in [SOW 20] a. through p.

4.4.7.2 **Criterion** – At not more than two (2) pages in length for each team member, the Offeror shall provide a CV for its offered Technical Team/ Subject Matter Experts detailing their individual experience in accordance with the requirements specified in the SOW Sections 3.1.4, 3.1.5, 3.1.7, 3.1.8, 3.1.9, 4.4, and in particular demonstrate that the team meets each of the requirements described in [SOW 20] a. through p.

4.4.7.3 Document Reference

4.4.7.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.5.21

4.4.7.3.2 SOW Sections 3.1.4, 3.1.5, 3.1.7, 3.1.8, 3.1.9, 4.4 and Annex A (SRS)

4.4.7.4 Pass/Fail Criteria

4.4.7.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.11.1 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal contains a CV for each member of the proposed Technical Team/ Subject Matter Experts which clearly explains how the requirements specified in the SOW Sections 3.1.4, 3.1.5, 3.1.7, 3.1.8, 3.1.9, 4.4, and in particular the requirements described in [SOW 20] a. through p., shall be met by the Offeror.

4.4.7.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.11.1 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not contain a CV for each member of the proposed Technical Team/ Subject Matter Experts which clearly explains how the requirements specified in the SOW Section 3.1.4, 3.1.5, 3.1.7, 3.1.8, 3.1.9, 4.4, and in particular the requirements described in [SOW 20] a. through p., shall be met by the Offeror.

4.4.8 <u>Key Personnel - Quality Assurance Representative (QAR)</u>

4.4.8.1 **Aim** – The purpose of this criterion is to provide confidence to the Purchaser that the Offeror's QAR has the necessary experience of delivering similar projects and can meet the requirements defined in the SOW Section 3.1.6.

4.4.8.2 **Criterion** – At not more than two (2) pages in length, the Offeror shall provide a CV for their offered QAR detailing their individual experience in accordance with the requirements specified in the SOW Section 7.3.

4.4.8.3 Document Reference

4.4.8.3.1 RFQ Instructions, Section III, Paragraph 3.5.1.5.3

4.4.8.3.2 SOW Sections 3.1.6, 7.3

4.4.8.4 Pass/Fail Criteria

4.4.8.4.1 Pass – The Offeror has included each element from Section III, Paragraph 3.5.1.11.2 of the Book I – RFQ Instructions in its Technical Proposal. The Offeror's Technical Proposal contains a QAR's CV which clearly explains how the requirements specified in the SOW Section 7.3 shall be met by the Offeror.

4.4.8.4.2 Fail – The Offeror has not included each element from Section III, Paragraph 3.5.1.11.2 of the Book I – RFQ Instructions in its Technical Proposal. The

Offeror has not submitted a response to this criterion, or the Offeror's Technical Proposal does not contain a QAR's CV which clearly explains how the requirements specified in the SOW Section 7.3 shall be met by the Offeror.

4.4.9 Any content provided over the page limit specified for each question will not be subject to evaluation.

4.4.10 If an Offeror's Technical Proposal is awarded a 'Fail' for any of the criteria listed in Section IV, Paragraph 4.4 above, its Proposal will be deemed technically non-compliant.

ANNEX A – Clarification Request Forms

INSERT COMPANY NAME HERE

INSERT SUBMISSION DATE HERE

ADMINISTRATIVE/CONTRACTUAL				
Serial Nr	**RFQ Section Ref.**	**OFFEROR'S QUESTION**	**NCI AGENCY ANSWER**	**Status***
A.1				
A.2				
A.3				

* Status: Is Amendment to RFQ required as a direct result of the Clarification Request?

INSERT COMPANY NAME HERE

INSERT SUBMISSION DATE HERE

PRICE				
Serial Nr	**RFQ Section Ref.**	**OFFEROR'S QUESTION**	**NCI AGENCY ANSWER**	**Status***
P.1				
P.2				
P.3				

* Status: Is Amendment to RFQ required as a direct result of the Clarification Request?

INSERT COMPANY NAME HERE

INSERT SUBMISSION DATE HERE

TECHNICAL				
Serial Nr	**RFQ Section Ref.**	**OFFEROR'S QUESTION**	**NCI AGENCY ANSWER**	**Status***
T.1				
T.2				
T.3				

* Status: Is Amendment to RFQ required as a direct result of the Clarification Request?

ANNEX B-1 - CERTIFICATE OF LEGAL NAME OF OFFEROR

This Quotation is prepared and submitted on behalf of the legal corporate entity specified below:

FULL NAME OF CORPORATION: _____

DIVISION (IF APPLICABLE): _____
SUB DIVISION (IF APPLICABLE): _____

OFFICIAL MAILING ADDRESS: _____

_____

_____

E-MAIL ADDRESS: _____

FAX NO.: _____

BOA NO.: _____

POINT OF CONTACT (POC) REGARDING THIS QUOTATION:

NAME: _____
POSITION: _____
TELEPHONE: _____
E-MAIL ADDRESS: _____

ALTERNATIVE POC:

NAME: _____
POSITION: _____
TELEPHONE: _____
E-MAIL ADDRESS: _____

_____ _____
DATE SIGNATURE OF AUTHORISED REPRESENTATIVE

_____
PRINTED NAME

_____
TITLE

ANNEX B-2 - CERTIFICATE OF INDEPENDENT DETERMINATION

1. Each Offeror shall certify signing this Quotation shall also certify that:

Each Offeror shall certify that in connection with this procurement:

a. This quotation has been arrived at independently, without consultation, communication or agreement, for the purpose of restricting competition, with any other Offeror or with any competitor;

b. The contents of this Quotation have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to award, directly or indirectly to any other Offeror or to any competitor, and;

c. No attempt has been made, or will be made by the Offeror to induce any other person or firm to submit, or not to submit, a Quotation for the purpose of restricting competition.

2. Each person signing this Quotation shall also certify that:

a. They are the person in the Offeror's organisation responsible within that organisation for the decision as to the quotation and that they have not participated and will not participate in any action contrary to 1(a) through 1(c) above, or;

b. (i) They are not the person in the Offeror's organisation responsible within that organisation for the quotation but that they have been authorised in writing to act as agent for the persons responsible for such a decision in certifying that such persons have not participated, and will not participate in any action contrary to 1(a) through 1(c) above, and as their agent does hereby so certify, and;

(ii) They have not participated and will not participate in any action contrary to 1(a) through 1(c) above.

…..
Date

…..
Signature of Authorised Representative

…..
Printed Name and Title

…..
Company

NOTE: IF THE OFFEROR DELETES OR MODIFIES SUBPARAGRAPH (1B) OF THIS ANNEX, THE OFFEROR MUST FURNISH WITH ITS QUOTATION A SIGNED STATEMENT SETTING FORTH IN DETAIL THE CIRCUMSTANCES OF THE DISCLOSURE.

ANNEX B-3 - CERTIFICATE OF QUOTATION VALIDITY

I, the undersigned, as an authorised representative of the firm submitting this quotation, do hereby certify that the pricing and all other aspects of our Quotation will remain valid for a period of six (6) months from the RFQ Closing Date of this Request for Quotation.

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

ANNEX B-4 - CERTIFICATE OF UNDERSTANDING

I certify that

.....
.....*(Company Name)* has read and fully understands the requirements of this Request for Quotation (RFQ) and that the Quotation recognises these requirements in total.

I also certify to the best of my expert knowledge that this Quotation is within the "state of art" boundaries as they exist at the time of quotation for this project.

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

ANNEX B-5 - CERTIFICATE OF EXCLUSION OF TAXES, DUTIES AND CHARGES

I hereby certify that the prices offered in the price quotation of this Quotation exclude all taxes, duties and customs charges from which the Purchaser has been exempted by international agreement.

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

ANNEX B-6 - ACKNOWLEDGEMENT OF RECEIPT OF RFQ AMENDMENTS

I confirm that the following Amendments to Request for Quotation No RFQ-CO-115518-NPKI-M have been received and the Quotation as submitted reflects the content of such Amendments:

Amendment Number	**Date of Issue by the Purchaser**	**Date of Receipt by the Offeror**

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

ANNEX B-7 - DISCLOSURE OF REQUIREMENTS FOR NCI AGENCY EXECUTION OF SUPPLEMENTAL AGREEMENTS

I, the undersigned, as an authorised representative of …… ……..……*(Company Name)*, certify the following statement (*Check the applicable statement below*):

☐ I do not have any supplemental agreements to disclose for the performance of this contract [*cross out points 1 to 6 of this certificate*].

☐ I do have supplemental agreements to disclose for the performance of this contract (*complete points 2 and 3 below in a separate attachment to this certificate*).

1. All supplemental agreements, defined as agreements, documents and/or permissions outside the body of the Contract but required by my Government, and the governments of my sub-Contractors, to be executed by the NCI Agency as a condition of my firm's performance of the Contract, have been identified, as part of the Quotation.

2. Examples of the terms and conditions of these agreements are attached hereto. The anticipated restrictions to be imposed on NATO, if any, have been identified in our offer along with any potential conflicts with the terms, conditions and specifications of the Prospective Contract, see …….. *(complete, if any)*. These anticipated restrictions and potential conflicts are based on our knowledge of and prior experience with such agreements and their implementing regulations. We do not certify that the language or the terms of these agreements will be exactly as we have anticipated.

3. The processing time for these agreements has been calculated into our delivery and performance plans and contingency plans made in the case that there is delay in processing on the part of the issuing government(s), see …….. *(complete, if any)*.

4. We recognise that additional supplemental agreements, documents and permissions presented as a condition of Contract performance or MOU signature after our firm would be selected as the successful Offeror may be cause for the NCIA to determine the submitted quotation to be non-compliant with the requirements of the RFQ.

5. We accept that should the resultant supplemental agreements issued in final form by the government(s) result in an impossibility to perform the Contract in accordance with its schedule, terms or specifications, the Contract may be terminated by the Purchaser at no cost to either Party.

…..
Date

…..
Signature of Authorised Representative

…..
Printed Name and Title

…..
Company

ANNEX B-8 - CERTIFICATION OF NATO MEMBER COUNTRY ORIGIN OF DELIVERED EQUIPMENT, SERVICES, MATERIALS AND INTELLECTUAL PROPERTY RIGHTS

The Offeror hereby certifies that, if awarded the Contract pursuant to this solicitation, it will perform the contract subject to the following conditions:

(a) none of the work, including project design, labour and services shall be performed other than by firms from and within participating NATO member countries;

(b) no material or items of equipment down to and including identifiable sub-assemblies shall be manufactured or assembled by a firm other than from and within a participating NATO member country (a sub-assembly is defined as a portion of an assembly consisting of two or more parts that can be provided and replaced as an entity)*; and

(c) the intellectual property rights to all design documentation and related system operating software shall reside in NATO member countries, and no license fees or royalty charges shall be paid by the Contractor to firms, individuals or governments other than within the NATO member countries.

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

*This definition purposely excludes components and/or parts (as defined in AcodP-1), which are not subject to this certification.

ANNEX B-9 - Comprehension and Acceptance of CONTRACT General and Special Provisions

The Offeror hereby certifies that it has reviewed the Contract Special Provisions set forth in the Prospective Contract, Book II of this Request for Quotation (RFQ) and the Contract Provisions set forth in the Basic Ordering Agreement signed with the NCI Agency. The Offeror hereby provides its confirmation that it fully comprehends the rights, obligations and responsibilities of the Contractor as set forth in the Articles and Clauses of the Prospective Contract. The Offeror additionally certifies that the Quotation submitted by the Offeror is without prejudice, qualification or exception to any of the Terms and Conditions and it will accept and abide by the stated Special Contract Provisions if awarded the contract as a result of this RFQ.

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

ANNEX B-10 - LIST OF PROSPECTIVE SUB-CONTRACTORS/CONSORTIUM MEMBERS[1]

Name and Address of Sub-Contractor, incl. country of origin/registration	Primary Location of Work	Items/Services to be Provided	Estimated Value of Sub-Contract

If no sub-Contractors/consortium members are involved, state this here:
……..
……
……
……..

…….....
Date

…….....
Signature of Authorised Representative

…….....
Printed Name and Title

…….....
Company

[1] In accordance with Section III, Paragraph 3.4.15 of Book I, the Offeror shall identify in this Certificate any subcontractors whose estimated value of the subcontract is expected to equal or exceed €125,000.00.

ANNEX B-11 - CERTIFICATE OF AQAP 2110 OR ISO 9001:2015 COMPLIANCE

I hereby certify that …… *(Company Name)* is fully compliant with the AQAP 2110 or ISO 9001:2015 Quality Assurance Standards and Procedures, is currently so certified, and will remain certified throughout the duration of the contract.

A copy of the quality certification is **attached herewith**.

…….
Date

…….
Signature of Authorised Representative

…….
Printed Name and Title

…….
Company

ANNEX B-12 - LIST OF KEY PERSONNEL

Name	Position

Personal Data Protection

Although NATO, as an international organization, is not subject to General Data Protection Regulation (GDPR) and national data protection law, it is committed to protecting the personal data that it processes. All processing of personal data will be done in accordance with applicable NATO policies and regulations.

ANNEX B-13 – DISCLOSURE OF INVOLVEMENT OF FORMER NCI AGENCY EMPLOYMENT

The Offeror hereby certifies that, in preparing its Quotation, the Offeror did not have access to solicitation information prior to such information been authorized for release to Offerors (e.g., draft statement of work and requirement documentation).

The Offeror hereby acknowledges the post-employment measures applicable to former NCI Agency Personnel as per the NCI Agency Code of Conduct.

The Offeror hereby certifies that its personnel working as part of the company's team, at any tier, preparing the Quotation:

- Have not held employment with NCI Agency within the last two years.
- Has obtained a signed statement from the former NCI Agency personnel below, who departed the NCI Agency within the last two years, that they were not previously involved in the project under competition (as defined in the extract of the NCI Agency Code of Conduct provided below):

Employee Name	Former NCIA Position	Current Company Position

The Offeror also hereby certifies that it does not employ and/or receive services from former NCI Agency Personnel at grades A5 and above or ranks OF-5 and above, who departed the NCI Agency within the last 12 months. This prohibitions covers negotiations, representational communications and/or advisory activities.

_____
Date

_____
Signature of Authorised Representative

_____
Printed Name

_____
Title

_____
Company

Excerpt of NCI Agency AD. 05.00, Code of Conduct dated May 2017

Article 14 PROCUREMENT AND CONTRACTORS

14.1 NCI Agency Personnel are required to maintain unquestionable integrity and impartiality in relation to procurements initiated by the NCI Agency.

14.2 NCI Agency Personnel shall not disclose any proprietary or contract related information regarding procurement directly or indirectly to any person other than a person authorized by the NCI Agency to receive such information. NCI Agency Personnel shall not disclose any documentation related to a procurement action to any third party without a need to know1 (e.g., draft statement of work, statement of requirements) unless this is expressly provided under NATO Procurement Regulations or authorized in writing by the Director of Acquisition. During an on-going selection, NCI Agency Personnel shall not disclose any information on the selection procedure unless authorized by the Chairman of the award committee/board. The NCI Agency Personnel concerned will ensure that proper access controls are put in place to prevent disclosure of procurement information that has not yet been authorized for release for outside distribution, including draft statements of work and requirement documentations.

14.3 NCI Agency Personnel will not participate in a source selection if an offer has been provided by a friend, family member, a relative, or by a business concern owned, substantially owned, or controlled by him/her or by a friend, family member or a relative. NCI Agency Personnel appointed as part of an evaluation shall report such links to the Director of Acquisition immediately upon becoming aware of it.

14.4 Contractors and consultants shall not be allowed to participate in the drafting of the statement of work or in the source selection process unless they and their company/employer will be excluded from competition of the related contract. The same will apply to contractors and consultants involved in the definition and development of requirements.

14.5 Contractors will be given specific and coherent statements of work, providing precise explanation of how she/he is going to be employed. Tasks to be performed and minimum qualifications are to be well defined from the start. In addition, supervisors will ensure that contractors do not occupy managerial positions within the Agency.

14.6 NCI Agency Personnel shall not enter into authorized commitments in the name of NCI Agency or NATO unless specifically authorized. NCI Agency Personnel must abstain from making promises or commitment to award or amend a contract or otherwise create the appearance of a commitment from the NCI Agency unless properly authorized by the NCI Agency.

14.7 NCI Agency Personnel shall not endorse directly or indirectly products from industry. Therefore, NCI Agency Personnel shall not name or make statements endorsing or appearing to endorse products of specific companies.

14.8 Industry partners will need to abide with the post-employment measures under this Directive upon submission of their Quotations / proposals to the NCI Agency. As part of the selection process, industry will be requested to agree with an ethical statement.

15 INDUSTRY INITIATIVES

15.1 Industry initiatives may include loans, displays, tests or evaluation of equipment and software, requesting NCI Agency speakers at industry gatherings and conferences, inviting speakers from industry to NCI Agency events, consultancy or studies of technical or organizational issues, etc. These initiatives are usually at no cost to the NCI Agency and take place at a pre-contractual phase or before the development of requirements and specifications. While there are benefits associated with the early involvement of industry in the definition of requirements and specifications, this also raises the potential for unfair treatment of potential competitors.

15.2 Industry initiatives which go beyond routine interaction in connection with on-going contracts must be reported to and coordinated by the NCI Agency Acquisition Directorate for approval. Industry initiatives shall be properly documented and governed by written agreements between the NCI Agency and the company concerned where relevant. Such agreements may contain provisions describing the nature of the initiative, the non-disclosure of NCI Agency/NATO information, NCI Agency ownership of any resulting work, the NCI Agency's right to release such work product to future competitors for any follow-on competition or contract, the requirement that any studies must provide non-proprietary solutions and/or an acknowledgement that the participating companies will not receive any preferential treatment in the contracting process.

15.3 Any authorized industry initiatives must be conducted in such a way that it does not confer an unfair advantage to the industry concerned or create competitive hurdles for potential competitors.

16 POST EMPLOYMENT MEASURES

16.1 The NCI Agency will not offer employment contracts to former NCI Agency Personnel who departed less than 2 years earlier, unless prior approval by the General Manager has been received.

16.2 Former NCI Agency Personnel will not be accepted as consultants or commercial counterpart for two (2) years after finalization of their employment at NCI Agency, unless the General Manager decides otherwise in the interest of the Agency and as long as NATO rules on double remuneration are observed. Such decision shall be recorded in writing. Commercial counterparts include owners or majority shareholders, key account managers, or staff member, agent or consultant of a company and/or subcontractors seeking business at any tier with the NCI Agency in relation to a procurement action in

which the departing NCI Agency staff member was involved when they were under the employment of the NCI Agency. As per the Prince 2 Project methodology, a Project is defined as a "temporary organization that is created for the purpose of delivering one or more business products according to an agreed business case". For the purpose of this provision, involvement requires (i) drafting, review or coordination of internal procurement activities and documentation, such as statement of work and statement of requirement; and/or (ii) access to procurement information that has not yet been authorized for release for outside distribution, including draft statements of work and requirement documentations; and/or (iii) being appointed as a representative to the Project governance (e.g., Project Board) with access to procurement information as per (ii) above; and/or (iv) having provided strategic guidance to the project, with access to procurement information as per (ii) above.

16.3 In addition to Section 16.2 above, former NCI Agency Personnel at grades A5 and above or ranks OF-5 and above are prohibited during twelve months following the end of their employment with the NCI Agency to engaging in negotiations, representational communications and/or advisory activities with the NCI Agency on behalf of a private entity, unless this has been agreed in advance by the NCI Agency General Manager and notified to the ASB.

16.4 NCI Agency Personnel leaving the Agency shall not contact their former colleagues in view of obtaining any information or documentation about procurement activities not yet authorized' release. NCI Agency Personnel shall immediately report such contacts to the Director of Acquisition.

16.5 The ASB Chairman will be the approving authority upon recommendation by the Legal Adviser when the NCI Agency Personnel concerned by the above is the NCI Agency General Manager and will notify the ASB.

16.6 NCI Agency Personnel leaving the Agency shall sign a statement that they are aware of the post-employment measures set out in this Directive.

16.7 The post-employment measures set out in this Directive shall be reflected in the NCI Agency procurement documents, such as IFBs, and contract provisions.

ANNEX B-14 - OFFEROR BACKGROUND IPR

The Offeror Background IPR specified in the table below will be used for the purpose of carrying out work pursuant to the Contract.

ITEM	DESCRIPTION

The Offeror has and will continue to have, for the duration of the Contract, all necessary rights in and to the Background IPR specified above.

The Background IPR stated above complies with the terms specified in Article 30 of the NCI Agency, Part III - General Provisions.

ANNEX B-15 - LIST OF SUBCONTRACTOR IPR

The Subcontractor IPR specified in the table below will be used for the purpose of carrying out work pursuant to the Contract.

ITEM	DESCRIPTION

The Offeror has and will continue to have, for the duration of the Contract, all necessary rights in and to the IPR specified above necessary to perform the Offeror's obligations under the Contract.

The Subcontractor IPR stated above complies with the terms specified in Article 30 of the NCI Agency, Part III - General Provisions.

ANNEX B-16 – VENDOR SUPPLY CHAIN SECURITY SELF-ATTESTATION STATEMENT

I hereby as [*Insert Company Name*] affirm that the security of the supply chain for the product [*list the product(s) below*]

has been assessed and assessed against the requirements laid down in directive AC/322-D(2017)0016 (INV), named "NATO SUPPLY CHAIN SECURITY REQUIREMENTS FOR COMMERCIAL OFF THE SHELF COMMUNICATION AND INFORMATION SYSTEMS SECURITY ENFORCING PRODUCTS".

I endorse this supply chain security statement for the product listed in the first paragraph of this certificate which covers the following items:

- Supply Chain Security Program Governance
- Security in Manufacturing and Operations
- Security in Logistics
- NATO Information Protection
- Vendor Physical and Personnel Security
- Security in Service Management
- Security in Incident Management
- 3rd Party Supplier Management

I can supply supporting evidence if required.

Date	Signature of Authorised Representative
	Printed Name
	Title
	Company

ANNEX B-17 – COMPANY COMPLIANCE WITH SAFEGUARDING NATO INFORMATION CONTROLS SELF-ATTESTATION STATEMENT

The security requirements required by the contract's Special Provisions clause, Basic Safeguarding of Contractor Communication and Information Systems (CIS), shall be implemented for NATO Information on all contractor communication information systems (CIS) that support the performance of this contract.

I, the undersigned, as an authorised representative of …… ……..……*(Company Name)*, certify that by submission of this bid, we assure the Purchaser that we will comply and implement the mandatory security measures in accordance with the Book II Special Provisions, "Basic Safeguarding of Contractor Communication and Information Systems (CIS)" and their mandatory references not later than by Contract Award or as agreed by the Contracting Officer.

I can supply supporting evidence, upon request by the Contracting Officer, by means of a completed System Security Plan[1] (or extract thereof) and any associated plans of actions developed to describe the Contractor's CIS where NATO Information associated with the execution and performance of this contract is processed, stored, developed, or transmitted.

Company:

Signature:

Date:

[1] *System Security Plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems.*

ANNEX C – PRICING SHEETS

[Provided under separate MS Excel File:]

"RFQ-CO-115518-NPKI-M_Book I_Annex C_Pricing Sheets"

ANNEX D – COMPLIANCE TABLE

Offeror shall complete column "QUOTATION REFERENCE" with Quotation references that locate the technical proposal documentation required by the RFQ, e.g. section, paragraph, table (if applicable), page number etc. One copy each of the duly completed Cross Reference/Compliance Table is to be included in the Quotation Technical Proposal package. The Quotation shall follow the instructions in Section III, Paragraph 3.5, and will be evaluated according to the instructions in Section IV, Paragraph 4.4.

RFQ Instructions Requirement Ref.	SOW Requirement Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	QUOTATION REFERENCE
3.5.1.1 Table of Contents	N/A	The Offeror shall compile a detailed Table of Contents which lists not only section headings but also major sub-sections, and topic headings required set forth in these Instructions or implicit in the organisation of the Technical Proposal	4.4.2	***Offeror to complete***
3.5.1.2 Cross-Reference / Compliance Table	N/A	The Offeror shall include the completed Technical Proposal Cross-Reference Table at Annex D of Book I. The Offeror shall complete the Column marked "QUOTATION REFERENCE" of the Table, citing the appropriate section of the Technical Proposal that corresponds to each paragraph of these Instructions for the Preparation of the Technical Proposal. The completed table serves as an index for the Purchaser's Technical Evaluation Panel and also as an aide memoire to the Offeror to ensure that all the required information has been provided in the Technical Proposal.	4.4.3	

RFQ Instructions Requirement Ref.	SOW Requirement Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	QUOTATION REFERENCE
3.5.1.3 3.5.1.3.1 3.5.1.3.2 Corporate Experience	N/A	The Offeror shall provide at least one (1) executive summary describing the successful delivery of a similar project in a similar environment during the last five (5) years. For each project, the Contractor shall describe: - The domain or area (ideally the customer name), the size (contract value range), duration and challenges encountered with remediation; - The scope of work, demonstrating the Offeror's capability to implement Data Centre Installation similar to the requirements defined in Book II Part IV SOW Annex A.	4.4.4	
3.5.1.4 3.5.1.4.1 3.5.1.4.2 Project Management Plan (PMP)	4.2	The Offeror shall submit a preliminary Project Management Plan in accordance with the requirements of the Statement of Work (Book II Part IV SOW Section 4.2) for the NATO Public-Key Infrastructure Capability (NPKI) WP 2 - Data Centre Installation, which clearly describes how the Offeror intends to implement the totality of the project in compliance with the contractual requirements. - The PMP shall consider all aspects of project management and control detailed in Book II Part IV SOW Section 4, and demonstrate how all the critical dates defined in the SOW will be met. - The PMP shall include a Project Breakdown Structure (PBS) that shall contain the critical work elements (tasks) of the project and illustrate their relationship to each other and to the project as a whole.	4.4.5	

RFQ Instructions Requirement Ref.	SOW Requirement Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	QUOTATION REFERENCE
3.5.1.5 Project Master Schedule (PMS)	4.4.2	The Offeror shall submit a preliminary Project Master Schedule that shall contain all contract events and milestones for the Project. As described in the SOW Section 4.4.2, the PMS shall show all contractual deliverables, their delivery dates, and the tasks associated with them, including the Purchaser's review stages. The PMS shall for each task identify the start and finish dates, duration, predecessors, constraints, and resources. The PMS shall provide network, milestone, and Gantt views, and identify the critical path for the overall project. Any PMS which does not align with the dates provided in the SSS may be determined to be non-compliant.	4.4.6	
3.5.1.6 System Design, Integration and Implementation	4.10 4.11	The Offeror shall describe how the NATO Public-Key Infrastructure Capability (NPKI) WP2 - Data Centre Installation will be implemented with sufficient technical detail for the Purchaser to determine compliance with the SOW. For this purpose the Offeror shall demonstrate compliance with the Requirements as specified under SOW Sections 4.10 and 4.11, and indicate how the components and quantities of equipment and licenses are to be deployed.	4.4.7	

RFQ Instructions Requirement Ref.	SOW Requirement Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	QUOTATION REFERENCE
3.5.1.7 Integrated Product Support (IPS)	2 5	The Offeror shall describe the Integrated Product Support (IPS) aspects of the Quotation. This description shall address, with an adequate level of detail, the following: Offeror's IPS Organisation, Roles, Responsibilities and Procedures; Maintenance Concept; Logistic Support Analysis (LSA) & Reliability, Maintainability, Availability, Testability (RAMT); Technical Documentation and Data, Supply Support, Support and Test Equipment Lists; Training, including Manpower and Personnel Requirements; Planning and execution of Handling and Storage; Warranty; and Planning of Supply Chain Security as set forth in the SOW Section 5 and in accordance with the applicable Standards and Specifications required in SOW Section 2. The description shall provide sufficient evidence to confirm that the Offeror will be able to meet the timelines in accordance with the requirements of the Schedule of Supplies and Services and the SOW.	4.4.8	
3.5.1.8 Testing	6	The Offeror shall describe how it can meet the NPKI WP 2 testing requirements and its methodology for conducting all related activities as detailed in SOW Section 6. This includes the development of all test documentation required under the prospective Contract, the conduct of all testing, the evaluation and documentation of the tests results by an Independent Verification and Validation (IV&V) as specified in SOW Section 6.	4.4.9	
3.5.1.9 Quality Assurance (QA)	7	The Offeror shall describe how it can meet the Quality Assurance and Quality Control aspects of the Project, as specified in SOW Section 7. The Offeror shall submit a preliminary QA Plan (QAP), with details of how the Offeror shall establish, execute, document and maintain an effective Quality Assurance (QA) programme, throughout the Contract lifetime.	4.4.10	

RFQ Instructions Requirement Ref.	SOW Requirement Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	QUOTATION REFERENCE
3.5.1.10 Configuration Management	2 8	The Offeror shall describe how it can meet the Configuration Management requirements as specified in SOW Section 8. In conformance with the required Standards and Specifications required in SOW Sections 2 and 8, this shall include a description of the unique Configuration Management framework, Baselines, the Product Lifecycle Management (PLM) tool, and the Configuration Management Database (CMDB).	4.4.11	
3.5.1.11 3.5.1.11.1 3.5.1.11.2 Key Personnel	4.3.2 Annex A (SRS) 7.3	The Offeror shall provide curriculum vitae (CV) of the proposed Technical Team/ Subject Matter Experts and Quality Assurance Representative (QAR). - For the Technical Team/ Subject Matter Experts, the Offeror shall provide details about qualifications and evidence that the proposed technical Subject Matter Experts possess the necessary knowledge, capability and experience of delivering similar projects and that they can meet the requirements defined and detailed in SOW Section 4.3.2 and Annex A (SRS). - For the Quality Assurance Representative (QAR), the Offeror shall provide details about the qualifications, evidence of four (4) years' experience in working with quality control methods and tools and have a broad knowledge of NATO Standards (e.g. STANAG 4107 Ed. 11), processes and procedures applicable to Quality Assurance (QA) and Quality Control (QC) in the industry.	4.4.12 4.4.13	

RFQ Instructions Requirement Ref.	SOW Requirement Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	QUOTATION REFERENCE
3.5.1.12 Purchaser Furnished Equipment (PFE) Management	Annex B	in accordance with SOW Annex B, the Offeror shall provide details on its approach to preventing projects from stalling following delay in the provision of PFE.	4.4.14	

Pricing Sheets Instructions

INTRODUCTION & IMPORTANT NOTES	
	Offerors should note that NCIA has recently updated its pricing sheet template and are encouraged to read the instructions in full for this new version before completing the pricing sheets. All Offerors are required to submit pricing details to demonstrate the Purchaser's Pricing Principles are being applied as part of their Quotations. All data submitted in these sheets shall be complete, verifiable and factual and include the required details. Any exclusions may render the Quotation as non compliant thus removing the Offeror from the RFQ process. Offerors are REQUIRED to complete the following tabs: - "Offer Summary", - "CLIN Summary", - "Labour", - "Material", - "Travel", - "ODC", - "Rates". Note that input cells in the "Offer Summary" and the "CLIN Summary" tabs are colour coded YELLOW. The instructions for the detailed tabs can be found below, as well as in the green boxes within each detailed tab. G&A, Overhead, material handling and other indirect rates do not need to be separately calculated in the detail sheets but must be included in the totals for each category (Labour/Material/Travel/ODC) as appropriate. A list of the direct and indirect rates applied in the Quotation must also be provided in the "Rates" tab, although they do not need to be linked to any and the detailed calculations. The list of these rates will be requested at pre-contract award stage from the winning Offeror.

	Note: any information found within GREEN boxes throughout the entire document is provided as an instruction and/or example only. Any formulas provided in these pricing sheets are intended only to assist the Offeror. Any changes in formula can be made at the Offeror's discretions, as long as the detailed costs are clear, traceable and accurate as required. Ultimately the Offeror is responsible for ALL values, formulas and calculations within the pricing sheets that are submitted to the Agency. Quotations in MULTIPLE CURRENCIES should follow the following instructions: - For the "Offer Summary" tab Offerors must add a "Firm Fixed Price" column to the right of the current table for each additional currency. - For the "CLIN Summary" tab, Offerors have 2 options: A) Two columns "Unit Price" and "Total Firm Fixed Price" may be added to the right of the current table for each additional currency of the quotation; B) Offerors may duplicate the CLIN Summary tab for each currency quotation. - For the Detailed tabs Offerors have 2 options: A) Provide all the detailed data for all currencies in the table provided, selecting the individual currencies from the dropdown lists and summing only common currencies together in CLIN Summary/Offer Summary Sheets B) Duplicate the CLIN Summary tab for each currency quotation.

DETAILED TABs	DESCRIPTION
MATERIAL **LABOUR** **TRAVEL** **ODCs**	The detailed tables are to be completed by the Offeror with all columns populated, and shall be expanded to include as many rows as necessary to provide the detail requested. The Offeror is required to identify for each item the CLIN it is associated with from the drop down menu. Each column should then be populated using the column- specific instructions in the first row. Offerors may not delete columns within tables, or omit information from columns, but may add columns if necessary, although it's not anticipated this will be needed. Note CLINs with no costs associated with that item should also be selected within the table, and noted that there is no cost within that table for the CLIN. For example, if there is no labour associated with CLIN X.1, Select CLIN X.1 in the first column and then in the second column note "No Labour is associated with this CLIN". This will help to ensure that all the proper detail has been accounted for and properly allocated. Important Note: The Total sum of the "fully burdened" cost column should equal the grand total cost for each category (Labour, Material, etc.) to include profit as well as all indirect rates (G&A/Overhead/Material handling/etc.) associated with that category. These indirect rates must be included in the total firm fixed price on the appropriate detailed tab but are no longer required to be shown as separate calculations at the RFQ stage. However, the Offeror is required to include the associated indirect costs in the totals of the detailed tab in the base unit costs. Alternatively, the Offeror may choose to show these as separate calculations by expanding the table columns to show the additional costs due to these indirect rates (similar to the way profit is calculated). Note again although the detailed indirect rate calculations are not required at the RFQ stage, this information will be requested from the winning Offeror during pre-contract award discussions.

RATES	As discussed previously in these instructions, the detailed indirect rate calculations are not required to be included in the pricing sheets, although the Offerors may chose to do so. However, ALL Offerors are required to state the G&A/OH/Material handling and any other indirect rates that they have applied to the Quotation.

CLIN Number	CLIN DESCRIPTION	Firm Fixed Price
	Declare Currency =>	

Grand Total Firm Fixed Price - Base Contract	-

CLIN 1	CLIN 1 (BASE-EVALUATED) - PROJECT MANAGEMENT ACTIVITIES	-
CLIN 2	CLIN 2 (BASE-EVALUATED) - DESIGN	-
CLIN 3	CLIN 3 (BASE-EVALUATED) - SOFTWARE, LICENSES AND SERVICES	-
CLIN 4	CLIN 4 (BASE-EVALUATED) - INSTALLATION AND IMPLEMENTATION	-
CLIN 5	CLIN 5 (BASE-EVALUATED) - ITEGRATED PRODUCT SUPPORT (IPS)	-
CLIN 6	CLIN 6 (BASE-EVALUATED) - TESTING AND QUALITY ASSURANCE	-
CLIN 7	CLIN 7 (BASE-EVALUATED) - CONFIGURATION MANAGEMENT	-
CLIN 8	CLIN 8 (BASE-EVALUATED) - WARRANTY	-
Total Firm Fixed Price Base Contract		**-**

RFQ-CO-115518-NPKI-M CLIN Summary
BASE CONTRACT

CLIN	Description	SOW Reference	Required Completion Date	Delivery Destination	Notes	Unit of measure	Quantity	Unit Price	Total Firm Fixed Price	Optional Comments (Mandatory for zero costs lines)
								Declare Currency =>		
1.0	CLIN 1 (BASE-EVALUATED) - PROJECT MANAGEMENT ACTIVITIES									
1.1	Project Management	4.1	From EDC +0 weeks to EDC +37 weeks	N/A	Includes all Project Management activities not separately listed below.	Task	1	-	-	
1.2	Project Kick-off Meeting	4.2	EDC +1 week	NCIA/ SHAPE, Mons		Task	1	-	-	
1.3	Project Review Meetings	4.9.2.2	From EDC +4 weeks to EDC +37 weeks	Virtual	Monthly	Task	8	-	-	
1.4	Contract Data Requirements List (CDRL)	Annex D	See SSS - Schedule A - CDRL	Project Portal	All deliverables as per SSS - Schedule A - CDRL	Lot	1	-	-	
TOTAL PRICE CLIN 1									-	
2.0	CLIN 2 (BASE-EVALUATED) - DESIGN									
2.1	System Design Review (SDR)	4.10	First session: EDC +4 weeks Second session: EDC +5 weeks	NCIA/ SHAPE, Mons	2 x sessions totalling 5 days	Task	2	-	-	
2.2	MS 1 - Design Review Approved	4.1	EDC +10 weeks	NCIA/ SHAPE, Mons		Task	1	-	-	
TOTAL PRICE CLIN 2									-	
3.0	CLIN 3 (BASE-EVALUATED) - SOFTWARE, LICENSES AND SERVICES									
3.1	Red Hat Enterprise Linux (RHEL) Licences with smartmanager add-on	4.11.2	EDC +20 weeks	NCIA/ SHAPE, Mons		Each	2	-	-	
TOTAL PRICE CLIN 3									-	
4.0	CLIN 4 (BASE-EVALUATED) - INSTALLATION AND IMPLEMENTATION									
4.1	Installation Preparation Shipping of HW & SW to site	4.11.1	EDC +10 weeks	NCIA/ SHAPE, Mons		Task	1	-	-	
4.2	MS 2 - NPKI-M Reference Environment High Side Completed and Accepted	3.3	EDC +20 weeks	NCIA/ SHAPE, Mons		Task	1	-	-	
4.3	MS 3 - NPKI-M Reference Environment Low Side Completed and Accepted	3.4	EDC +25 weeks	NCIA/ SHAPE, Mons		Task	1	-	-	
4.4	MS 4 - NPKI-M Production Environment High Side Completed and Accepted	3.5	EDC +30 weeks	SHAPE, Mons/BXL		Task	1	-	-	
4.5	MS 5 - NPKI-M Production Environment Low Side Completed and Accepted	3.6	EDC +35 weeks	SHAPE, Mons/BXL		Task	1	-	-	
4.6	MS 6 - Final System Acceptance (FSA)	3.7	EDC +37 weeks	SHAPE, Mons/BXL		Task	1	-	-	
TOTAL PRICE CLIN 4									-	
5.0	CLIN 5 (BASE-EVALUATED) - INTEGRATED PRODUCT SUPPORT (IPS)									
5.1	Training Session for Administrators	5.6	First session: n.l.t. EDC +30 weeks Second session: n.l.t. EDC +33 weeks	NCIA/ SHAPE, Mons	Training sessions (2 in total)	Task	2	-	-	
5.2	Labelling activities	5.9	From MS2 (EDC + 20W) to MS5 (EDC + 35W) completion	NCIA/ SHAPE, Mons	Labelling after testing completion and beofre MS2-MS5 are granted	Task	4	-	-	
TOTAL PRICE CLIN 5									-	
6.0	CLIN 6 (BASE-EVALUATED) - TESTING AND QUALITY ASSURANCE									
6.1	Engineering Tests & Qualification Tests	6.2	From EDC +10 weeks to EDC +37 weeks	NCIA/ SHAPE, Mons	Testing executed by the Contractor during Installation, Implementation and Testing phase and reviewed by IV&V.	Task	1	-	-	
6.2	IV&V Assessment	6.2	From EDC +10 weeks to EDC +37 weeks	NCIA/ SHAPE, Mons	Including Test Readiness Review Meetings and Test Review Meetings	Task	1	-	-	
6.3	Operational Test and Evaluation	6.2	From EDC +35 weeks to EDC +37 weeks	NCIA/ SHAPE, Mons		Task	1	-	-	
TOTAL PRICE CLIN 6									-	
7.0	CLIN 7 (BASE-EVALUATED) - CONFIGURATION MANAGEMENT									
7.1	PCA events (preparation and attendance pre-test and post test)	8	Before test start and after test completion	NCIA/ SHAPE, Mons	Baselining before test start and re-check before acceptance	Task	4	-	-	
TOTAL PRICE CLIN 7									-	
8.0	CLIN 8 (BASE-EVALUATED) - WARRANTY									
8.1	Periods from MS2-MS5 to MS6	5.14	From MS2 (EDC + 20W) to MS5 (EDC + 35W) till MS6 (EDC + 37W)	NCIA	Warranty services as per SOW 5.14; fixed duration unless extensions are due	Task	1	-	-	
8.2	Period from MS6 to MS6 + 12 months (FSA - FSA + 12m)	5.14	From MS6 (EDC +37W) to MS6 + 12 months (EDC + 89W)	NCIA	Warranty services as per SOW 5.14; fixed duration unless extensions are due	Task	1	-	-	
TOTAL PRICE CLIN 8									-	
Total Firm Fixed Price- Base Contract									-	

CLIN	Labour Category	Currency	Man-Days 2022	Man-Days 2023	Man-Days 2024	Man-Days 2025	Man-Days 2026	Man-Days 2027	Man-Days 2028	Man-Days 2029	Man-Days 2030	Man-Days 2031	Lab-rate 2022	Lab-rate 2023	Lab-rate 2024	Lab-rate 2025	Lab-rate 2026	Lab-rate 2027	Lab-rate 2028	Lab-rate 2029	Lab-rate 2030	Lab-rate 2031	Extended cost	Expat Allowance (ONLY if applicable)	Profit	Fully burdened cost	Subcontracted/ Name of Subcontractor
Example. CLIN 1.1.1	Systems Engineer	Euro (EUR)	25	20	15	10	5	10	15	20	25	30	50.00	51.00	52.00	53.00	54.00	55.00	56.00	57.00	58.00	59.00	9,600.00		960.00	10,560.00	No
CLIN 1.1	Insert Labour category name here																						-	-	0.00	0.00	
CLIN 1.2	Insert Labour category name here																						-		0.00	0.00	
CLIN 1.3	Insert Labour category name here																						-		0.00	0.00	
CLIN 1.4	Insert Labour category name here																						-		0.00	0.00	
CLIN 2.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 2.2	Insert Labour category name here																						-		0.00	0.00	
CLIN 3.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 4.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 4.2	Insert Labour category name here																						-		0.00	0.00	
CLIN 4.3	Insert Labour category name here																						-		0.00	0.00	
CLIN 4.4	Insert Labour category name here																						-		0.00	0.00	
CLIN 4.5	Insert Labour category name here																						-		0.00	0.00	
CLIN 4.6	Insert Labour category name here																						-		0.00	0.00	
CLIN 5.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 5.2	Insert Labour category name here																						-		0.00	0.00	
CLIN 6.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 6.2	Insert Labour category name here																						-		0.00	0.00	
CLIN 6.3	Insert Labour category name here																						-		0.00	0.00	
CLIN 7.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 8.1	Insert Labour category name here																						-		0.00	0.00	
CLIN 8.2	Insert Labour category name here																						-		0.00	0.00	
Total																										**0.00**	

CLIN	Equipment Name	Item Description	Currency	Quantity 2022	Quantity 2023	Quantity 2024	Quantity 2025	Quantity 2026	Quantity 2027	Quantity 2028	Quantity 2029	Quantity 2030	Quantity 2031	Unit cost 2022	Unit cost 2023	Unit cost 2024	Unit cost 2025	Unit cost 2026	Unit cost 2027	Unit cost 2028	Unit cost 2029	Unit cost 2030	Unit cost 2031	Extended cost	Profit	Fully burdened cost	Subcontracted/ Name of Subcontractor
Example. CLIN 1.1.1	EXAMPLE: BrandX Server: TS1593	Example: HT800003 (model number)	Euro (EUR)	10	20	25	5	5	10	15	20	10	5	150.00	155.00	160.00	165.00	170.00	175.00	180.00	185.00	190.00	195.00	21,300.00	2,130.00	24,430.00	No
CLIN 1.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 1.2	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 1.3	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 1.4	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 2.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 2.2	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 3.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 4.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 4.2	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 4.3	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 4.4	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 4.5	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 4.6	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 5.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 5.2	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 6.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 6.2	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 6.3	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 7.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 8.1	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
CLIN 8.2	Insert Purchased Equipment name	Insert Item Description/Model number																						0.00	0.00	0.00	
Total																										**0.00**	

CLIN	Origin/Destination	Year	Currency	Nr of trips	Nr of people	Nr of Days per trip	Cost per roundtrip	Per Diem	Extended cost	Profit	Total Cost
Example. CLIN 1.1.1	Rome/The Hague	2022	Euro (EUR)	4	3	5	600.00	150.00	16,200.00	810.00	17,010.00
CLIN 1.1	Insert Origin/destination								-	0.00	0.00
CLIN 1.2	Insert Origin/destination								-	0.00	0.00
CLIN 1.3	Insert Origin/destination								-	0.00	0.00
CLIN 1.4	Insert Origin/destination								-	0.00	0.00
CLIN 2.1	Insert Origin/destination								-	0.00	0.00
CLIN 2.2	Insert Origin/destination								-	0.00	0.00
CLIN 3.1	Insert Origin/destination								-	0.00	0.00
CLIN 4.1	Insert Origin/destination								-	0.00	0.00
CLIN 4.2	Insert Origin/destination								-	0.00	0.00
CLIN 4.3	Insert Origin/destination								-	0.00	0.00
CLIN 4.4	Insert Origin/destination								-	0.00	0.00
CLIN 4.5	Insert Origin/destination								-	0.00	0.00
CLIN 4.6	Insert Origin/destination								-	0.00	0.00
CLIN 5.1	Insert Origin/destination								-	0.00	0.00
CLIN 5.2	Insert Origin/destination								-	0.00	0.00
CLIN 6.1	Insert Origin/destination								-	0.00	0.00
CLIN 6.2	Insert Origin/destination								-	0.00	0.00
CLIN 6.3	Insert Origin/destination								-	0.00	0.00
CLIN 7.1	Insert Origin/destination								-	0.00	0.00
CLIN 8.1	Insert Origin/destination								-	0.00	0.00
CLIN 8.2	Insert Origin/destination								-	0.00	0.00
Total											**0.00**

CLIN	Item Name	Item Description	Year	Currency	Unit Type	Quantity	Unit cost	Extended cost	Profit	Total Cost
Example. CLIN 1.1.1	Shipping	Shipping USA to BRU	2021	Euro (EUR)	Lot	2	3,000.00	6,000.00	300.00	6,300.00
CLIN 1.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 1.2	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 1.3	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 1.4	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 2.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 2.2	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 3.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 4.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 4.2	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 4.3	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 4.4	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 4.5	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 4.6	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 5.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 5.2	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 6.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 6.2	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 6.3	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 7.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 8.1	Insert Other Direct Cost item							0.00	0.00	0.00
CLIN 8.2	Insert Other Direct Cost item							0.00	0.00	0.00
Total										**0.00**

Rate Name	Rate description*	Percentage
[Insert Rate Name]		0%
[Insert Rate Name]		0%
[Insert Rate Name]		0%

RFQ-CO-115518-NPKI-M

PROVIDE NATO PUBLIC-KEY INFRASTRUCTURE CAPABILITY (NPKI)
WP 2 - DATA CENTRE INSTALLATION

BOOK II

THE PROSPECTIVE CONTRACT

GENERAL INDEX

NCI AGENCY CONTRACT	
1. Original Number:	**2. Purchase Order Number:**
3. Contract Number: CO-115518-NPKI-M	**4. Effective Date of Contract:**
5. Contractor:	**6. Purchaser:** NATO Communications and Information Agency Boulevard Leopold III B-1110 Bruxelles Belgium
7. Schedule of Supplies and Services: The Contractor shall deliver supplies and/or services in accordance with the attached Part I - Schedule of Supplies and Services (SSS) and Part IV - Statement of Work (SOW).	
8. TOTAL AMOUNT OF CONTRACT **DDP (Incoterms 2020)** Firm Fixed Price:	
9. DELIVERY: See: Part I - Schedule of Supplies and Services (SSS); Part IV - Statement of Work (SOW). Purchaser is exempt from VAT and Customs Duties	**10. SHIP TO/MARK FOR:** See: Part I - Schedule of Supplies and Services (SSS); Part IV - Statement of Work (SOW).
11. CONTRACT AGREEMENT: **a.** The Contractor agrees to furnish all items and perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this Contract shall be subject to and governed by this award/Contract, and such provisions, representations, certifications, and specifications, as are attached or incorporated by Reference. **b.** Modifying paragraph 1 of the Contract General Provisions, the Order of Precedence of the Contract is as follows: 1. This Signature Page; 2. Part I - Schedule of Supplies and Services; 3. Part II - Contract Special Provisions and Annexes; 4. Part II - Contract General Provisions and Annexes; 5. Part IV - Statement of Work and Annexes; 6. Any document expressly incorporated by reference into this Contract.	
12. Signature of Contractor	**13. Signature of Purchaser**
14. Name and Title of Signer	**15. Name and Title of Signer**
16. Date signed by Contractor	**17. Date Signed by Purchaser**

RFQ-CO-115518-NPKI-M

PROVIDE NATO PUBLIC-KEY INFRASTRUCTURE CAPABILITY (NPKI)
WP 2 - DATA CENTRE INSTALLATION

BOOK II, PART I

SCHEDULE OF SUPPLIES AND SERVICES

RFQ-CO-115518-NPKI-M WORK PACKAGE 2
BOOK II PART I - SCHEDULE OF SUPPLIES AND SERVICES

CLIN	Description	SOW Reference	Required Completion Date	Delivery Destination	Notes	Unit of measure	Quantity	Unit Price	Total Firm Fixed Price
								Declare Currency =>	
1.0	CLIN 1 - PROJECT MANAGEMENT ACTIVITIES								
1.1	Project Management	3	EDC +62 weeks	NCIA	Includes all Project Management activities not separately listed below.	Task	1	-	-
1.2	Project Kick-off Meeting	3.5.2.1	EDC +1 week	NCIA		Task	1	-	-
1.3	Project Review Meetings	3.5.2.3	From EDC +4 weeks until FSA, then quarterly	Virtual/NCIA	Monthly	Lot	1	-	-
1.4	Documentation delivery	3.4	As defined in SOW	Project Portal	As defined in SOW	Lot	1	-	-
TOTAL PRICE CLIN 1									-
2.0	CLIN 2 - DESIGN								
2.1	System Requirements Review (SRR)	4.5.2	EDC +4 weeks	NCIA	Minimum 2 days	Task	1	-	-
2.2	Integrated Product Support Plan (IPSP)	5.2	EDC +4 weeks	Project Portal	PDR and CDR	Task	1	-	-
2.3	Configuration Management Plan (CMP)	8	EDC +4 weeks	Project Portal	PDR and CDR	Task	1	-	-
2.4	Requirements Traceability Matrix (RTM)	6.3.4	EDC +6 weeks	Project Portal	PDR and CDR	Task	1	-	-
2.5	Master Test Plan (MTP)	6.3.1	EDC +6 weeks	Project Portal	PDR and CDR	Task	1	-	-
2.6	Event Test Plan (ETP)	6.3.3	EDC +6 weeks	Project Portal	one per environment	Task	8	-	-
2.7	MS 0 - Design Review Approved	4.2.1	EDC +16 weeks	Project Portal	PDR and CDR	Task	1	-	-
TOTAL PRICE CLIN 2									-
3.0	CLIN 3 - SOFTWARE, LICENSES AND SERVICES								
3.1	Red Hat Enterprise Linux (RHEL) Licences with smartmanager add-on, directory services licenses and any additional components and add-ons required	4.1.2	EDC +20 weeks	NCIA		Lot	1	-	-
TOTAL PRICE CLIN 3									-
4.0	CLIN 4 - INSTALLATION AND IMPLEMENTATION								
4.1	MS 1 - NPKI-M Reference Environment High Side (PSA1)	4.2.2	EDC +22 weeks	Mons/Brussels		Task	1	-	-
4.2	MS 2 - NPKI-M Reference Environment Low Side (PSA2)	4.2.3	EDC +28 weeks	Mons/Brussels		Task	1	-	-
4.3	MS 3 - NPKI-M Production Environment High Side (PSA3)	4.2.4	EDC +43 weeks	Mons/Brussels		Task	1	-	-
4.4	MS 4 - NPKI-M Production Environment Low Side (PSA4)	4.2.5	EDC +58 weeks	Mons/Brussels		Task	1	-	-
4.5	MS 5 - Final System Acceptance (FSA)	4.2.6	EDC +62 weeks	Mons/Brussels		Task	1	-	-
TOTAL PRICE CLIN 4									-
5.0	CLIN 5 - INTEGRATED PRODUCT SUPPORT (IPS)								
5.1	Training Session for Administrators	5.8	EDC +58 weeks	NCIA	Training sessions (2 in total)	Task	2	-	-
5.2	Technical Documentation and Data	5.7	EDC +58 weeks	NCIA	Multiple documents	Lot	1		
5.3	Physical Labelling	5.14	EDC +58 weeks	Mons/Brussels	Labelling standards	Task	4	-	-
TOTAL PRICE CLIN 5									-
6.0	CLIN 6 - TESTING AND QUALITY ASSURANCE								
6.1	Engineering Tests & Qualification Tests	6.3	EDC +58 weeks	Mons/Brussels	Testing executed by the Contractor during Installation, Implementation and Testing phase and reviewed by IV&V.	Task	4	-	-
6.2	IV&V Assessment	6.4	EDC +58 weeks	Mons/Brussels	Including Test Readiness Review Meetings and Test Review Meetings	Task	4	-	-
TOTAL PRICE CLIN 6									-
7.0	CLIN 7 - CONFIGURATION MANAGEMENT								
7.1	Allocated Baseline (ABL) and Product Baseline (PBL)	8	One each per delivery milestone	Mons/Brussels		Task	4	-	-
7.2	Physical configuration Audits	4.6.1 4.8 8.1	Pre and Post test events	Mons/Brussels	Baselined before test start and re-check before acceptance	Task	8	-	-
TOTAL PRICE CLIN 7									-
8.0	CLIN 8 - WARRANTY								

8.1	Warranty Milestone 5 (FSA) → FSA+12 m	5.15	EDC +114 weeks	NCIA		Task	1	-	-
TOTAL PRICE CLIN 8									-
Total Firm Fixed Price- Base Contract									-

RFQ-CO-115518-NPKI-M

PROVIDE NATO PUBLIC-KEY INFRASTRUCTURE CAPABILITY

NATO PKI – MITIGATION

WP 2 – DATA CENTRE INSTALLATION

BOOK II, PART II

CONTRACT SPECIAL PROVISIONS

INDEX OF CLAUSES

1. ALTERATIONS, MODIFICATIONS AND DELETIONS OF THE NCI AGENCY CONTRACT GENERAL PROVISIONS

1.1. Clause 8 “Performance Guarantee” of Part III – Contract General Provisions is not applicable and hereby removed.

1.2. Clause 7 “Participating Countries” of these Contract Special Provisions augments Clause 9 “Participating Countries” of Part III – Contract General Provisions.

1.3. Clause 8 "Security" of these Contract Special Provisions augments Clause 11 "Security" of Part III - Contract General Provisions.

1.4. Clause 27 “Inspection and Acceptance of Work” of these Contract Special Provisions augments Clause 21 “Inspection and Acceptance of Work” of Part III – Contract General Provisions

1.5. Clause 28 "Invoices and Payment" of these Contract Special Provisions replaces Clause 25 "Invoices and Payment" of Part III - Contract General Provisions.

1.6. Clause 29 "Liquidated Damages" of these Contract Special Provisions augments Clause 38 "Liquidated Damages" of Part III - Contract General Provisions.

2. ORDER OF PRECEDENCE

2.1. In the event of any inconsistency in this Contract, the inconsistency shall be resolved by giving precedence in the following order:

a. Signature Page

b. Part I - The Schedule of Supplies and Services (SSS)

c. Part II - The Contract Special Provisions

d. Part III – The Contract General Provisions

e. Part IV - The Statement of Work (SOW) and SOW Annexes

f. The Contractor’s Technical Proposal including any clarifications thereto, incorporated by reference, and the formal documentation of pre-Contract discussions.

3. TYPE OF CONTRACT

3.1. This is a Firm-Fixed Price (FFP) Contract established for the supplies and services defined in Part I - SSS and Part IV - SOW.

3.2. The FFP include all expenses related to the performance of the prospective Contract to include travel. The Purchaser assumes no liability for costs incurred by the Contractor in excess of the stated FFP except as provided under other provisions of this Contract.

3.3. The Total Contract price is inclusive of all expenses related to the performance of the present contract.

4. SCOPE

4.1. The primary objective of WP 2 – Data Centre Installation, which is the subject of this Contract, relates to the design and installation of an underlying infrastructure, to be built in two data centres at NATO HQ and in Mons (BEL), that will provide a platform to host NATO's new PKI Services, which will enhance the security of NATO systems

4.2. The geographical location within the scope of the Contract is defined in Part I - SSS and Part IV - SOW.

4.3. The full requirements, Contractor Deliverables and scope is defined in Part I - SSS and Part IV – SOW.

5. PERIOD OF PERFORMANCE (POP)

5.1. The Period of Performance (PoP) of this Contract shall be from the Effective Date of Contract (EDC) until EDC +101 weeks, to include a period of warranty of no less than 12 months from Final System Acceptance (FSA).

6. COMPREHENSION OF CONTRACT AND SPECIFICATIONS

6.1. The Contractor warrants that he has read, understood and agreed to each and all terms, articles, clauses, specifications and conditions specified in the Contract and that this signature of the Contract is an acceptance through delivery, without reservations, of the said Contract terms within their normal and common meaning.

6.2. The Contractor hereby acknowledges that he has no right to assert against the Purchaser, its officers, agents or employees, any claims or demands with respect to the aforesaid specifications as are in effect on the date of award of this Contract.

6.2.1. Based upon impossibility of performance, defective, inaccurate, impracticable, insufficient or invalid specifications, or,

6.2.2. Otherwise derived from the aforesaid specifications, and hereby waives any claims or demands so based or derived as might otherwise arise.

6.2.3. Notwithstanding Clause 16 “Changes” in Part III - Contract General Provisions or any other Clause(s) of the Contract, the Contractor hereby agrees that no changes to the aforesaid specifications which may be necessary to permit achievement of the requirements specified herein for the Contractor’s proposed work shall entitle the Contractor either to any increase in the FFP as set forth in this Contract.

7. PARTICIPATING COUNTRIES

7.1. This Clause augments Clause 9 “Participating Countries” of Part III - Contract General Provisions.

7.2. The following NATO member nations are Participating Countries to this acquisition effort: (in alphabetical order): BELGIUM, BULGARIA, CANADA, CZECH REPUBLIC, DENMARK, ESTONIA, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TÜRKIYE, UNITED KINGDOM, UNITED STATES OF AMERICA.

8. SECURITY

8.1. This Clause augments Clause 11 “Security” of Part III - Contract General Provisions.

8.2. The security classification of this Contract is NATO UNCLASSIFIED.

8.3. Contractor and Subcontractor personnel employed under this Contract that will require access to NATO locations, such as sites and headquarters, where classified material and information up to and including "NATO SECRET" are handled shall be required to have a NATO security clearance up to this level. Contractor personnel who need System Administrator or Operator privileges when working on NATO SECRET systems shall be required to hold NATO CTS (Cosmic Top Secret) clearances.

8.4. The Contractor will be required to handle and store classified material to the level of "NATO SECRET".

8.5. It is the responsibility of the Contractor to ensure that its personnel obtain the required security clearances and transmit this information to the sites to be visited in adequate time that the site may perform the appropriate

administration. Contractors are advised that the personnel security process may be lengthy. The Purchaser bears no responsibility for the failure of the Contractor to secure the required clearances for its personnel within the necessary time.

8.6. Failure to obtain or maintain the required level of security for Contractor personnel for the period of performance of this Contract shall not be grounds for any delay in the scheduled performance of this Contract and may be grounds for termination under Clause 11 “Sub-Contracts” and Clause 39 “Termination for Default” of Part III - Contract General Provisions.

8.7. The Contractor’s Team Members shall possess a valid passport or ID Card and is required to maintain its validity for duration of the contract.

8.8. All NATO CLASSIFIED material entrusted to the Contractor shall be handled and safeguarded in accordance with the applicable security regulations.

8.9. At the end of the Contract, the Contractor shall deliver all the documentation and information collected and generated in support of this Contract to the Purchaser. This includes a certificate that no copies are retained at the Contractor’s facilities. Additionally, any equipment that had been connected to a classified network during this Contract shall be returned to the Purchaser (i.e. laptops, USB-keys, etc.).

8.10. The Contractor shall note that there are restrictions regarding the carriage and use of electronic device (e.g. laptops, cell/mobile telephones) in Purchaser secured locations. The Contractor shall be responsible for satisfying and obtaining from the appropriate site authorities the necessary clearance to bring any such equipment into the facility.

9. CONTRACTOR’S COTS RESPONSIBILITY

9.1. The Contractor shall monitor changes and/or upgrades to commercial off the shelf (COTS) software or hardware (if any) to be utilized under subject Contract.

9.2. For COTS items which are or could be impacted by obsolescence issues, as changes in technology occur, the Contractor will propose substitution of new products/items for inclusion in this Contract. The proposed items should provide at least equivalent performance and/or lower life-cycle support costs, or enhanced performance without a price or cost increase.

9.3. The Contractor will provide evidence with respect to price and performance of the equipment being proposed as well as data proving an

improvement in performance and/or a reduction in price and/or life-cycle support costs. If necessary for evaluation by the Purchaser, the Contractor shall provide a demonstration of the proposed items. Should the Purchaser decide that the proposed item(s) should be included in the Contract, an equitable price adjustment will be negotiated and the proposed item(s) shall be added to the Contract by bilateral modification under the authority of this Clause.

9.4. The Contractor shall notify the Purchaser of any proposed changes in the commercial off the shelf software or hardware to be utilized. Such notification shall provide an assessment of the changes and the impact to any other items to be delivered under this Contract.

10. WAIVER

10.1. No act or omission of either Party shall by itself amount to a waiver of any right or remedy unless expressly stated by that Party in writing. In particular, no reasonable delay in exercising any right or remedy shall by itself constitute a waiver of that right or remedy.

10.2. No waiver in respect of any right or remedy shall operate as a waiver in respect of any other right or remedy.

11. THIRD PARTY RIGHTS

11.1. Notwithstanding anything to the contrary elsewhere in the Contract, no right is granted to any person who is not a Party to the Contract to enforce any term of the Contract in its own right and the Parties to the Contract declare that they have no intention to grant any such right.

12. ENTIRE AGREEMENT

12.1. This Contract constitutes the entire agreement between the Parties relating to the subject matter of the Contract. The Contract supersedes, and neither Party has relied upon, any prior negotiations, representations and undertakings, whether written or oral, except that this condition shall not exclude liability in respect of any fraudulent misrepresentation.

13. NON DISCLOSURE

13.1. The Contractor’s performance under this Contract may require access to third party data and information. The Contractor shall exercise the same degree of care for such third party data and information that it undertakes to preserve and protect its own data and information.

13.2. All Contractor and Sub Contractor personnel working at any NATO Organisations/ Commands premises or having access to NATO classified/commercial-in-confidence information must certify and sign the Non-Disclosure Declaration at Annex A hereto and provide it to the Purchaser's Contracting Authority prior to the commencement of any performance under this contract.

13.3. The Contractor and Subcontractors may be reasonably required to sign subject to their review other non-disclosure agreements or certificates for access to specific information to complete tasks.

13.4. The Contractor shall ensure that its officers, employees, agents and Sub-Contractors shall have been made aware of the requirements of confidentiality and shall not cause or permit the data and/or information to be either totally or partially disclosed to any unauthorised Contractor personnel or third party personnel.

13.5. The Contractor shall be liable for all damages resulting from the non-authorised use of the data and/or information by the Contractor's personnel.

14. ADVERTISEMENTS, PUBLICIZING AWARDS, NEWS RELEASES, AND CONFERENCES

14.1. All press releases or announcements about any contract award hereunder shall be approved by the Purchaser's Contracting Authority prior to release. Under no circumstances shall the Contractor, subcontractor, teaming partner, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the Purchaser's Contracting Authority. The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Purchaser or is considered by the Purchaser to be superior to other products or services.

14.2. Any presentation, white paper, article et cetera written, submitted or presented by Contractor personnel shall be reviewed and approved by the Purchaser's Contracting Authority prior to delivery. This special requirement shall apply whether the Contractor personnel is acting on behalf of the company or unofficially on behalf of himself or herself.

15. EQUALITY

15.1. Without prejudice to Clause 7 above:

15.1.1. the Contractor shall not unlawfully discriminate either directly or indirectly on the grounds of age, disability, gender, sex or sexual orientation, marital status (including civil partnerships), pregnancy and maternity, race, or religion or belief.

15.1.2. the Contractor agrees to take reasonable efforts to secure the observance of the provisions of this Clause 14 by any of its employees, agents, or other persons acting under its direction or Control who are engaged in the performance of the Contract.

15.1.3. the Contractor agrees to take reasonable efforts to reflect this Clause 14 in any subcontract that it enters into to satisfy the requirements of the Contract and to require its Subcontractors to reflect this Clause 16 in their subcontracts that they enter into to satisfy the requirements of the Contract.

16. CONFLICT OF INTEREST

16.1. A conflict of interest means that because of other activities or relationships with other persons or entities, a Contractor is unable, or potentially unable to render impartial assistance or advice to the Purchaser, or the Contractor's objectivity in performing the Contract work is, or might be otherwise impaired, or the Contractor has an unfair competitive advantage. Conflict of interest includes situations where the capacity of a Contractor (including the Contractor's executives, directors, consultants, subsidiaries, parent companies or Subcontractors) to give impartial, technically sound advice or objective performance is or may be impaired or may otherwise result in a biased work product or performance because of any past, present or planned interest, financial or otherwise in organizations whose interest may substantially affected or be substantially affected by the Contractor's performance under the Contract.

16.2. The Contractor is responsible for maintaining and providing up-to-date conflict of interest information to the Purchaser's Contracting Authority. If, after award of this Contract herein, the Contractor discovers a conflict of interest with respect to this Contract which could not reasonably have been known prior to award, or if any additional conflicts or potential conflicts arise after award, the Contractor shall give written notice to the Purchaser's Contracting Authority as set forth below.

16.3. If, after award of this Contract herein, the Purchaser discovers a conflict of interest with respect to this Contract, which has not been disclosed by the Contractor, the Purchaser may at its sole discretion request additional information to the Contractor, impose mitigation measures, or terminate the Contract for default in accordance with Clause 39 "Termination For Default" of Part III – Contract General Provisions.

16.4. The Contractor's notice called for in Clause 18.2 above shall describe the actual, apparent, or potential conflict of interest, the action(s) the Contractor has taken or proposes to take to avoid or mitigate any conflict, and shall set forth any other information which the Contractor believes would be helpful to the Purchaser's Contracting Authority in analyzing the situation. Any changes to the contractors Conflict of Interest Mitigation Plan, if any is incorporated in the Contract, should be also detailed.

16.5. The Contractor has the responsibility of formulating and forwarding a proposed conflict of interest mitigation plan to the Purchaser's Contracting Authority, for review and consideration. This responsibility arises when the Contractor first learns of an actual, apparent, or potential conflict of interest.

16.6. If the Purchaser's Contracting Authority in his/her discretion determines that the Contractor's actual, apparent, or potential conflict of interest remains, or the measures proposed are insufficient to avoid or mitigate the conflict, the Purchaser's Contracting Authority will direct a course of action to the Contractor designed to avoid, neutralize, or mitigate the conflict of interest. If the parties fail to reach agreement on a course of action, or if having reached such agreement the Contractor fails to strictly adhere to such agreement during the remaining period of Contract performance, the Purchaser's Contracting Authority has the discretion to terminate the Contract for default or alternatively refrain from exercising any further Option or Work Package under the contract.

16.7. The Contractor's misrepresentation of facts in connection with a conflict of interest reported or a Contractors failure to disclose a conflict of interest as required shall be a basis for default termination of this contract.

17. MERGERS, ACQUISITIONS, NOVATIONS, AND CHANGE-OF-NAME AGREEMENTS

17.1. If a Contractor merges, is acquired, or recognizes a successor in interest to Purchaser contracts when Contractor assets are transferred; or, recognizes a change in a Contractor's name; or, executes novation agreements and change-of-name agreements by a Contracting Officer other than the Purchaser's Contracting Authority named in Clause 22 of these Contract Special Provisions, the Contractor must notify the Purchaser's Contracting Authority at least thirty (30) days in advance and provide a copy of the novation or other any other agreement that changes the status of the Contractor for signature by the Purchaser. Any successor must be in full compliance with all terms and conditions of this Contract.

18. SUPPLY OF CONTRACTOR DELIVERABLES AND QUALITY ASSURANCE

18.1. The Contractor shall:

18.1.1. provide the Contractor Deliverables to the Purchaser, in accordance with Part I - SSS and Part IV - SOW (including any standards or processes specified therein).

18.1.2. allocate sufficient resources to the provision of the Contractor Deliverables to enable it to comply with the obligations in Part I - SSS and Part IV - SOW.

18.2. The Contractor shall:

18.2.1. comply with any applicable quality assurance requirements specified in Part IV - SOW Section 7 in providing the Contractor Deliverables;

18.2.2. comply with all applicable Law and Legislation;

18.2.3. discharge its obligations under the Contract with all due skill, care, diligence and operating practice by appropriately experienced, qualified and trained personnel.

18.3. The provisions of Clause 18.2 shall survive any performance, acceptance or payment pursuant to the Contract and shall extend to any remedial services provided by the Contractor.

19. KEY PERSONNEL

19.1. The designated Contractor personnel fulfilling the roles described in the SOW are considered Key Personnel for successful Contract performance and are subject to the provisions of this Clause as set forth in the following paragraphs.

19.2. The following personnel are considered Key Personnel for successful contract performance and is subject to the provisions of this Clause as set forth in the following table:

Role	Name
Project Manager	
Technical Lead	
Test Director	
Quality Assurance Representative (QAR)	
Integrated Product Support Manager	
Security Accreditation Manager	
Configuration Manager	

19.3. Under the terms of this Clause, Key Personnel may not be voluntarily diverted by the Contractor to perform work outside the Contract unless approved by the Purchaser. In cases where the Contractor has no control over the individual's non-availability (e.g. resignation, sickness, incapacity, etc.), the Contractor shall notify the Purchaser immediately of a change of Key Personnel and offer a substitute with equivalent qualifications at no additional costs to the Purchaser within 21 days of the date of knowledge of the prospective vacancy.

19.4. The Contractor shall take all reasonable steps to avoid changes to Key Personnel assigned to this project except where changes are unavoidable or are of a temporary nature. Any replacement personnel shall be of a similar grade, standard and experience as the individual to be substituted and must meet the minimum qualifications and required skills cited in the attached SOW.

19.5. In the event of a substitution of any Key Personnel listed above and prior to commencement of performance, the Contractor shall provide a CV for the personnel proposed. The CV shall clearly stipulate full details of professional and educational background, and evidence that the personnel is qualified in relevant Contract related areas prescribed in the SOW.

19.6. The Purchaser reserves the right to interview any Contractor personnel proposed in substitution of previously employed Contractor Key Personnel to verify their language skills, experience and qualifications, and to assess technical compliance with the requirements set forth in the SOW.

19.7. The interview, if required, may be conducted virtually, or may be carried out at the Purchaser's premises at the discretion of the Purchaser Project Manager..

19.8. If, as a result of the evaluation of the CV and/or interview the Purchaser judges that the proposed replacement Key Personnel does not meet the required skills levels, he/she shall have the right to request the Contractor to offer another qualified individual in lieu thereof.

19.9. All costs to the Contractor associated with the interview(s) shall be borne by the Contractor, independently from the outcome of the Purchaser's evaluation.

19.10. The Purchaser Contracting Authority will confirm any consent given to a substitution in writing through an Amendment to the Contract stating the effective date of change of personnel and only such written consent shall be deemed as valid evidence of Purchaser consent. Each of the

replacement personnel will also be required to sign the Non-Disclosure Declaration at Annex A hereto prior to commencement of work.

19.11. Furthermore, even after acceptance of Contractor personnel on the basis of his/her CV and/or interview, the Purchaser reserves the right to reject Contractor personnel, if the individual is not meeting the required level of competence. The Purchaser will inform the Contractor, in writing, in cases where such a decision is taken and the Contractor shall propose and make other personnel available within ten (10) working days after the written notification. The Purchaser shall have no obligation to justify the grounds of its decision and the Purchaser's acceptance of Contractor personnel shall in no way relieve the Contractor of their responsibility to achieve the Contractual and technical requirements of this Contract nor imply any responsibility of the Purchaser.

19.12. The Purchaser may, for just cause, require the Contractor to remove their employee. Notice for removal will be given to the Contractor by the Purchaser in writing and will state the cause justifying the removal. The notice will either demand substitution for the individual involved and/or contain a notice of default and the remedies to be sought by the Purchaser.

19.13. In those cases where, in the judgment of the Purchaser, the inability of the Contractor to provide a suitable replacement in accordance with the terms of this Clause may potentially endanger the progress under the Contract, the Purchaser shall have the right to terminate the Contract as provided under Clause 39 "Termination for Default" of Part III - General Provisions.

20. INDEPENDENT CONTRACTOR

20.1. The Personnel provided by the Contractor in response to this Contract are at all times employees of the Contractor and not the Purchaser. In no case shall Contractor personnel act on behalf of or as an agent for NATO or any of its bodies. In no way shall the Contractor personnel claim directly or indirectly to represent NATO in an official capacity or claim themselves to be NATO employees.

20.2. The Purchaser shall not be responsible for securing work permits, lodging, leases nor tax declarations, driving permits, etc., with national or local authorities. Contractor's personnel employed under this Contract are not eligible for any diplomatic privileges or for NATO employee benefits.

20.3. The Contractor is responsible for providing the necessary insurance for his personnel and equipment as needed in the area of operations and for performing the contract.

21. ENVIRONMENTAL REQUIREMENTS

21.1. The Contractor shall in all its operations to perform the Contract, to the maximum extent possible, adopt a sound proactive environmental approach that identifies, considers, and where possible, mitigates the environmental impacts of its supply chain. If requested by the Purchaser, the Contractor shall provide evidence of so doing in the monthly Project Status Report.

22. BASIC SAFEGUARDING OF CONTRACTOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

22.1. Definitions. As used in this clause—

"Contractor *Communication and Information System*" means an information system that is owned or operated by a contractor that processes, stores, or transmits NATO Information.

"NATO Information" means all information, classified and unclassified, circulated within NATO, whether such information originates in NATO Civil or Military bodies or is received from member nations or from non-NATO sources to include but not limited to:

NATO Information that is provided by or generated for the Purchaser under a contract to develop or deliver a product or service to NATO, but not including information provided by the Purchaser to the public (such as on public websites) or simple transactional information, such as necessary to process payments. Examples of NATO Information are:

NATO technical information that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination that is technical data or computer software in nature; such as, research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, executable code and source code, design details, or formulae and related material that would enable the software to be reproduced, recreated, or recompiled.

NATO infrastructure information such as Emergency Management, Infrastructure Security Information, Information Systems Vulnerability Information, Physical Security.

NATO security information such as Internal Data or Operations Security, Security Agreement Information, Security Enforcement Information, Transportation Arrangements, Personnel Security Information, Privacy Information, or Sensitive Personally Identifiable Information.

"*Information*" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

"*Information system*" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Safeguarding" means measures or controls that are prescribed to protect information systems.

22.2. Safeguarding requirements and procedures. The Contractor shall provide adequate security on all contractor CIS. To provide adequate security, the Contractor shall implement, at a minimum:

22.2.1. For contractor CIS that are part of a cloud computing service or an Information Technology (IT) service or system developed or operated on behalf of NATO shall be subject to the security requirements specified elsewhere in this contract.

22.2.2. For contractor CIS storing, processing, or transmitting NATO RESTRICTED Information the security requirements specified in SoW clause, “Safeguarding of NATO Restricted Information” as mandated in NATO’s Security Committee reference document number, AC/35-D/2003-REV5, dated 13 May 2015, entitled, “Directive on Classified Project and Industrial Security” shall apply.

22.2.3. For contractor CIS storing, processing, or transmitting NATO UNCLASSIFIED Information that are not part of a cloud computing service or IT service or system operated on behalf of NATO, the Contractor shall apply the minimum mandatory security measures as prescribed for NU controls for national systems in the NATO’s Consultation, Command and Control Board (C3B) reference document number AC/322-D/0048-REV3 (INV) dated 18 November 2019, entitled, “Technical and Implementation Directive on CIS Security”.

22.2.4. ***Other requirements***. This clause does not relieve the Contractor of any other specific safeguarding requirements specified elsewhere in this contract or of other applicable NATO or national regulatory requirements.

22.2.5. A breach of these obligations may subject the Contractor to contractual actions in law and equity for penalties, damages, and other appropriate remedies by the Purchaser.

22.2.6. ***Subcontracts***. The Contractor shall include the substance of this clause, including this paragraph (1.1.2.6), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or services in which the subcontractor may have NATO Information residing in or transiting through its CIS.

23. THIRD PARTY CO-OPERATION

23.1. Subject to its other obligations under this Contract, the Contractor shall be open, co-operative and provide reasonable assistance to any third party supplier providing services to the Purchaser or to any third party to whom the Purchaser sub-contracts or delegates (or tasks to act in pursuance of) any of its rights and obligations under this Contract (each such third party being a “Purchaser Third Party”. This assistance shall include:

23.1.1. providing such information about the manner in which the Contractor Deliverables are provided as is reasonably necessary for Purchaser Third Parties to provide their services and deliverables to the

Purchaser or carry out such activities as have been delegated to them by the Purchaser;

23.1.2. making available to, or accepting information from, Purchaser Third Parties (including, where appropriate and agreed with the Purchaser, through the development of interfaces or information exchanges between the Contractor and Purchaser Third Parties);

23.1.3. using its reasonable endeavours to prevent, resolve and limit the impact on the Purchaser of any disputes or disagreements between it and any Purchaser Third Parties; and

23.1.4. meeting with the Purchaser and Purchaser Third Parties to discuss the Contractor Deliverables and the services and deliverables provided by third parties.

23.2. Without limiting the Contractor's obligations, the Contractor shall inform the Purchaser of any disputes or disagreements between it and any of Purchaser Third Parties that may affect the provision of the Contractor Deliverables.

24. ACCESS TO PURCHASER'S PREMISES

24.1. The Contractor acknowledges that Purchaser premises to which it shall provide the Contractor Deliverables vary in physical size, occupancy levels and types.

24.2. The Contractor shall observe, and ensure that the Contractor's Team and Subcontractors observe, all health and safety rules and regulations and any other security requirements that apply at any of Purchaser's premises, including any the Purchaser policies and processes which may be communicated by the Purchaser to the Contractor.

25. CARE AND DILIGENCE OF PROPERTY – RISK OF LOSS

25.1. The Contractor shall use reasonable care to avoid damaging building, equipment, and vegetation (such as trees, shrub and grass) on the work site.

25.2. If the Contractor damages any such building or equipment, he shall repair the damage as directed by the Purchaser and at no expenses to the Purchaser. If he fails or refuses to make such repair or replacement, the Contractor shall be liable for the cost thereof, which may be deducted from the Contract price.

25.3. The Purchaser shall exercise due care and diligence for Contractor's and Purchaser's equipment, tools and materials at each site supplied and/or

used for the performance of this Contract. Notwithstanding anything to the contrary herein contained in this Contract, the Purchaser will not assume any liability for damages occurring to or occasioned by said equipment, tools and materials except for (i) gross negligence or wilful misconduct of the Purchaser or his servants, agents or subcontractors or (ii) loss due to events covered under Article 39 “Termination for Default” of Part III – Contract General Provisions.

26. RESPONSIBILITY OF THE CONTRACTOR TO INFORM EMPLOYEES OF WORK ENVIRONMENT

26.1. The Contractor shall inform his employees under this Contract of the terms of the Contract and the conditions of the working environment.

26.2. Specifically, personnel shall be made aware of all risks associated with the performance under this Contract, the conditions of site in which the performance is to take place and living conditions while performing within the boundaries of the Contract. The selection of adequate personnel shall remain sole responsibility of the Contractor.

27. INSPECTION AND ACCEPTANCE OF WORK

27.1. This Clause augments Clause 21 “Inspection and Acceptance of Work” of Part III – Contract General Provisions.

27.2. Should the Purchaser give the Contractor the opportunity, at the Contractor’s expense, to carry out remedial services as is necessary to correct the Contractor’s failure or otherwise to rectify any breach, these remedial services shall be completed within Purchaser-specified time limits.

27.3. The services to be provided by the Contractor's personnel under this Contract shall conform to the highest professional and industry standards and practices. Inspection of the services provided will be made by the Purchaser's Technical representatives or another authorised designee in accordance with the specifications in Part IV - SOW. Services performed by the Contractor which do not conform to the highest professional and industry standards may result in the Purchaser requesting that such work be performed again at no increase in the price of the contract. Repeated instances of work performed which fails to meet the standards and practices may result in termination of the Contract for Default.

27.4. This Clause 27 of Contract Special Provisions and Clause 21 of Contract General Provisions shall also apply to any remedial services carried out by the Contractor.

27.5. The Purchaser's rights and remedies under the Clause 27 of Contract Special Provisions and Clause 21 of Contract General Provisions are in addition to its rights and remedies under this Contract.

28. INVOICES AND PAYMENT

28.1. This Clause replaces Clause 25 "Invoices and Payment" of Part III - Contract General Provisions.

28.2. Following Purchaser acceptance, in writing, payment for supplies and services furnished shall be made in the currency specified for the relevant portion of the Contract. Invoices shall be accompanied by a copy of the letter of acceptance issued by the Purchaser. It shall be the responsibility of the Contractor to ensure such letter is provided.

28.3. The term of the Contract may not be exceeded without prior approval of the Purchaser. In no case will the Purchaser make payment above the total of the corresponding CLINs.

28.4. No payment will be made if CLIN items agreed for delivery before milestones are not complete as described in Part I - SSS and Part IV - SOW.

28.5. No payment shall be made with respect to undelivered supplies; works not performed, services not rendered and/or incorrectly submitted invoices.

28.6. No payment will be made for additional items delivered that are not specified in the contractual document.

28.7. The invoice amount shall be exclusive of VAT and exclusive of all Taxes and Duties as per Clause 26 Taxes and Duties, Part III – Contract General Provisions.

28.8. CLINs will be paid as below based on Purchaser milestone approval in writing.

28.9. The Purchaser is released from paying any interest resulting from any reason whatsoever.

28.10. The Purchaser shall not bear any liability related to financial guarantees, which the Contractor is required to provide under this Contract.

28.11. The Contractor shall render all invoices in a manner, which shall provide a clear reference to the Contract. Invoices in respect of any service and/or deliverable shall be prepared and submitted as specified hereafter and shall contain:

28.11.1. VAT number;

28.11.2. Contract number;

28.11.3. Contract Amendment number (if any);

28.11.4. Purchase Order number;

28.11.5. Contract Payment Milestone and CLINs as they are defined in Part I - SSS;

28.11.6. The address of the bank to which payment shall be made, together with **either** pertinent information concerning the International Bank Account Number (IBAN) and BIC/SWIFT address **or** pertinent information concerning transit number/sort code, account number and SWIFT address. The Purchaser makes payment only by wire transfer and therefore wire transfer particulars shall be included on the invoice.

28.11.7. The payment conditions in line with the Contract.

28.12. The invoice shall contain the following certificate which shall be signed by a duly authorised company official on the designated original:

"I certify that the above invoice is true and correct, that the delivery of the above described items has been duly effected and/or that the above mentioned services have been rendered and the payment therefore has not been received.

*Order placed for official use. Exemption from VAT Article 42,§3&3*of VAT Code for Belgium or Article 151, §1b of the Council Directive 2006/112/EC dd. 28 November 2006 on intra-community purchases and/or services.".*

28.13. Invoices shall be addressed to "NCI Agency - Financial Management" and submitted in electronic format only to: accountspayable@ncia.nato.int

AND

An electronic copy of the invoice shall be sent to the Purchaser's Contracting Authority, at the email address specified in the Clause 31 of the Contract Special Provisions.

28.14. NCI Agency will make payment within 45 days of receipt by NCI Agency of a properly prepared and documented invoice.

28.15. The approval for payment of a valid and undisputed invoice by the Purchaser shall not be construed as acceptance by the Purchaser of the performance of the Contractor's obligations nor as a waiver of its rights and remedies under this Contract.

28.16. The Contractor shall be entitled to submit invoices for accepted milestones as follows:

Payment Milestone	Description	CLIN	Percentage of Total Contract Price	Value
P1	MS 0 – Design Review Approved		15%	
P2	MS 1 – NPKI-M Reference Environment High Side MS 2 – NPKI-M Reference Environment Low Side	4.1, 4.2	20%	
P3	MS 3 - NPKI-M Production Environment High Side MS 4 - NPKI-M Production Environment Low Side	4.3, 4.4	20%	
P4	MS 5 - Final System Acceptance (FSA)	4.5	35%	
P5	End of Warranty Period	8.1	10%	

29. LIQUIDATED DAMAGES

29.1. This Clause augments Clause 38 "Liquidated Damages" of Part III - Contract General Provisions.

29.2. The amount of Liquidated Damages due by the Contractor shall be recovered by the Purchaser in the following order of priority:

a. By deducting such damages from the amounts due to the Contractor against the Contractor's invoices;

b. By proceeding against any surety or deducting from the Performance Guarantee, if any;

c. By reclaiming such damages through appropriate legal remedies.

30. TECHNICAL DIRECTION

30.1. The Contract will be administered by the NATO CI Agency in accordance with Clause 31 of these Contract Special Provisions entitled “Contract Administration”.

30.2. The individuals working on this Contract shall perform the effort within the general scope of work identified in the Contract Part IV - SOW. This effort will be directed on a more detailed level by the Purchaser’s Project Manager who will provide detailed tasking and instruction on how to proceed.

30.3. The Purchaser reserves its right to assign a Technical Representative who will provide the Contractor personnel with instruction and guidance, within the general scope of work, in performance of their duties and working schedule.

30.4. Neither the Purchaser’s Project Manager, as identified in Clause 31 of these Contract Special Provisions, nor any Technical Representative has the authority to change the terms and conditions of the Contract. If the Contractor has reason to believe that the Project Manager/Technical Representative is requesting effort on terms inconsistent with that in the scope of the Contract, the Contractor shall immediately inform the Purchaser’s Contracting Authority for confirmation of the actions. Failure to obtain confirmation that the action of the Project Manager is outside of the authority of the Contract shall render any subsequent claim null and void.

30.5. Upon receipt of such notification above, the Purchaser’s Contracting Authority will:

a. confirm the effort requested is within scope, or

b. confirm that the instructions received constitute a change and request a quotation for a modification of scope and/or price, or

c. rescind the instructions.

30.6. Failure of the Contractor to notify the Purchaser of direction constituting change of the Contract will result in a waiver of any claims pursuant to such change.

31. CONTRACT ADMINISTRATION

31.1. The Purchaser reserves the right to re-assign this contract to a representative(s) for administrative purposes, in whole or in part, provided that the Purchaser shall always be responsible for his obligations under

the contract and for actions or lack of actions of its assigned administrator. The Purchaser undertakes to advise the Contractor in writing whenever this right is to be exercised.

31.2. The Purchaser is the NATO Communications and Information Agency (NCI Agency). The NCI Agency is the Point of Contact for all Contractual and Technical issues. The Contractor shall accept Contract modifications only in writing from the Purchaser's Contracting Authority.

31.3. All notices and communications between the Contractor and the Purchaser shall be written and conducted in English. Contract modifications only become valid when received in writing from the General Manager, NCI Agency, or his authorized representative.

31.4. Formal letters and communications shall be personally delivered or sent by e-mail, mail, registered mail, courier or other delivery service, to the official points of contact quoted in this Contract. Telefax or other electronic means may be used to provide an advance copy of a formal letter or notice which shall subsequently be delivered through the formal communications means.

31.5. Informal notices and informal communications may be exchanged by any other communications means including telephone and e-mail.

31.6. All notices and communications shall be effective upon receipt.

31.7. Official Points of Contact are:

PURCHASER

Contractual issues:

NCI Agency
Acquisition
Boulevard Léopold III
B-1110 Brussels
Belgium

POC: Ms Sumiko Duncan
Tel: +32 2 360 4180
E-mail: sumiko.duncan@ncia.nato.int

Technical issues:

NCI Agency
NATO Cyber Security Centre
Building 100
B-7010 SHAPE, Mons
Belgium

POC: Mr Miles Knight
Tel: +31 70 374 3527
E-mail: miles.knight@ncia.nato.int

CONTRACTOR

Contractual issues:

To be confirmed

Technical issues:

To be confirmed

32. LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION

32.1. Definitions. As used in this Clause:

32.1.1. Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized Media may have occurred.

32.1.2. Controlled Technical Information means Technical Information with NATO military application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions.

32.1.3. Covered defense information means unclassified Controlled Technical Information and is:

32.1.3.1. Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of the NCI Agency in support of the performance of the contract; or,

32.1.3.2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

32.1.4. Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

32.1.5. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

32.1.6. Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

32.1.7. Technical Information means technical data or computer software such as research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

32.2. Restrictions

32.2.1. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third party's reporting of a cyber-incident:

32.2.1.1. The Contractor shall access and use the information only for furnishing advice or technical assistance directly to the Purchaser in support of the Purchaser's activities, and shall not be used for any other purpose.

32.2.1.2. The Contractor shall protect the information against unauthorized release or disclosure.

32.2.1.3. The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this Clause prior to the employees being provided access to or use of the information.

32.2.1.4. The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Purchaser and Contractor.

32.2.1.5. A breach of these obligations or restrictions may subject the Contractor to:

32.2.1.5.1. Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies; and

32.2.1.5.2. Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this Clause.

33. CYBER INCIDENT REPORTING

33.1. **Definitions**. As used in this clause—

33.1.1. “Contractor attributional/proprietary Information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

33.1.2. “Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

33.1.3. “NATO Information” means as defined in clause, Basic Safeguarding of Contractor Communication Information Systems (CIS).

33.1.4. “Cyber incident” means any detected anomaly compromising, or that has the potential to compromise, communication, information or other electronic systems or the information that is stored, processed or transmitted in these systems.

33.1.5. “Forensic analysis” means the practice of gathering, retaining, and analyzing computer- related data for investigative purposes in a manner that maintains the integrity of the data.

33.1.6. “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

33.1.7. “Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

33.1.8. “Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which NATO Information is recorded, stored, or printed within a contractor CIS.

33.2. **Cyber incident reporting requirement.**

33.2.1.1. When the Contractor discovers a cyber incident that affects a contractor CIS or NATO Information residing therein, or that affects the

contractor's ability to perform the requirements of the contract, the Contractor shall—

33.2.1.2. Conduct a review for evidence of compromise of the NATO Information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing contractor CIS that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised NATO Information, or that affect the Contractor's ability to perform the requirements of the contract; and,

33.2.1.3. Report the cyber incident(s) to the Contracting Officer within 72 hours of discovery of any cyber incident.

33.3 **Cyber incident report**. The cyber incident report shall be treated as information created by or for the Purchaser and shall include, at a minimum, the following content:

- Company name
- Facility Clearance Level
- Company point of contact information (name, position, telephone, email)
- NCI Agency Project Manager point of contact (name, position, telephone, email)
- Contract number(s) or other type of agreement affected or potentially affected
- Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
- Contract or other type of agreement classification level
- Impact to NATO Information and/or provided products/services
- Ability to provide operational support
- Date incident discovered
- Location(s) of compromise
- NATO programs, platforms or systems involved
- Classification of the systems involved
- Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
- Description of technique or method used in the cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)

- Incident/Compromise narrative (Ex: Chronological explanation of event/incident, threat actor TTPs, indicators of compromise, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred) Include in this section what actions have been taken to mitigate the risk/damage of both hardware and software assets.
- Confirm whether news media are already aware/informed of the incident
- Any additional information

33.3.1 Subject to the Purchaser's consultation with the contractor's national cyber defence authority and/or as prescribed in the contractor's nation's Memorandum of Understanding (MoU) on Cyber Defence with NATO, the Purchaser reserves the right to request the following:

33.3.2 **Malicious software**. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, inform the Contracting Officer to allow the Purchaser to request the malicious software or decline interest. Do not send the malicious software to the Contracting Officer.

33.3.3 **Media preservation and protection**. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph 33.2.1.1 of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow the Purchaser to request the media or decline interest.

33.3.4 **Access to additional information in support of an incident investigation.** Upon request by the Purchaser, the Contractor shall provide the Purchaser with access to additional information that is necessary to conduct an incident investigation**.**

33.3.5 **Cyber incident damage assessment activities**. If the Purchaser elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph 33.4 of this clause.

33.4 **Information Handling**. The Purchaser shall protect information reported or otherwise provided to the Purchaser under this clause that includes contractor attributional/proprietary information in accordance with applicable NATO policies. To the maximum extent practicable, the Contractor shall identify and mark contractor attributional/proprietary information. The Purchaser may use contractor attributional information and disclose it only for purposes and activities consistent with this clause. The Purchaser will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such an authorized release, seeking to include only that information

that is necessary for the authorized purpose(s) for which the information is being released.

33.5 The Contractor shall conduct activities under this clause in accordance with applicable NATO regulations and contractor national laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

33.6 **Other reporting requirements**. The cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other cyber incident reporting as required by other applicable clauses of this contract, or as a result of other applicable NATO regulations or contractor national law or regulatory requirements.

33.6.1 **Subcontracts**. The Contractor shall—

33.6.1.1 Include this clause, including this paragraph 33.6.1.1, in subcontracts, or similar contractual instruments, for which subcontract performance will involve NATO Information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as NATO Information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and,

33.6.1.2 Require subcontractors to provide a copy of the incident report to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to the Purchaser as required in paragraph 33.2 of this clause.

34. NCI AGENCY SUPPLIER CODE OF CONDUCT

34.1. The NCI Agency has a Supplier Code of Conduct located at https://www.ncia.nato.int/business/do-business-with-us/code-of-conduct.html and it constitutes part of this Contract.

34.2. This Supplier Code of Conduct sets standards and practices for suppliers and their subcontractors to adhere to when doing business with the NCI Agency in the areas of labour rights, human rights, data protection, ethical conduct and the environment. It contains fundamental, basic principles that any supplier based in a NATO country should already be operating in compliance with.

34.3. In the event of any inconsistency in language, terms or conditions with the Contract General Provisions, the Contract General Provisions takes precedence.

35. REACH CAPABILITY

35.1. The purpose of this Article is to define the conditions under which specific Purchaser provided REACH capability is made available to the Contractor in the execution of this Contract.

35.2. The provision of the REACH capability is governed by the General Provisions, Article 13, Purchaser Furnished Property, Article 35 and Annex B to the Special Provisions.

35.3. Should the Purchaser not be able to meet the SLA related to the provision of the REACH capability as laid down in Annex B of these Special Provisions, the Contractor shall not be entitled to claim an excusable delay nor any compensation against any Articles for the Performance of this Contract and its Amendments.

36. LIMITATIONS ON THE USE OR DISCLOSURE OF PURCHASER FURNISHED INFORMATION (PFI)

36.1. *Definitions.* As used in this clause, “Purchaser Furnished Information” includes

Contractor-acquired information, which means information acquired or otherwise collected by the Contractor on behalf of the Purchaser in the context of the Contractor's duties under the contract.

Purchaser Furnished Information (PFI), which means information in the possession of, or directly acquired by, the Purchaser and subsequently furnished to the Contractor for performance of a contract. PFI also includes contractor- acquired information if the contractor-acquired information is a deliverable under the contract and is for continued use under the contract. Otherwise, PFI does not include information that is created by the Contractor and delivered to the Purchaser in accordance with the requirements of the work statement or specifications of the contract. The type, quantity, quality, and delivery requirements of such deliverable information are set forth elsewhere in the contract schedule.

36.2. *Information Management and Information*

36.2.1. The Contractor shall manage, account for, and secure all PFI provided or acquired by the contractor in accordance with the special provisions clause, “Basic Safeguarding of Contractor Communication and Information Systems (CIS)”. The Contractor shall be responsible for all PFI provided to its subcontractors.

36.2.2.

36.3. *Use of PFI*

36.3.1. The Contractor shall not use any information provided or acquired under this contract for any purpose other than in the performance of this contract.

36.3.2. The Contractor shall ensure that its employees are subject to use and non- disclosure obligations consistent with this clause prior to the employees being provided access to or use of any PFI covered by this clause.

36.4. *Information alteration and disposal*

36.4.1. Except as otherwise provided for in this contract, the Contractor shall not alter, destroy, or otherwise dispose of any PFI unless expressly directed by the Contracting Officer to do so.

36.5. *Subcontracts*

36.5.1. The Contractor shall include the substance of this clause in subcontracts under this contract for the acquisition of commercial products or services in which the subcontractor may have access to PFI).

ANNEX A: NATO CI AGENCY NON-DISCLOSURE DECLARATION

We, the undersigned ……(Company) duly represented by the named individual below (hereinafter "Contractor") do hereby certify that we shall ensure that the following conditions be accepted and observed by all (Contractor) employees working under CO-115518-NPKI-M.

_____

Date Full name (in block capitals) Signature

TO BE SIGNED BY THE CONTRACTOR'S EMPLOYEES WORKING IN THE NATO'S PREMISES UPON COMMENCEMENT OF THEIR WORK.

I UNDERSTAND:

That I must preserve the security of all classified /commercial-in-confidence information which comes to my knowledge as a result of this contract with NATO and that I undertake to comply with all relevant security regulations.

That I must not divulge to any unauthorized person, any classified/commercial-in confidence information gained by me as a result of my contract with NATO, unless prior permission for such disclosure has been granted by the General Manager of the NCI Agency or by his designated representative.

That I must not, without the approval of the General Manager of the NCI Agency, publish (in any document, article, book, CD, video, film, play, or other form) any classified /commercial-in-confidence information which I have acquired in the course of my work under CO-115518-NPKI-M.

That, at the end of contract and after performance of all required tasks, I must surrender any official document or material made or acquired by me in the course of my work under CO-115518-NPKI-M, save such as I have been duly authorized to retain.

That the provisions of the above Declaration apply not only during the period of work under CO-115518-NPKI-M, but also after my contract has ceased and that I am liable to prosecution if either by intent or negligence I allow classified/commercial-in-confidence information to pass into unauthorized hands.

ANNEX B: SERVICE LEVEL AGREEMENT (SLA) FOR THE PROVISION OF REACH LAPTOPS IN ACCORDANCE WITH ARTICLE 35 OF THE CONTRACT SPECIAL PROVISIONS

Introduction

To improve collaboration between the Contractor and the Purchaser teams, a collaborative environment for the two teams will be established that will provide the ability to process, store and handle information up to and including NATO RESTRICTED (NR). Access to the collaborative environment is provided to the Contractor's Team via the Purchaser NR capability (informally called REACH). This capability will be complemented by a limited access to the Purchaser's Project Portal.

Parties

The REACH capability will be provided by the Purchaser to support the Contractor Team under Contract No CO-115518-NPKI-M.

General Overview

This is an agreement between the Purchaser and the Contractor under this Contract to establish the:

• Provision of REACH capability for the Contractor Team;

• General levels of response, availability, and maintenance associated with the REACH capability;

• Respective responsibilities of the Purchaser and the Contractor Team.

These provisions shall be in effect for an initial period of three years from the effective date of the Contract or until the end of Contract CO-115518-NPKI-M, whichever occurs first. It can be extended based on a mutual agreement between the Parties.

Provided Capability

References

https://dnbl.ncia.nato.int/Pages/ServiceCatalogue/CPSList.aspx

(WPS006, WPS003, WPS008 services)

The Purchaser accepts no liability and provides no warranty in respect of the third party software mentioned above. It is emphasized that the REACHs can only be used by the Contractor's Team within the limits set out in this project description.

Scope

• As described in reference Service Descriptions above.

Aim

The REACH capability enables exchanges of information and collaboration up to and including NR classification.

Limitations

• The use of the REACH capability requires a NATO Security clearance at NATO SECRET level. Proof of the users' security clearances will be provided to the Purchaser.

• The exchange and collaboration of information is provided through e-mail and Instant Messaging.

• Direct printing capability is not provided, but can be arranged through an extension of this contract requested by the Contractor's Team.

• In case of any problems which cannot be solved remotely from the service desk (The Hague, NLD), the equipment shall be sent to NCIA, The Hague at the Contractor's expenses. Any damages resulting from inappropriate operation or operation in harsh environment or adverse weather conditions, as well as a loss of the system shall be compensated by the Contractor.

• A maximum of two users can be configured to share one REACH laptop capability.

Assumptions

The following assumptions apply to this Agreement:

• Any support provided by Purchaser is documented in the service descriptions above

• Security violations of the non-NCIA REACH users are investigated through their local security officers/managers applying NATO rules (CM(2002)49, NCIA (CapDev)AD3-2, and NCIA(CapDev)NR SECOPS).

• Required changes to this Agreement and/or the provision of the REACH capability will be jointly assessed and the implementation agreed between the Parties. The implementation of changes may have an impact on the charges which will be handled through an update of this Agreement.

Roles and Responsibilities

The roles and responsibilities for the provision of the REACH capability are defined in the referenced Service Description, but summarized also herein:

• Contractor Team will receive 4 REACH terminal.

• The Purchaser will provide the REACH capability and related services.

Points of Contact

• As described in the service descriptions above (WPS008 Service Desk).

Purchaser's responsibilities

The Purchaser will:

• Provide to the Purchaser the necessary documentation required for the activation of user accounts and certifications;

• Provide the REACH capability including basic end-user training (1.5-hour duration) and deliver the REACH laptop(s);

• Set up and maintain the project web-portal at NR level;

• Provide introduction to the management of the portal (1-2 hours) and service desk for the portal on-site at NCIA, The Hague or through electronic media;

• Grant temporary use of REACH hardware and the software licences for the contracted period.

Contractor Team Responsibilities

The Contractor Team shall:

• Sign and return to the Purchaser the required security documentation;

• Provide the internet access required for Remote Access via NCIA REACH;

• Be responsible for the backup of files and data of the REACH on NR accredited media on an authorized Removable Storage Device provided by service provider;

• Ensure that Contractor personnel operating the REACH units possess security clearance of a minimum of NS;

• Provides Security clearance for up to and including NS for the personnel using the REACH capability;

• Provides the contact details of the local Security Officer/Manager and the commitment to apply NATO rules as defined in (CM(2002)49, NCIA (CapDev)AD3-2, and NCIA(CapDev)NR SECOPS)for the investigation;

• Return the equipment at the end of the Agreement at its expenses to the Purchaser;

• Not use the equipment for any other purposes than the purpose set out herein;

• Not lend, rent, lease and/or otherwise transfer the equipment to a third party;

• Not copy or reverse engineer the equipment.

Hours of Coverage, Response Times & Escalation

• As described in the service descriptions above.

Incidents

• As described in the service descriptions above.

• Resolution of disagreements

In case of disagreements, all disputes shall be resolved by consultation between the Parties and shall not be referred to any national or international tribunal or other third party for settlement.

Changes

• For any changes of the REACH capability which will be required to be made during the term of this Agreement, the Purchaser will notify the Contractor CISAF Team at least one week prior to the event and inform about the required consequences.

• Any changes concerning the elements provided by the Contractor Team shall be communicated to the NCIA Service Desk at least one week prior to the event.

Maintenance

Use of the REACH capability and/or related components require regularly scheduled maintenance (“Maintenance Window”) performed by the Purchaser. These activities will render systems and/or applications unavailable for normal user interaction as published in the maintenance calendar. Users will be informed of the maintenance activities with sufficient notice.

[End of Agreement]

ANNEX C: SECURITY ASPECTS LETTER (SAL), INCLUDING COMPREHENSION AND ACCEPTANCE OF THE SECURITY ASPECTS LETTER (SAL)

1. In the performance of this contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the work is performed or in the contracts involving NR information only as established in the contract's Statement of Work (SoW) requirement entitled, "Safeguarding of NATO Restricted Information".

2. All classified information and material shall be protected in accordance with the requirements established by the NSA/DSA of the nation in which the work is performed or in the case of NR information as may also be established in the Safeguarding of NATO Restricted Information Requirement.

3. In particular, the Contractor shall:

(a) appoint an officer to be responsible for supervising and directing security measures in relation to the solicitation, contract or sub- contract;

(b) submit in due time to the NSA/DSA the personal particulars of the person the contractor wishes to employ on the project with a view to obtaining PSCs at the required level where NC and above is involved;

(c) maintain, preferably through this officer responsible for security measures, a continuing relationship with the NSA/DSA and / or the Contracting Authority in order to ensure that all NATO classified information involved in the bid, contract or sub-contract is properly safeguarded;

(d) limit the copying of any classified materiel (including documents) to the absolute minimum to perform the contract;

(e) supply the NSA/DSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information;

(f) maintain a record of his employees taking part in the project and who have been cleared for access to NATO classified information. This record must show the period of validity and the level of the clearances;

(g) deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DSA or in the case of NR information as determined by the need-to-know;

(h) limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub- contract;

(i) comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information, and that they recognise that they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

(j) report to the Security Officer and to his NSA/DSA any breaches or suspected breaches of security, suspected sabotage or subversive activity, any breach giving rise to doubts as to the trustworthiness of an employee, any changes in the ownership, supervisory or managerial staff of the facility or any changes that affect the security arrangements and

security status of the facility, and any other information which may be required by the NSA/DSA, such as reports on holdings of NATO classified information or materiel;

(k) obtain the approval of (programme/project office and NSA/DSA) before beginning negotiations with a view to sub-contracting any part of the work which would involve the Sub-contractor having possible access to NATO classified information, and to place the Sub-contractor under appropriate security obligations which in no case may be less stringent than those provided for his own contract;

(l) undertake not to utilise, other than for the specific purpose of the bid, contract or sub-contract, without the written permission of (programme/project office) or the prime Contractor, any NATO classified information supplied to him, and return to (programme/project office) all classified information referred to above, as well as that developed in connection with the contract or sub-contract unless such information has been destroyed, or its retention has been duly authorised by the contracting office or the sub-contracting officer. Such NATO classified information shall be returned at such time as the contracting office may direct; and

(m) comply with any procedure established with respect to the dissemination of NATO classified information in connection with the contract or sub-contract.

(n) Any person taking part in the performance of work the classified parts of which are to be safeguarded, must possess the appropriate NATO security clearance issued by his NSA/DSA. The level of this clearance must be at least equal to the security category of the materiel, the related information or specifications where NC or above is involved.

(o) Unless specifically authorised to do so by (programme/project office), the Contractor may not pass on any NATO classified information to any third party to whom a request to supply goods or services has been submitted.

(p) No change in level of classification or de-classification of documentation or materiel may be carried out unless written authority in this respect is obtained from (programme/project office).

(q) No CIS may be used for processing classified information without prior accreditation by the responsible authorities. At the level of NR, such accreditation can be under delegated authority of the responsible accreditation authority or the contracting authority in accordance with Special Provisions clause entitled, “Safeguarding of NATO Restricted Information.

(r) Failure to implement these provisions and the security regulations established by the NSA of the nation where the contractual work is being performed may result in termination of this contract without reimbursement to the Contractor or claim against NATO, (programme/project office) or the national government of the said nation.

(s) The (programme/project office) security classification check list indicates the degree of classification of the data and materiel (equipment, information, technical manuals, specifications) which may be handled in the performance of work under this contract and which must be safeguarded in accordance with the provisions of this letter.

(t) The contractor shall destroy or return any classified information provided or generated under the contract unless the contracting authority has given written approval to retain such classified information, e.g. for warranty purposes.

(u) The Contractor shall be required to acknowledge receipt of an accompanying SAL or Program Security Instruction (PSI) that is made part of the applicable contract and confirm

that it understands the security aspects defined. With respect to contracts involving only NR information the Contractor shall also be required to confirm that it will comply with the provisions of the Safeguarding of NATO Restricted Information Requirement provided in Book II, Statement of Work and specifically that any company CIS used to handle or process NR classified information has been appropriately security accredited.

Comprehension and Acceptance of the Security Aspect Letter (SAL)

The Bidder hereby acknowledges receipt of the SAL letter in relation to the NATO Restricted Information that will be handled during the Contract Administration Phase of Contract number CO-115518-NPKI-M and certifies:

a.) full comprehension of the security aspects defined in the SAL and compliance with the provisions of the Safeguarding of NATO Restricted Information requirement provided in Book II, Statement of Work; and,

b.) any company CIS used to handle or process NR classified information has been appropriately security accredited.

…….…… .....

Date Signature of Authorised Representative

…….....

Printed Name and Title

…….....

Company

NATO COMMUNICATIONS AND INFORMATION AGENCY

CONTRACT GENERAL PROVISIONS

V 1.0 dated 16 Oct 2014

Index of Clauses

The Contract General Provisions

1. ORDER OF PRECEDENCE

In the event of any inconsistency in language, terms or conditions of the various parts of this Contract, precedence will be given in the following order:

1.1. The Signature Page;

1.2. The Contract Schedules, Part I;

1.3. The Contract Contract Special Provisions, Part II;

1.4. The Contract General Provisions, Part III;

1.5. The Statement of Work, Part IV of the Contract;

1.6. The Annexes to the Statement of Work.

2. DEFINITIONS OF TERMS AND ACRONYMS

2.1 ***Assembly***- An item forming a portion of equipment that can be provisioned and replaced as an entity and which normally incorporates replaceable parts or groups of parts.

2.2 ***Acceptance-*** Acceptance is the act by which the Contracting Authority recognises in writing that the delivered Work meets the Contract requirements..

2.3 ***Claims-*** A written demand or written assertion by one of the Parties seeking, as a matter of right, the payment of money in a sum certain, the adjustment or interpretation of Contract terms, or other relief arising under or in relation to this Contract.

2.4 ***Clause-*** A provision of the Special or General Provisions of this Contract.

2.5 ***Codification Authority-*** The National Codification Bureau (NCB) or authorised agency of the country in which the Work is produced.

2.6 ***Commercial Off-the-Shelf Items (COTS)-*** The term “Commercially Off-the-Shelf Item (COTS)” means any item that:is a commercial item, customarily used by the general public, that has been sold, leased, or licensed to the general public or has been offered for sale, lease or license to the general public;

a) is sold in substantial quantities in the commercial marketplace; and

b) is offered to the Purchaser, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.

2.7 ***Component-*** A part or combination of parts, having a specific function, which can be installed or replaced only as an entity.

2.8 ***Contractor Background IPR-*** Any IPR owned by the Contractor and/or any Sub-contractor or licensed by a third party to the Contractor which is not created in relation to or as the result of work undertaken for any purpose contemplated by the Contract and which is needed for the performance of the Contract or for the exploitation of Foreground IPR.

2.9 ***Correction-*** Elimination of a Defect.

2.10 ***Contract-*** The agreement concluded between the Purchaser and Contractor, duly signed by both contracting parties. The Contract includes the documents referred to in Clause 1 (Order of Preference).

2.11 ***Contracting Authority-*** The General Manager of the NCI Agency, the Director of Acquisition, the Chief of Contracts of the NCI Agency or the authorised representatives of the Chief of Contracts of the NCI Agency.

2.12 ***Contractor-*** The person or legal entity from a Participating Country which has signed this Contract and is a Party thereto.

2.13 ***Day-*** A calendar day

2.14 ***Defect-*** Any condition or characteristic in any Work furnished by the Contractor under the Contract that is not in compliance with the requirements of the Contract.

2.15 ***Deliverable-*** Any and all goods (including movable and immovable goods) to be delivered pursuant to the terms of this Contract including, without limitation, building, raw materials, components, intermediate Assemblies, Parts, end products, equipment, documentation, data, software.

2.16 ***Design Defect-*** Defect attributable to incompatibility, unsuitability or erroneous application of theory, drawings or formula.

2.17 ***Effective Date of Contract (or "EDC")-*** The date upon which this Contract is deemed to start. Unless otherwise specified, a Contract enters into force on the date of the last signature of the Contract by the Parties.

2.18 ***Failed Component-*** A part or combination of parts, having a specific function, which can be installed or replaced only as an entity which ceases to perform in a manner consistent with its intended use and specifications of the Contract.

2.19 ***Foreground IPR*** - Any IPR created by the Contractor or any subcontractor of the Contractor in the course of or as the result of work undertaken for any purpose contemplated by the Contract.

2.20 ***IPR-*** Any intellectual property rights of any qualification irrespective of their stage of development or finalisation, including but not limited to patents, trademarks (registered of not), designs and models (registered or not) and applications for the same, copyright (including on computer software), rights in databases, know-how, confidential information and rights in records (whether or not stored on computer) which includes technical and other data and documents.

2.21 ***Manufacturing Defect-*** Defect attributable to improper manufacturing processes, testing or quality control procedures.

2.22 ***NATO-*** The North Atlantic Treaty Organisation. For the purpose of this contract, the term NATO includes NATO bodies, the NATO military command structure, agencies and NATO nations.

2.23 ***NCI AGENCY-*** The NATO Communications and Information Agency. The NCI Agency is part of the NCIO. The General Manager of the Agency is authorised to enter into contracts on behalf of the NATO CI Organisation.

2.24 ***NATO COMMUNICATIONS AND INFORMATION ORGANISATION (NCIO)-*** The NATO Communications and Information Organisation. The NCI Organisation constitutes an integral part of the North Atlantic Treaty Organisation (NATO) The NCI Organisation is the legal personality from whence flows the authority of its agent, the NCI Agency, to enter into contracts.

2.25 ***NATO Purposes-*** Activities conducted by or on behalf of NATO to promote the common defence and common interests of NATO, such as, among others, NATO operations, NATO procurement, NATO training and NATO maintenance.

2.26 ***Part-*** An item of an assembly or sub-assembly, which is not normally further broken down.

2.27 ***Participating Country-*** A NATO member country that participates in financing the effort.

2.28 ***Parties-*** The Contracting Parties to this Contract, i.e., the Purchaser and the Contractor.

2.29 ***Purchaser***- The NCI Organisation, as represented by the General Manager, NCI Agency. The Purchaser is the legal entity who awards and administers the Contract on behalf of NATO and stands as one of the Contracting Parties.

2.30 ***Purchaser Background IPR-*** Any IPR owned by the Purchaser as of the Effective Date of Contract and which has been developed by, assigned to or licensed to the Purchaser prior to the Effective Date of Contract.

2.31 ***Purchaser Furnished Property-*** Any item of equipment, material, document, technical data, information and Software or any other item of property furnished by the Purchaser to the Contractor required or useful for the performance of the Contract. The Purchaser Furnished Property, if any, shall be detailed in the Contract.

2.32 ***Software (Computer Software)-*** A computer program comprising a series of instructions, rules, routines regardless of the media in which it is recorded, that allows or cause a computer to perform a specific operation or a series of operations.

2.33 ***Software Defect-*** Any condition or characteristic of Software that does not conform with the requirements of the Contract.

2.34 ***Sub-Assembly-*** A portion of an Assembly consisting of two or more parts that can be provisioned and replaced as an entity. The definition purposely excludes Components and/or Parts.

2.35 ***Sub-contract-*** Any agreement made by the Contractor with any third party in order to fulfil any part of the obligations under this Contract. Sub-contracts may be in any legal binding form, *e.g.*, contract, purchase order, etc.

2.36 ***Sub-contractor-*** Any person or legal entity directly or indirectly under Sub-contract to the Contractor in performance of this Contract.

2.37 ***Third Party IPR-*** Any IPR owned by a third party not being the Purchaser or the Contractor or its Subcontractor, which is needed for the performance of the Contract or for the exploitation of Foreground IPR. This includes, for example, third party software, including open source software.

2.38 ***Work-*** Any deliverable, project design, labour or any service or any other activity to be performed by the Contractor under the terms of this Contract.

3. AUTHORITY

3.1. All binding contractual instruments and changes, including amendments, additions or deletions, as well as interpretation of and instructions issued pursuant to this Contract shall be valid only when issued in writing by the Purchaser and signed by the Contracting Authority only.

3.2. No direction which may be received from any person employed by the Purchaser or a third party shall be considered as grounds for deviation from any of the terms, conditions, specifications or requirements of this Contract except as such direction may be contained in an authorised amendment to this Contract or instruction duly issued and executed by the Contracting Authority. Constructive change may not be invoked by the Contractor as a basis for Claims under this Contract.

3.3. The entire agreement between the Parties is contained in this Contract and is not affected by any oral understanding or representation, whether made previously to or subsequently to this Contract.

3.4. Personal notes, signed minutes of meetings, comments to delivered documentation and letters, e-mails and informal messages from project or other Purchaser staff which may indicate the intent and willingness to make changes to the Contract, do not implement the change to the Contract and shall not be used as a basis for claiming change to the Contract by the Contractor.

4. APPROVAL AND ACCEPTANCE OF CONTRACT TERMS

4.1. By his signature of the Contract, the Contractor certifies that he has read and unreservedly accepts and approves of all terms and conditions, specifications, plans, drawings and other documents which form part of and/or are relevant to the Contract. The Contractor further agrees that the terms of the Contract take precedence over any proposals or prior commitments made by the Contractor in order to secure the Contract. Contractor also hereby waives any and all rights to invoke any of the Contractor's general and special terms and conditions of sales and/or supply.

5. LANGUAGE

5.1. All written correspondence, reports, documentation and text of drawings delivered to the Purchaser by the Contractor shall be in the English language.

6. AUTHORISATION TO PERFORM/CONFORMANCE TO NATIONAL LAWS AND REGULATIONS

6.1. The Contractor warrants that he and his Sub-contractors are duly authorised to operate and do business in the country or countries in which this Contract is to be performed and that he and his Sub-contractors have obtained or will obtain all necessary licences and permits required in connection with the Contract. No claim for additional monies with respect to any costs or delay to obtain the authorisations to perform shall be made by the Contractor.

6.2. The Contractor acknowledges that he and his Sub-contractors are responsible during the performance of this Contract for ascertaining and complying with all applicable laws and regulations, including without limitation: labour standards, environmental laws, health and safety regulations and export controls laws and regulations in effect at the time of Contract signature or scheduled to go into effect during Contract performance. Failure to fully ascertain and comply with such laws, regulations or standards shall not be the basis for claims for change to the specifications, terms, conditions or monetary value of this Contract.

7. FIRM FIXED PRICE CONTRACT

7.1 This is a Firm Fixed Price Contract. The Firm Fixed Price of this Contract is as stated on the signature page of the Contract or any amendments thereto. The Purchaser assumes no liability for costs incurred by the Contractor in excess of the stated Firm Fixed Price except as may be authorised under certain provisions of this Contract.

8. PERFORMANCE GUARANTEE

8.1. As a guarantee of performance under the Contract, the Contractor shall deposit with the Purchaser within thirty (30) calendar days from the Effective Date of Contract a bank guarantee (the "Performance Guarantee") denominated in the currency of the Contract, to the value of ten per cent (10%) of the total Contract price.

8.2. The Performance Guarantee, the negotiability of which shall not elapse before the expiration of the warranty period, or such other period as may be specified in the Contract, shall be made payable to the Purchaser and shall be in the form of certified cheques or a Standby Letter of Credit subject to the agreement of the Purchaser. In the case of a Standby Letter of Credit, payment shall be made to the Purchaser without question and upon first demand by the Purchaser against a certificate from the Purchaser's Contracting Authority that the Contractor has not fulfilled its obligations under the Contract. The Contractor shall have no right to enjoin or delay such payment.

8.3. Certified Cheques issued to fulfil the requirements of the Performance Guarantee will be cashed by the Purchaser upon receipt and held in the Purchaser's account until the term of the Performance Guarantee has expired.

8.4. The standby letter of credit shall be subject to Belgian Law and shall be issued by (i) a Belgian bank, (ii) the Belgian subsidiary of a foreign bank licensed to provide financial services in Belgium; or (iii) an insurance company licensed to do business in Belgium and belonging to a Belgian banking institution provided the banking institution guarantees explicitly the demand for payment, unless otherwise specified by the Purchaser.

8.5. The Contractor shall request in writing relief from the Performance Guarantee upon expiration of the warranty period or such other period as may be specified in the Contract and such relief may be granted by the Purchaser.

8.6. The Contractor shall be responsible, as a result of duly authorised adjustments in the total contract price and/or period of performance by the Purchaser, for obtaining a commensurate extension and increase in the Performance Guarantee, the value of which shall not be less than ten per cent (10%) of the total contract price (including all amendments), and for depositing such guarantee with the Purchaser, within thirty (30) calendar days from the effective date of aforesaid duly authorised adjustment.

8.7. The failure of the Contractor to deposit and maintain such Performance Guarantee with the Purchaser within the specified time frame, or any extension thereto granted by the Purchaser's Contracting Authority, is a material breach of the Contract terms and conditions subject to the

provisions of the Contract regarding Termination for Default.

8.8. The rights and remedies provided to the Purchaser under the present Clause are in addition to any other rights and remedies provided by law or under this Contract. The certificate described in Clause 8.2 above shall not be regarded as a Termination for Default and this Clause is in addition to and separate from the Clause of the Contract detailing termination for default.

8.9. If the Contractor elects to post the Performance Guarantee by Standby Letter of Credit, the form of the document shall be substantially as follows:

PERFORMANCE GUARANTEE STANDBY LETTER OF CREDIT

Standby Letter of Credit Number: _____

Issue Date: _____

Initial Expiry Date: _____

Final Expiry Date: _____

Beneficiary: NCI Agency, Finance, Accounting & Operations
Boulevard Leopold III, B-1110, Brussels
Belgium

1. We hereby establish in your favour our irrevocable standby letter of credit number {number} by order and for the account of (NAME AND ADDRESS OF CONTRACTOR) in the amount of _____. We are advised this undertaking represents fulfilment by (NAME OF CONTRACTOR) of certain performance requirements under Contract No. _____ dated _____ between the NCI Agency ("NCIA and (NAME OF CONTRACTOR).

2. We hereby engage with you that drafts drawn under and in compliance with the terms of this letter of credit will be duly honoured upon presentation of documents to us on or before the expiration date of this letter of credit.

3. Funds under this letter of credit are available to you without question or delay against presentation of a certificate signed by the NCI Agency Contracting Officer which states:

> "(NAME OF CONTRACTOR) has not fulfilled its obligations under Contract No. _____ dated _____ between NCI Agency and (NAME OF CONTRACTOR) (herein called the "Contract"), and the NCI Agency, as beneficiary, hereby draws on the standby letter of credit number _____ in the amount denominated in the currency of the Contract, Amount up to the maximum available under the LOC), such funds to be transferred to the account of the Beneficiary

number _____(to be identified when certificate is presented)."

Such certificate shall be accompanied by the original of this letter of credit.

4. This Letter of Credit is effective the date hereof and shall expire at our office located at ____(Bank Address)_____ on _____. All demands for payment must be made prior to the expiry date.

5. It is a condition of this letter of credit that the expiry date will be automatically extended without amendment for a period of one (1) year from the current or any successive expiry date unless at least 90 (ninety) calendar days prior to the then current expiry date we notify you by registered mail and notify (NAME OF CONTRACTOR) that we elect not to extend this letter of credit for such additional period. However, under no circumstances will the expiry date extend beyond _____ ("Final Expiry Date") without amendment.

6. We may terminate this letter of credit at any time upon 90 (ninety) calendar days notice furnished to both (NAME OF CONTRACTOR) and the NCI Agency by registered mail.

7. In the event we (the issuing bank) notify you that we elect not to extend the expiry date in accordance with paragraph 6 above, or, at any time, to terminate the letter of credit, funds under this credit will be available to you without question or delay against presentation of a certificate signed by the NCI Agency Contracting Officer which states:

"The NCI Agency has been notified by {issuing bank} of its election not to automatically extend the expiry date of letter of credit number {number} dated {date} pursuant to the automatic renewal clause (or to terminate the letter of credit). As of the date of this certificate, no suitable replacement letter of credit, or equivalent financial guarantee has been received by the NCI Agency from, or on behalf of (NAME OF CONTRACTOR). (NAME OF CONTRACTOR) has, therefore, not fulfilled its obligations under Contract No. _____ dated _____ between NCI Agency and (NAME OF CONTRACTOR), and the NCI Agency, as beneficiary, hereby draws on the standby letter of credit number _____ in the amount of (Amount up to the maximum available under the LOC), such funds to be transferred to the account of the Beneficiary number _____ (to be identified when certificate is presented)."

Such certificate shall be accompanied by the original of this letter of credit and a copy of the letter from the issuing bank that it elects not to automatically extend the standby letter of credit, or terminating the letter of credit.

8. The Beneficiary may not present the certificate described in paragraph 7 above

until 20 (twenty) calendar days prior to a) the date of expiration of the letter of credit should {issuing bank} elect not to automatically extend the expiration date of the letter of credit, b) the date of termination of the letter of credit if {issuing bank} notifies the Beneficiary that the letter of credit is to be terminated in accordance with paragraph 6 above.

9. Multiple partial drawings are allowed to the maximum value of the standby letter of credit.

10. This letter of credit sets forth in full the terms of our undertaking, and this undertaking shall not in any way be modified, amended, or amplified by reference to any document, instrument, or agreement referred to herein (except the International Standby Practices (ISP 98) hereinafter defined) or in which this letter of credit is referred to or to which this letter of credit relates, and any such reference shall not be deemed to incorporate herein by reference any document, instrument, or agreement.

11. This Letter of Credit is subject to The International Standby Practices-ISP98 (1998 Publication) International Chamber of Commerce Publication No.590.

9. PARTICIPATING COUNTRIES

9.1 Unless prior written authorisation of the Purchaser has been obtained, none of the Work, shall be performed other than by firms from and within NATO Participating Countries. Unless otherwise specified in the Contract Special Provisions, the Participating Countries are the twenty-eight (28) Member Nations of the North Atlantic Treaty Organisation.

9.2 Unless prior written authorisation of the Purchaser has been obtained, no material or items of equipment down to and including identifiable Sub-Assemblies shall be manufactured or assembled by a firm other than from and within a NATO Participating Country.

9.3 The Contractor shall not place any Sub-contracts outside the NATO Participating Countries without the prior written authorisation of the Purchaser.

9.4 Unless prior written authorisation of the Purchaser has been obtained, the intellectual property rights for all software and documentation incorporated by the Contractor and/or its Sub-contractors into the Work shall vest with persons or legal entities from and within NATO participating nations and no royalties or licence fees for such software and documentation shall be paid by the Contractor to any source that does not reside within a NATO participating nation.

9.5 Any modification in the nationality, ownership and/or change of control of the Contractor and/or its Sub-contractor(s) shall be immediately notified in writing to the Purchaser with all necessary details to allow the Purchaser to determine whether or not the Contractor and/or its Sub-contractors continue

to comply with the Clauses above. Non-compliance with the Clauses above, by the Contractor and/or its Subcontractor may constitute ground for termination of this Contract under Clause 39 (Termination for Default).

10. SUB-CONTRACTS

10.1 The Contractor shall place and be responsible for the administration and performance of all Sub-contracts including terms and conditions which he deems necessary to meet the requirements of this Contract in full.

10.2 Prior to the Sub-contractors being given access to any classified information, the Contractor shall ensure that any Sub-contractor that has a need to access classified information for the performance of any part of this Contract has been granted the appropriate facility and personnel security clearances by the Sub-contractor's national authorities and that such clearances are still in effect at the time the information is disclosed and remains in effect throughout the performance of the work to be carried out under the Sub-contract concerned.

10.3 The Contractor shall seek the approval in writing of the Purchaser prior to the placing of any Sub-contract if:

10.3.1 the Sub-contract was not part of the Contractor’s original proposal;

and

10.3.2 the value of the Sub-contract is known or estimated to exceed 15 per cent of the total Contract value; or

10.3.3 the Sub-contract is one of a number of Sub-contracts with a single Sub-contractor for the same or related Work under this Contract that in the aggregate are known or expected to exceed 15 per cent of the total Contract value.

10.4 The Contractor shall inform the Purchaser of any change in Sub-contractors for Sub-contracts of a value known or estimated to exceed 15 per cent of the total Contract value.

10.5 The Contractor shall submit a copy of any such proposed Sub-contract including prices when seeking approval to the Contracting Authority but such approval by the Contracting Authority shall in no way relieve the Contractor of his responsibilities to fully achieve the contractual and technical requirements of this Contract.

10.6 The Contractor shall, as far as practicable, select Sub-contractors on a competitive basis consistent with the objectives and requirements of the Contract.

11. SECURITY

11.1 The Contractor shall comply with all security measures as are prescribed by the Purchaser and the national security authority or designated security agency of each of the NATO countries in which the Contract is being performed. The Contractor shall be responsible for the safeguarding of classified information, documentation, material and equipment entrusted to him or generated by him in connection with the performance of the Contract.

11.2 In particular the Contractor undertakes to:

11.2.1 appoint an official responsible for supervising and directing security measures in relation to the Contract and communicating details of such measures to the Purchaser on request;

11.2.2 maintain, preferably through the official responsible for security measures, a continuing relationship with the national security authority or designated security agency charged with ensuring that all NATO classified information involved in the Contract is properly safeguarded;

11.2.3 abstain from copying by any means, without the authorisation of the Purchaser, the national security authority or designated security agency, any classified documents, plans, photographs or other classified material entrusted to him;

11.2.4 furnish, on request, information to the national security authority or designated security agency pertaining to all persons who will be required to have access to NATO classified information;

11.2.5 maintain at the work site a current record of his employees at the site who have been cleared for access to NATO classified information. The record should show the date of issue, the date of expiration and the level of clearance;

11.2.6 deny access to NATO classified information to any person other than those persons authorised to have such access by the national security authority or designated security agency;

11.2.7 limit the dissemination of NATO classified information to the smallest number of persons (“need to know basis”) as is consistent with the proper execution of the Contract;

11.2.8 comply with any request from the national security authority or designated security agency that persons entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding both of their obligations under national legislation affecting the safeguarding of classified information, and of their comparable obligations

under the laws of the other NATO nations in which they may have access to classified information;

11.2.9 report to the national security authority or designated security agency any breaches, suspected breaches of security, suspected sabotage, or other matters of security significance which would include any changes that may occur in the ownership, control or management of the facility or any changes that affect the security arrangements and security status of the facility and to make such other reports as may be required by the national security authority or designated security agency, e.g. reports on the holdings of NATO classified material;

11.2.10 apply to the Purchaser for approval before Sub-contracting any part of the work, if the Sub-contract would involve that the Sub-contractor would have access to NATO classified information, and to place the Sub-contractor under appropriate security obligations no less stringent than those applied to his own contract;

11.2.11 undertake not to utilise, other than for the specific purpose of the Contract, without the prior written permission of the Purchaser or his authorised representative, any NATO classified information furnished to him, including all reproductions thereof in connection with the Contract, and to return all NATO classified information referred to above as well as that developed in connection with the Contract, unless such information has been destroyed, or its retention has been duly authorised with the approval of the Purchaser. Such NATO classified information will be returned at such time as the Purchaser or his authorised representative may direct;

11.2.12 classify any produced document with the highest classification of the NATO classified information disclosed in that document.

12. RELEASE OF INFORMATION

12.1 Except as otherwise specified elsewhere in the Contract and to the extent that it is demonstratively unavoidable and without prejudice to the Clause 11 (Security), the Contractor and/or his employees shall not, without prior authorisation from the Purchaser, release to third parties any information pertaining to this Contract, its subject matter, performance there under or any other aspect thereof.

12.2 The Contractor shall seek the prior written approval of the Purchaser before publishing any press release or disclosing any other information, orally or in writing, in relation to the Contract. The approval of the Purchaser shall be required for both the opportunity and the content of the information.

12.3 This provision shall remain in effect after the termination of the Contract and shall cease to apply to any particular piece of information once that information becomes public knowledge other than through an act, default or omission of the Contractor or its Sub-contractors.

13. PURCHASER FURNISHED PROPERTY

13.1 The Purchaser shall deliver to the Contractor, for use only in connection with this Contract, the Purchaser Furnished Property at the times and locations stated in the Contract. In the event that Purchaser Furnished Property is not delivered by such time or times stated in the Schedule, or if not so stated, in sufficient time to enable the Contractor to meet such delivery or performance dates the Purchaser shall, upon timely written request made by the Contractor, and if the facts warrant such action, equitably adjust any affected provision of this Contract pursuant to Clause 16 (Changes).

13.2 In the event that Purchaser Furnished Property is received by the Contractor in a condition not suitable for its intended use, the Contractor shall immediately notify the Purchaser. The Purchaser shall within a reasonable time of receipt of such notice replace, re-issue, authorise repair or otherwise issue instructions for the disposal of Purchaser Furnished Property agreed to be unsuitable. The Purchaser shall, upon timely written request of the Contractor, equitably adjust any affected provision of this\ Contract pursuant to Clause 16 (Changes).

13.3 Title to Purchaser Furnished Property will remain in the Purchaser. The Contractor shall maintain adequate property control records of Purchaser Furnished Property in accordance with sound industrial practice and security regulations.

13.4 Unless otherwise provided in this Contract, the Contractor, upon delivery to him of any Purchaser Furnished Property, assumes the risk of, and shall be responsible for, any loss thereof or damage thereof except for reasonable wear and tear, and except to the extent that Purchaser Furnished Property is consumed in the performance of this Contract.

13.5 Upon completion of this Contract, or at such earlier dates as may be specified by the Purchaser, the Contractor shall submit, in a form acceptable to the Purchaser, inventory schedules covering all items of Purchaser Furnished Property.

13.6 The inventory shall note whether:

13.6.1 The property was consumed or incorporated in fabrication of final deliverable(s);

13.6.2 The property was otherwise destroyed;

13.6.3 The property remains in possession of the Contractor;

13.6.4 The property was previously returned

13.7 The Contractor shall prepare for shipment, deliver DDP at a destination agreed with the Purchaser, or otherwise dispose of Purchaser Furnished Property as may be directed or authorised by the Purchaser. The net proceeds of any such disposal shall be credited to the Contract price or paid to the Purchaser in such other manner as the Purchaser may direct.

13.8 The Contractor shall not modify any Purchaser Furnished Property unless specifically authorised by the Purchaser or directed by the terms of the Contract.

13.9 The Contractor shall indemnify and hold the Purchaser harmless against claims for injury to persons or damages to property of the Contractor or others arising from the Contractor's possession or use of the Purchaser Furnished Property. The Contractor shall indemnify the Purchaser for damages caused by the Contractor to the Purchaser, its property and staff and arising out of the Contractor's use of the Purchaser Furnished Property.

14. CONTRACTOR'S PERSONNEL WORKING AT PURCHASER'S FACILITIES

14.1 The term "Purchaser Facilities" as used in this Clause shall be deemed to include sites, property, utilities, ships or vessels and the term "Facility Representative" shall be deemed to refer to the authority designated by the Purchaser responsible for the site, property, utility, ship or vessel.

14.2 The Facility Representative shall provide such available administrative and technical facilities for Contractor's personnel working at Purchaser's Facilities for the purpose of the Contract as in the opinion of the Facility Representative may be necessary for the effective and economical discharge of Work. The Facility Representative shall also determine whether these facilities will be provided free of charge to the Contractor or determine what charges are payable. The Contractor shall have no claim against the Purchaser for any such additional cost or delay or any additional cost or delay occasioned by the closure for holidays of said facilities, or other reasons, where this is generally published or made known to the Contractor by the Purchaser or his authorised representatives.

14.3 The Contractor shall, except as otherwise provided for in the Contract, make good or, at the option of the Purchaser, pay compensation for all damage occurring to any Purchaser's Facilities occasioned by the Contractor, his servants, agents or Sub-contractors, arising from his or their presence and activities in, and use of, the Purchaser's Facilities; provided that this

Condition shall not apply to the extent that the Contractor is able to show that any such damage was not caused or contributed to, by his neglect, or default or the neglect or default of his servants, agents or Sub-contractors, or by any circumstances within his or their control.

14.4 All property of the Contractor while at a Purchaser Facility shall be at the risk of the Contractor, and the Purchaser shall accept no liability for any loss or damage, except to the extent that any loss or damage is the result of a wilful act or gross negligence on the part of the Purchaser's employees or agents.

15. HEALTH, SAFETY AND ACCIDENT PREVENTION

15.1 If the Purchaser notifies the Contractor in writing of any non-compliance in the performance of this Contract with safety and health rules and requirements prescribed on the date of this Contract by applicable national or local laws, ordinances and codes, and the Contractor fails to take immediate corrective action, the Purchaser may order the Contractor to stop all or part of the Work until satisfactory corrective action has been taken. Such an order shall not entitle the Contractor to an adjustment of the Contract price or other reimbursement for resulting increased costs, or to an adjustment of the delivery or performance schedule.

16. CHANGES

16.1 The Purchaser may at any time, by written order of the Contracting Authority designated or indicated to be a change order ("Change Order") make changes within the general scope of this Contract, including, without limitation, in any one or more of the following:

16.1.1 Specifications (including drawings and designs);

16.1.2 Method and manner of performance of the work, including engineering standards, quality assurance and configuration management procedures;

16.1.3 Marking and method of shipment and packing;

16.1.4 Place of delivery;

16.1.5 Amount, availability and condition of Purchaser Furnished Property.

16.2 The Purchaser shall submit a proposal for Contract amendment describing the change to the Contract.

16.3 If any such Change Order causes an increase in the Contractor's cost of, or the time required for, the performance of any part of the Work under this Contract, whether or not changed by any such order, the Contractor shall submit a written proposal for adjustment to the Purchaser describing the general nature and amount of the proposal for adjustment. The Contractor shall submit this proposal for adjustment within thirty (30) days after receipt of a written Change Order under (a) above unless this period is extended by the Purchaser.

16.4 If any such Change Order causes a decrease in the Contractor's cost of, or the time required for, the performance of any part of the Work under this Contract, whether or not changed by any such order, the Purchaser shall submit a proposal for adjustment within thirty (30) days from the issuance of the Change Order by submitting to the Contractor a written statement describing the general nature and amount of the proposal for adjustment.

16.5 Where the cost of property made obsolete or in excess as a result of a change is included in the Contractor's claim for adjustment, the Purchaser shall have the right to prescribe the manner of disposition of such property.

16.6 The Purchaser reserves the right to reject the introduction of the change, after the evaluation of the change proposal, even if the Purchaser initiated such change.

16.7 Failure to agree to any requested adjustment shall be a dispute within the meaning of the Clause 41 (Disputes). However, nothing in this Clause shall excuse the Contractor from proceeding with the Contract as changed.

16.8 No proposal for adjustment by the Contractor for an equitable adjustment shall be allowed if asserted after final payment and acceptance under this Contract.

16.9 Any other written or oral order (which, as used in this paragraph includes direction, instruction, interpretation, or determination) from the Purchaser that causes a change shall be treated as a Change Order under this Clause, provided, that the Contractor gives the Purchaser a written notice within thirty (30) Days after receipt of such order stating (i) the date, circumstances, and source of the order; (ii) that the Contractor regards the order as a Change Order; and (iii) a detailed cost and time analysis of the impact of the change, and that the Order is accepted in writing by the Purchaser as a Change Order. The timely written notice requirement, as detailed above, remains in force in all cases, even where, for example, the Purchaser has positive knowledge of the relevant facts.

16.10 All tasks and activities carried out by the Contractor in relation to the processing of the Change Order or in relation to this Clause shall form part of the Contractor’s routine work and cannot be charged as additional work.

17. STOP WORK ORDER

17.1 The Purchaser may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the Work called for by this Contract for a period of ninety (90) days after the order is delivered to the Contractor, and for any further period to which the Parties may agree.

17.2 Any such stop work order shall be specifically identified as a stop work order issued pursuant to this Clause (the "Stop Work Order"). The Stop Work Order may include a description of the Work to be suspended, instructions concerning the Contractor's issuance of further orders for material or services, guidance to the Contractor on actions to be taken on any Sub-contracts and any suggestion to the Contractor for minimizing costs.

17.3 Upon receipt of such a Stop Work Order, the Contractor shall forthwith comply with its terms and take all reasonable steps to minimise costs incurred allocable to the Work covered by the Stop Work Order during the period of work stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to the Contractor, or within any extension of that period to which the Parties shall have agreed, the Purchaser shall either:

17.3.1 cancel the Stop Work Order; or

17.3.2 terminate the Work covered by such Stop Work Order as provided in Clause 40 (Termination for Convenience of the Purchaser).

17.4 If a Stop Work Order issued under this Clause is cancelled or the period of the Stop Work Order or any extension thereof expires, the Contractor shall resume work.

17.5 An equitable adjustment shall be made in the delivery schedule or Contract price, or both, and the Contract shall be modified in writing accordingly, if:

17.5.1 the Stop Work Order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this Contract, and;

17.5.2 the Contractor asserts a Claim for such adjustment within thirty (30) days after the end of the period of work stoppage; provided that, if the Purchaser decides the facts justify such action, he may receive and act upon any such claim asserted at a later date but prior to final payment under this Contract.

17.6 If a Stop Work Order is not cancelled and the Work covered by such Stop Work Order is terminated for the convenience of the Purchaser the reasonable costs resulting from the Stop Work Order shall be allowed in

arriving at the termination settlement.

18. CLAIMS

18.1 The Contractor shall specifically identify the Contract Clause(s) under which the Claim(s) is/are based.

18.2 Claims shall be specifically identified as such and submitted:

18.2.1 within the time specified in the Clause under which the Contractor alleges to have a Claim. If no time is specified in the Clause under which the Contractor intends to base his Claim, the time limit shall be sixty (60) days from the date the Contractor has knowledge or should have had knowledge of the facts on which he bases his Claim; and

18.2.2 before final payment, pursuant to and with the exceptions specified in Clause 33 entitled" Release of Claims".

18.2.3 Section 18.2.2 above shall only apply to those Claims for which the Contractor could not have had earlier knowledge and were not foreseeable.

18.3 The Contractor shall be foreclosed from his Claim unless he presents complete documentary evidence, justification and costs for each of his Claims within ninety (90) calendar days from the assertion date of such Claims. Claims shall be supported by specifically identified evidence (including applicable historical and planned cost and production data from the Contractor's books and records). Opinions, conclusions or judgmental assertions not supported by such evidence will be rejected by the Purchaser.

18.4 An individual breakdown of cost is required for each element of Contractor's Claims at the time of claim submission or for any material revision of the Claim.

18.5 The Contractor shall present, at the time of submission of a Claim, an attestation as follows:

> I .....the responsible senior company official authorised to commit the ..... with respect to its claims dated ..... being duly sworn, do hereby depose and say that: (i) the facts described in the claim are current, complete and accurate; and (ii) the conclusions in the claim accurately reflect the material damages or contract adjustments for which the Purchaser is allegedly liable.

.....

……..

SIGNATURE Date

18.6 Failure to comply with any of the above requirements shall result in automatic foreclosure of the Claim. This foreclosure takes effect in all cases and also where, for example, the Claim is based on additional orders, where the facts are known to the Purchaser, where the Claim is based on defective specifications of the Purchaser or an alleged negligence in the pre-contractual stage.

18.7 Claims submitted by the Contractor will be reviewed by the Contracting Authority. The Contracting Authority will respond within sixty (60) days with a preliminary decision, based on an assessment and evaluation of the facts presented by the Parties, as to whether the Contracting Authority considers the Claim to have merit for consideration. If the preliminary decision of the Contracting Authority is that the Claim, as submitted is without merit, the Contractor shall have fourteen (14) days to present a rebuttal to the Contracting Authority and request reconsideration of the Contracting Authority's decision. Within thirty (30) days receipt of the Contractor's request for reconsideration, the Contracting Authority will issue a decision. The time requirements stated herein may be extended by the Contracting Authority in order to accommodate additional preparation efforts and fact finding discussions but the Contracting Authority may not unreasonable extend such a period. A decision that the submitted claim is without merit will be identified as such, will be issued in writing by the Contracting Authority and will be conclusive. A decision may only be challenged by the Contractor through the Disputes provisions described herein.

18.8 A decision by the Purchaser that the claim has merit will result in a Contracting Authority request to enter into negotiations with the Contractor to arrive at a mutually agreed fair and equitable settlement. The Contracting Authority's decision will contain a target date for the commencement and conclusion of such operations. If the Parties are unable to arrive at an agreement on a fair and reasonable settlement by the target date for conclusion, or any extension thereto made by the Contracting Authority, the latter may declare that negotiations are at an impasse and issue a preliminary decision as to the fair and reasonable settlement and the reasons supporting this decision. The Contractor shall have a period of thirty (30) days to present a rebuttal to the Contracting Authority and request reconsideration of the Contracting Authority's decision. Within sixty (60) days of receipt of the Contractor's request for reconsideration, the Contracting Authority will issue its decision on the request for reconsideration. This timeframe will be respected unless an authorisation is needed from a NATO or other authority , the schedule for which is beyond the Contracting Authority's control. A

decision of the Contracting Authority on the reconsideration of the matter will be identified as such, will be issued in writing by the Contracting Authority and will be conclusive. A decision on the reconsideration may only be challenged by the Contractor through the Disputes provisions described herein.

18.9 No Claim arising under this Contract may be assigned by the Contractor without prior approval of the Purchaser.

18.10 The Contractor shall proceed diligently with performance of this Contract, pending final resolution of any request for relief, claim appeal, or action arising under the Contract, and comply with any decision of the Contracting Authority.

19. PRICING OF CHANGES, AMENDMENTS AND CLAIMS

19.1 Contractor's pricing proposals for Changes, amendments and Claims shall be priced in accordance with the Purchaser's Pricing Principles (Annex 1 hereto and the sample spreadsheet and its " Instructions to Complete" at Appendix 1) or the national government pricing rules and regulations for the Contractor's own country, where in force. The Contractor shall provide cost information accompanied by appropriate substantiation as required by the Purchaser in accordance with Purchaser's Pricing Principles, or such other format as may be agreed between the Contractor and the Purchaser.

19.2 With respect to Clause 19.1 above, when the price or price adjustment is based on adequate price competition, established catalogue or market price of commercial items sold in substantial quantities to the general public, or prices set by law or regulation, the Contractor shall be responsible for substantiation of such cases to the satisfaction of the Purchaser.

19.3 For the purposes of verifying that the cost or pricing data submitted in conjunction with Clause 19.1 above are accurate, complete and current, the Purchaser or any Purchaser authorised representative shall have the right of access to the Contractor's facilities to examine, until the expiration of three (3) years from the date of final payment of all sums due under the Contract:

19.3.1 those books, records, documents and other supporting data which will permit adequate evaluation and verification of the cost or pricing data submitted; and/or

19.3.2 the computations and projections which were available to the Contractor as of the date of the Contractor price proposal.

19.4 The Contractor, subject to the provisions of this Clause, shall require Sub-contractors to provide to the Purchaser, either directly or indirectly:

19.4.1 cost or pricing data;

19.4.2 access to Sub-contractor's facilities and records for the purposes of verification of such cost or pricing data; and

19.4.3 a Certificate of Current Cost or Pricing Data, when required.

19.5 If any price, including profit, negotiated in connection with this Contract was proposed, taking any of the following into account:

19.5.1 the Contractor furnished cost or pricing data which was not complete, accurate and current as certified in the Contractor's Certificate of Current Cost or Pricing Data provided in accordance with Clause 19.6 below;

19.5.2 a Sub-contractor, pursuant to Clause 19.4 above or any Sub-contract clause therein required, furnished cost or pricing data which was not complete, accurate and current as certified in the Sub-contractor's Certificate of Current Cost or Pricing Data;

19.5.3 a Sub-contractor or prospective Sub-contractor furnished cost or pricing data which was required to be complete, accurate and current and to be submitted to support a Sub-contract cost estimate furnished by the Contractor but which was not complete, accurate and current as of the date certified in the Contractor's Certificate of Current Cost or Pricing Data; or

19.5.4 the Contractor or a Sub-contractor or prospective Sub-contractor furnished any data, not within 19.5.1 through 19.5.3 above, which, as submitted, was not complete, accurate and current;

19.5.5 then the price and/or cost shall be adjusted accordingly and the Contract shall be modified in writing as may be necessary to reflect such.

19.6 At the time of negotiating any price, including profit, which is based upon the submission of cost or pricing data by the Contractor, the Contractor shall be required to submit a certificate of current cost or pricing data (“Certificate”).

19.6.1 Such Certificates will certify that, to the best of the Contractor's knowledge and belief, cost or pricing data submitted to the Purchaser in support of any proposal for a price, price adjustment or claim, are accurate, complete and current, as per the completion of the negotiations or, in the case of a claim, as per the submission date of the claim.

19.6.2 All such Certificates shall be in the format shown below and shall be dated and signed by a responsible officer of the company:

CERTIFICATE OF CURRENT COST OR PRICING DATA

This is to certify that cost or pricing data as submitted, either actually or by specific identification in writing to the Purchaser or his representative in support of.....*(Claim, Amendment, ECP#, etc.,)* are accurate, complete and current as of .....*(Date).*

By submitting the price proposal, the Contractor/sub-Contractor or prospective sub-Contractor grant the Purchaser or his authorized representative(s) the right to examine those records, data and supporting information, used as a basis for the pricing submitted.

_____

Name of Company

_____

Signature

_____

Printed Name of Signatory

_____

Title of Signatory

_____

Date of Signature

19.6.3 The Contractor shall insert the substance of this Clause 19.7 in each Sub-contract.

19.7 For all additional or follow-up agreements which are made for Work which are furnished to the Purchaser without competition, the Contractor shall offer prices on a “Preferred Customer” basis, that is offer prices which are as favourable as those extended to any Government, Agency, Company, Organisation or individual purchasing or handling like quantities of

equipment and/or Parts covered by the Contract under similar conditions. In the event that prior to completing delivery under this Contract the Contractor offers any of such items in substantially similar quantities to any customer at prices lower than those set forth herein, the Contractor shall so notify the Purchaser and the prices of such items shall be correspondingly reduced by a supplement to this Contract. Price in this sense means "Base Price" prior to applying any bonus, export tax reduction, turn-over tax exemptions and other reductions based on National Policies.

20. NOTICE OF SHIPMENT AND DELIVERY

20.1 Except as may be specified in the Contract Special Provisions, delivery of all items under this Contract shall be made by the Contractor on the basis of “Delivery Duty Paid” (DDP) as defined by the INCOTERMS 2000 (International Chamber of Commerce Publication No. 560). It shall be noted, however, that because the Purchaser is exempted from direct taxes and duty as set forth in Clause 26 (Taxes and Duties), there is no duty to be paid by the Contractor.

20.2 "Delivery" of required Work by the Contractor does not constitute "Acceptance" by the Purchaser for purposes of meeting the requirements of the Contract Schedule where Purchaser acceptance is the stated payment or schedule milestone.

20.3 Thirty (30) Days, or such other period as specified in the Contract, prior to the delivery of any shipment of Work, the Contractor shall give prepaid notice of shipment to the Purchaser. The Notice of Shipment shall contain, as appropriate, the request for customs form 302, or equivalent document, which shall enable any carrier to conduct duty free import/export clearance through customs for the Purchaser on behalf of NATO.

20.4 The customs form 302 is an official customs clearance declaration issued in advance of shipment by the Purchaser to provide certified information as to the duty free import, export, or transit of NATO consignments between NATO countries.

20.5 The Notice of Shipment and request for Form 302 or equivalent document shall contain the following information:

20.5.1 Purchaser's Contract number;

20.5.2 Contract item number, designation and quantities;

20.5.3 destination;

20.5.4 number and description of the packages (gross and net weight);

20.5.5 description of the goods and their value (for custom purpose only, not commercial value)

20.5.6 consignor's name and address;

20.5.7 consignee's name and address;

20.5.8 method of shipment (i.e. road, rail, sea, air, etc.);

20.5.9 name and address of freight forwarder.

20.6 Forwarding Agents, Carriers or other responsible organisations shall be informed by the Contractor of the availability of Form 302 or equivalent document and how the form shall be utilised to avoid the payment of custom duties. Form 302 or equivalent document shall be incorporated in all shipping documents provided to the carrier.

20.7 Upon receipt of the Notice of Shipment from the Contractor, the Purchaser may require the Contractor to send copies of the Notice of Shipment to the receiving parties and the Contractor shall comply with this requirement.

21. INSPECTION AND ACCEPTANCE OF WORK

21.1 For the purposes of this Clause, Work does not include documentation which is addressed in Clause 22 (Inspection and Acceptance of Documentation) hereafter.

21.2 Unless otherwise specifically provided for in the Contract, all Work and all Parts and equipment incorporated in the Work are to be new and of the most suitable grade of their respective kinds for the purpose, notwithstanding the requirements for testing, inspection and performance as required under this Contract. All workmanship shall be as specified under the Contract or, if no workmanship standards are specified, best commercial or “state of the art” complying with relevant (National and International) standards.

21.3 All Work may be subject to inspection and test by the Purchaser or his authorised representative(s) to the extent practicable at all times and places prior to Acceptance, including the period of manufacture, or after delivery or as otherwise specified in the Contract. For the purposes of inspection and testing the Purchaser may delegate as his representative the authorised National Quality Assurance Representative (NQAR) in accordance with STANAG 4107.

21.4 No representative or NQAR appointed by the Purchaser for the purpose of determining the Contractor's compliance with the technical requirements of the Contract shall have the authority to change any of the specifications. Such changes may only be made by the Contracting Authority in writing in accordance with Clause 16 (Changes).

21.5 The presence or absence of an NQAR or other Purchaser representative shall not relieve the Contractor from conforming to the requirements of this Contract.

21.6 Acceptance or rejection of the Work shall be made as promptly as practicable after delivery, except as otherwise provided in the Contract. Failure to timely

accept or reject the Work shall neither relieve the Contractor from responsibility for such Work nor impose liability on the Purchaser.

21.7 In the event that any Work, or lots thereof, or services are defective in design, material, workmanship or manufacturing quality, or as a result of undue wear and tear or otherwise not in conformity with the requirements of this Contract, including any characteristic or condition which is or becomes at variance to the performance specifications, to the intended function of the Work or the function to which it could reasonably be expected that the Work would perform, the Purchaser shall have the right either to reject them (with or without instructions as to their disposition) or to require their correction or replacement. Work which has been rejected or required to be corrected or replaced shall, at the expense of the Contractor, be removed, or, if permitted or required by the Contracting Authority, corrected in place by the Contractor promptly after notice, and shall not thereafter be tendered for acceptance by the Contractor unless the former rejection or requirement of correction or replacement is withdrawn. If the Contractor fails promptly to remove, replace or correct such Work the Purchaser may either:

21.7.1 by contract or otherwise return, replace or correct such Work or services and charge to the Contractor the cost incurred by the Purchaser; and/or

21.7.2 terminate this Contract for default as provided in Clause 39 (Termination for Default).

21.8 When NQAR is not applicable based on the scale of the project, the Purchaser reserves the right to perform inspections through his own staff in accordance with the latest ISO standard at the time of inspection.

21.9 Unless the Contractor corrects or replaces such Work within the delivery schedule, the Purchaser may require the delivery of such Work at a reduction in price which is equitable under the circumstances. Failure to agree to such reduction of price shall be a dispute within the meaning of Clause 41 (Disputes).

21.10 If any inspection or test is made by the Purchaser's representatives on the premises of the Contractor or Sub-contractor, the Contractor, without additional charge, shall provide all reasonable facilities and assistance for the safety and convenience of the Purchaser's representatives in the performance of their duties. The NQAR or other Purchaser representatives shall have the right of access to any area of the Contractor's or his Sub-contractor's premises where any part of the contractual work is being performed.

21.11 If Purchaser inspection or test is made at a point other than the premises of the Contractor or Sub-contractor, it shall be at the expense of the Purchaser except as otherwise provided in this Contract; provided, that in case of rejection the Purchaser shall not be liable for any reduction in value of samples used in connection with such inspection or test.

21.12 All inspections and tests by the Purchaser shall be performed in such a

manner as not to unduly delay the Work.

21.13 The Purchaser reserves the right to charge to the Contractor any additional cost of Purchaser inspection and test when Work is not ready at the time such inspection and test is requested by the Contractor or when re-inspection or retest is necessitated by prior rejection.

21.14 Acceptance or rejection of the Work shall be made as promptly as practicable after delivery, except as otherwise provided in this Contract, but failure to inspect and accept or reject Work shall neither relieve the Contractor from responsibility for such Work as are not in accordance with the Contract requirements nor impose liability on the Purchaser thereof.

21.15 The inspection and test by the Purchaser of any Work or lots thereof, or services, does not relieve the Contractor from any responsibility regarding defects or other failures to meet the Contract requirements which may be discovered prior to acceptance.

21.16 Acceptance of Work shall take place when the Contracting Authority confirms acceptance in writing of the Work in accordance with the procedure specified in the Contract, or if none is so specified then the Contracting Authority shall be deemed to have accepted the Work without prejudice to any other remedies, when and as soon as any of the following events have occurred:

21.16.1 the Purchaser has taken the Work into use, except as specifically provided by Clause 23 (Use and Possession Prior to Acceptance);

21.16.2 the Purchaser has not exercised its right of rejection of the Work within any period specified for that purpose in the Contract;

21.16.3 there being no period for exercising the right of rejection specified in the Contract, a reasonable time, all the circumstances having been taken into account, has elapsed since inspection of the Work was effected in accordance with the Contract.

21.17 Except as otherwise provided in this Contract, acceptance shall be conclusive except as regards latent defects, fraud, or such gross mistakes as amount to fraud.

21.18 Unless otherwise specified in this Contract, the Contractor shall have or establish, implement and maintain an effective and economical quality control system necessary to satisfy the Contract requirement. The system shall provide for the early and prompt detection of deficiencies, trends and conditions which could result in unsatisfactory quality and for timely and effective corrective action. Objective evidence that the system is effective shall be readily available to the Purchaser and its authorised representatives. Records of all inspection and testing work by the Contractor shall be kept complete and available to the Purchaser’s representatives during the performance of this Contract and for such longer periods as may be specified elsewhere in this Contract.

22. INSPECTION AND ACCEPTANCE OF DOCUMENTATION

22.1 The Contractor shall provide to the Purchaser a draft version of the required documentation as provided by the Contract Schedule and the Statement of Work. Review of draft documentation under this Contract will be made by the Purchaser upon the delivery of these items by the Contractor. The review will be conducted by the Purchaser through duly authorised representatives.

22.2 Upon delivery of the draft documentation, the Purchaser will have a period of review as provided by the Statement of Work. At the end of the review period or before if deemed practical by the Purchaser, the Purchaser's comments will be presented to the Contractor in writing. The substance of such comments will pertain to items of error, non-conformity, omission and guidance in relation to the requirements of the Statement of Work.

22.3 Purchaser Review of the delivered items will emphasise the conformity with the requirements of the Statement of Work, thoroughness of analysis, logical bases of conclusions and models and coherence and completeness of presentation. The review process will also examine editorial and grammatical correctness and the suitability and accuracy of graphics supporting the text.

22.4 The Contractor shall, after receipt of Purchaser comments, incorporate changes, revisions and corrections required by the Purchaser and present the revised documentation in final form to the Purchaser for inspection in accordance with the delivery date specified in the Schedule.

22.5 During the review process the Contractor is not required to halt efforts on further tasks as identified in the Statement of Work. The Purchaser, however, shall not be held liable for any work carried out by the Contractor which is based on draft documentation yet to be reviewed.

22.6 Upon receipt of the items in final form, the Purchaser will inspect the items for a period not exceeding two weeks (or as otherwise stated in the Statement of Work). At the end of the inspection, the Purchaser will notify the Contractor that:

22.6.1 the items have been accepted;

22.6.2 the acceptance of the items is deferred pending further revision;

or

22.6.3 The items are rejected and significantly fail to meet Contract requirements.

22.7 In the case of Clause 22.6.2 above, the Contractor shall only be responsible for those revisions and corrections requested by the Purchaser and the

Purchaser may not request additional revisions during inspection after required revisions have been made. However, if the Purchaser determines that a directed revision has not been made or if such directed revision was cause for revision of other portions of content which were not made by the Contractor, the Purchaser may withhold acceptance until such revisions are made by the Contractor.

22.8 The Contractor shall provide to the Purchaser on request supporting technical data, computer software, databases and background analyses in order to validate findings contained in the delivered items.

22.9 Purchaser acceptance shall be made in writing by the Contracting Authority.

23. USE AND POSSESSION PRIOR TO ACCEPTANCE

23.1 Except as otherwise provided in the Contract Special Provisions, the Purchaser shall have the right to take possession of, or use, any completed or partially completed Work under the Contract at any time, when notified by the Contracting Authority, however such possession or use shall not constitute Acceptance by the Purchaser, as defined in the Contract.

23.2 While the Purchaser has such use or is in such possession, the Contractor shall be relieved of the responsibility for loss or damage to the Work concerned other than that resulting from the Contractor's fault, negligence or defect to the Work.

23.3 If such prior possession or use by the Purchaser delays the progress of the Work or causes additional expense to the Contractor, an equitable adjustment in the Contract price or the time of delivery will be made, in accordance with the Clause 16 (Changes), and the Contract shall be modified in writing accordingly.

24. OWNERSHIP AND TITLE

24.1 Except as may be otherwise stated in the Contract Special Provisions and Clause 23 (Use and Possession prior to Acceptance), ownership and title to all Work will pass to the Purchaser only upon Acceptance by the Contracting Authority in writing. Where the Contract provides for Provisional Acceptance and Final Acceptance, ownership and title will pass to the Purchaser upon written notification of Final Acceptance.

25. INVOICES AND PAYMENT

25.1 Unless otherwise specified in the Contract Special Provisions, invoices shall only be submitted after delivery and Acceptance of the Work and for the total prices and currency(ies) as set out under the Schedule of Work.

25.2 Invoices in respect of any Work or services shall be prepared and submitted

to the Purchaser and shall contain all of the elements listed below:

25.2.1 Contract number;

25.2.2 Purchaser's Purchase Order number ;

25.2.3 accounting codes (as specified in this Contract);

25.2.4 item number (as defined in the Contract);

25.2.5 Contract description of Work or services, sizes, quantities, unit prices, and extended totals (exclusive of taxes and duties for which relief is available); and

25.2.6 extended totals. Details of Bills of Lading or Freight Warrant numbers and weight of shipment shall be identified on each invoice as appropriate.

25.3 In addition, documentary evidence of Acceptance including copies of certificates of conformity shall be submitted together with each invoice. Invoices shall not be submitted to the Purchaser without Acceptance having been previously made by the Purchaser.

25.4 Each copy of the invoice shall contain the following certificate which shall be signed by a duly authorised company official on the designated original invoice:

"I certify that the above invoice is true and correct, that the delivery of the above described items has been duly carried out and the payment thereof has not been received.

*Order placed for official use. Exemption from VAT Article 42,§3&3*of VAT Code for Belgium or Article 151, §1b of the Council Directive 2006/112/EC dd. 28 November 2006 on intra-community purchases and/or services.".*

25.5 All invoices shall be addressed to the NCI Agency - Financial Management

Either at the following addresses:

NCI Agency * If used for NCI Agency Brussels

NATO Communications and Information Agency
Finance, Accounting & Operations
Batiment Z
Av du Bourget 140
B-1140 Belgium

OR

shall be addressed to Financial Management at the following electronic address:
"NCIA-CAPDEV-FMU-BEL_E-INVOICES@NCIA.NATO.INT (note there is an underscore between BEL and E-INVOICES)

Note: When used for NCI Agency The Hague or Mons the addresses shall be dictated in the Contract Special Provisions

Once the manner of forwarding the invoice is chosen, the contractor shall keep this manner throughout the contract.

25.6 All invoices submitted shall include the address of the bank to which payment shall be made, together with **either** pertinent information concerning the International Bank Account Number (IBAN) and BIC/SWIFT address **or** pertinent information concerning transit number/sort code, account number and SWIFT address. The Purchaser makes payment only by wire transfer and therefore wire transfer particulars shall be included on the invoice.

25.7 Invoices will be settled by the Purchaser within sixty (60) days of receipt of a properly prepared and submitted invoice.

25.8 The Contractor shall mention on the invoice the payment conditions in line with the Contract.

26. TAXES AND DUTIES

26.1 The Purchaser, by virtue of his status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct taxes (incl. VAT) and all customs duties on merchandise imported or exported. The Contractor, therefore, certifies that the prices stipulated in this Contract do not include amounts to cover such direct taxes or customs duties.

26.2 The Contractor shall be responsible for ensuring that his respective Sub-contractors are aware that the Purchaser is exempt from taxes and customs duties. The Contractor (and his respective Sub-contractors) shall be responsible for complying with all applicable national and local legal and administrative procedures to ensure that authorities do not attempt to assess taxes and customs duties on goods and property imported or exported through NATO member nation frontiers under this Contract nor assess direct taxation (VAT) on goods sold to the NCI Agency under this Contract.

26.3 The Purchaser shall give reasonable assistance in providing evidence/documents which might be required by the Contractor to ensure that NCI Agency receives tax exemption by virtue of its status under the Ottawa Agreement.

26.4 If, after complying with all national and local legal and administrative

procedures, the authorities persist in attempting to impose taxes or duties on goods provided under this Contract, the Contractor shall inform the Contracting Authority providing the particulars of the situation, the procedures which have been followed and the point of contact at the national authority which is attempting to impose taxation or duty. The Contracting Authority will examine the situation and attempt to clarify the legal and administrative basis of the difficulty. If the Contracting Authority so directs, the Contractor shall pay the required taxes and duties and file for reimbursement or rebate from the national authorities in accordance with national legislative and administrative procedures.

26.5 In the event that the petition for reimbursement or rebate is denied by the national authorities concerned and providing that the Contractor and/or his Sub-contractor have complied with the national legislative and administrative procedures, the Purchaser shall reimburse the full amount of the payment(s) upon receipt of the Contractor's invoice indicating such tax or duty as a separate item of cost and fully identified by reference to any governmental law, regulation and/or instruction pursuant to which such tax or duty is enforced. The Contractor shall offer assistance and execute any such document that may be useful or required to ensure that Purchaser obtains the reimbursement of any tax or duty retained by a national authority.

26.6 In the event of the Contractor and/or Sub-contractor not complying with national legislative or administrative procedures, taxes and duties paid by the Contractor and/or Sub-contractors shall not be reimbursed by the Purchaser.

26.7 Following payment by the Purchaser of the taxes and/or duties pursuant to Clause 26.4 above, should the Contractor subsequently receive a rebate of any amount paid by the Purchaser, the Contractor shall immediately notify the Purchaser and the amount of such rebate shall be credited or reimbursed to the Purchaser, as directed. The Contractor shall be responsible for taking any and all action that could reasonably be required in order to obtain such rebate.

26.8 The Contractor shall be liable for all other taxes, assessments, fees, licences, administrative charges or other Government assessments or charges which are applicable to the performance of this Contract. It is the Contractor's responsibility to inform himself of his liability in each country where such liability may arise.

27. WARRANTY OF WORK (Exclusive of Software)

27.1 For the purpose of this Clause:

27.1.1 “Acceptance” shall mean the act of an authorised representative of the Purchaser by which the Purchaser

assumes title and ownership of delivered Work rendered as partial or complete performance of the Contract. "Acceptance" in this regard, unless specifically provided otherwise in the Contract Contract Special Provisions, means final Acceptance where the Contract provides for Provisional or Partial Acceptance;

27.1.2 "Correction" shall mean the elimination of a defect;

27.1.3 "Work" shall not include software.

27.2 The Contractor shall not be responsible under this Clause for the Correction of Defects in Purchaser Furnished Property, except for Defects in Contractor performed installation, unless the Contractor performs, or is obligated to perform, any modifications or other work on Purchaser Furnished Property. In that event, the Contractor shall be responsible for Correction of Defects that result from the modifications or other Work.

27.3 Unless another period of time is indicated in the Contract Contract Special Provisions, the duration of the warranty provided by the Contractor and its Subcontractors shall be twelve (12) months from the date of Acceptance under this Contract as notified in writing by the Contracting Authority.

27.4 Any Work or parts thereof corrected or furnished in replacement and any services re-performed shall also be subject to the conditions of this Clause 27 to the same extent as Work initially accepted. The warranty, with respect to these Work, or parts thereof shall be equal in duration to that set forth in Clause 27.3, and shall run from the date of delivery of the corrected or replaced Work.

27.5 If the Contractor becomes aware at any time before Acceptance by the Purchaser (whether before or after tender to the Purchaser) or at a later time, that a Defect exists in any Work, the Contractor shall either promptly correct the Defect or promptly notify the Purchaser, in writing, of the Defect, using the same procedures prescribed in Clause 27.8.

27.6 The Purchaser will notify in writing the Contractor of the existence of a Failed Component and return to the Contractor the Failed Component within thirty (30) Days of the discovery of such failure. The transport of the Failed Component shall be at the expense of the Purchaser. The notification of the failure will include as much information as practicable about the circumstances and operating environment at the time of the failure. Upon receipt of such notification by the Purchaser (which may precede receipt of the Failed Component), the Contractor shall ship to the location of the Failed Component an identical component for installation by Purchaser personnel. The Contractor shall ship such replacement component(s) Delivery Duty Paid. Such transportation and replenishment charges are included in the cost of line item of the Contract identified as the warranty.

27.7 In such rare cases where the Failed Component is either too large to be

easily transported or the Failed Component cannot be readily identified and isolated within the larger entity, the Contractor shall be notified by the Purchaser of the failure immediately by telephone, fax or e-mail. The Contractor shall provide technical support to the Purchaser personnel in identifying the Failed Component so as to afford the Purchaser the opportunity to return the Failed Component. In such a case where the Failed Component cannot be identified or is not cost effective or practical to ship to the Contractor's facility, the Contractor may elect to send field service personnel to the site of the failure and repair such equipment on location. In this event, such field service personnel shall be dispatched to the site of the failure within forty-eight (48) hours of initial notification. The expense of the technical support and field service shall be borne by the Contractor.

27.8 The Contractor shall conduct analysis of all Failed Components which are returned to him by the Purchaser or repaired in the field by Contractor field service personnel to determine the cause of the failure. The Contractor shall issue a report to the Purchaser within thirty (30) days of receipt of a returned item or field repair which contains the results of the analysis. The report shall contain the conclusion of the Contractor as to whether the cause of the failure was due to a Manufacturing Defect or a Design Defect and declare what course of remedial action the Contractor shall implement to prevent further failures of a similar nature. Repetitive failures of the same component may be grounds for a de facto determination by the Purchaser that a Design Defect exists.

27.9 If the Purchaser determines that a Design Defect exists in any of the Work accepted by the Purchaser under this Contract, the Purchaser shall promptly notify the Contractor of the Defect, in writing, within ninety (90) days after discovery of the Defect. Upon timely notification of the existence of a Defect, or if the Contractor independently discovers a Design Defect or Manufacturing Defect in accepted Work, the Contractor shall submit to the Purchaser, in writing within thirty (30) days, a recommendation for corrective actions, together with supporting information in sufficient detail for the Purchaser to determine what corrective action, if any, shall be undertaken.

27.10 The Contractor shall also prepare and furnish to the Purchaser data and reports applicable to any Correction required under this Clause (including revision and updating of all other affected data and already accepted documentation called for under this Contract) at no increase in the Contract price.

27.11 In the event of timely notice of a decision not to correct or only to partially correct, the Contractor shall submit a technical and cost proposal within forty-five (45) days to amend the Contract to permit Acceptance of the affected Work in accordance with the revised requirement, and an equitable reduction in the Contract price shall promptly be negotiated by the Parties and be reflected in a supplemental agreement to this Contract.

27.12 Within thirty (30) days after receipt of the Contractor's recommendations for corrective action and adequate supporting information in accordance with

Clause 27.9, the Purchaser using sole discretion, shall give the Contractor written notice not to correct any Defect, or to correct or partially correct any Defect within a reasonable time.

27.13 The Contractor shall promptly comply with any timely written direction from the Purchaser to correct or partially correct a manufacturing or Design Defect, at no increase in the Contract price.

27.14 The Purchaser shall give the Contractor a written notice specifying any failure or refusal of the Contractor to:

27.14.1 conduct analyses of Failed components and implement a course of remedial action as required by Clauses 27.7 and 27.8;

27.14.2 provide replacement components, technical support or on-location field repair service in accordance with Clauses 27.6 and 27.7; or

27.14.3 prepare and furnish data and reports as required by Clause 27.10.

27.15 The notice referred to in Clause 27.14 shall specify a period of time following receipt of the notice by the Contractor in which the Contractor must remedy the failure or refusal specified in the notice.

27.16 If the Contractor does not comply with the Purchaser's written notice in Clause 27.14, the Purchaser may by Contract or otherwise:

27.16.1 Obtain detailed recommendations for corrective action from its own resources or third parties and either:

27.16.2 correct the Work;

27.16.3 replace the Work, and if the Contractor fails to furnish timely disposition instructions, the Purchaser may dispose of the non-confirming Work for the Purchaser's account in a reasonable manner, in which case the Purchaser is entitled to reimbursement from the Contractor, or from the proceeds, for the reasonable expenses of care and disposition, as well as for excess costs incurred or to be incurred;

27.16.3.1 obtain applicable data and reports; and/or

27.16.3.2 charge the Contractor for the costs incurred by the Purchaser.

27.17 In no event shall the Purchaser be responsible for any extension or delays in the scheduled deliveries or periods of performance under this Contract as a result of the Contractor's obligations to correct Defects, nor shall there be any adjustment of the delivery schedule or period of performance as a result of the Correction of Defects unless provided by a supplemental agreement with adequate consideration.

27.18 The rights and remedies of the Purchaser provided in this Clause shall not be affected in any way by any terms or conditions of this Contract concerning the conclusiveness of inspection and Acceptance and are in addition to, and do not limit, any rights afforded to the Purchaser by any other Clause of this Contract or applicable law.

28. RIGHT OF ACCESS, EXAMINATION OF RECORDS

28.1 The Contractor shall give to the Purchaser and/or his representative(s) full and free access to his premises as and when required for the purpose of this Contract and shall ensure the same right of access to the premises of his Sub-contractors, by the inclusion in any such Sub-contracts of a provision substantially as set forth in this Clause.

28.2 The Purchaser and/or his representative(s) shall continue to have such right of access and examination of records as set forth in Clause 28.1 above until final payment under the Contract or the end of the warranty provisions under the Contract, whichever occurs later.

28.3 The expiration of the Purchaser's rights as set forth in Clause 28.2 is further subject to the provisions of Clause 19 (Pricing of Changes, Amendments and Claims), where a three (3) year right is established following the agreement of contractual amendments or the settlement of claims based upon the submission of cost and pricing data.

28.4 The period of access and examination described in Clause 28.1 above for records not related to cost aspects of a dispute or claim but which relate to issues of fact arising under either proceedings under Clause 41 (Disputes) or Clause 42 (Arbitration), or the settlement of claims made by either Party pursuant to the performance of this Contract, shall continue until such appeals, litigation or claims have been disposed of.

29. PATENT AND COPYRIGHT INDEMNITY

29.1 The Contractor shall assume all liability against any and all third party claims that the services, Work and/or parts thereof, in whole or in part, infringe(s) an IPR in force in any countries, arising out of the manufacture, import, export, performance of the services or delivery of Work and/or out of the use or disposal by, or for the account of, the Purchaser of such Services and/or Work. The Contractor shall reimburse and/or indemnify the Purchaser, its officers, agents, employees and/or consultants: (i) for all costs, fees, damages, awards, settlement amounts and any other expenses awarded to the third party right holder against Purchaser and/or the final beneficiaries of the Work in relation to said third party claim; and (ii) for the costs and expenses incurred by the Purchaser in relation to said third party claims, including attorney fees. The Contractor shall be responsible for obtaining any licences necessary for the performance of this Contract and for making all other arrangements required to indemnify

the Purchaser from any liability for IPR infringement in said countries.

29.2 Each Party shall immediately notify the other of any intellectual property infringement claims of which he has knowledge and which pertain to the Work under this Contract.

29.3 This indemnity shall not apply under the following circumstances:

29.3.1 Patents or copyright which may be withheld from issue by order of the applicable government whether due to security regulations or otherwise;

29.3.2 An infringement resulting from specific written instructions from the Purchaser under this Contract;

29.3.3 An infringement resulting from changes made to the Work by the Purchaser without the Contractor prior written consent;

29.3.4 An infringement resulting from changes or additions to the Work subsequent to final delivery and Acceptance under this Contract.

30. INTELLECTUAL PROPERTY

30.1 ***Purchaser Background IPR***

30.1.1 The Contractor is licensed to use, non-exclusively and royalty-free any Purchaser Background IPR that is or will be made available for the sole purpose of carrying out the Work.

30.1.2 The Contractor shall not use any Purchaser Background IPR other than for the purpose of carrying out the Work without the prior written agreement of the Purchaser. Any such agreement shall include the terms relating to such use.

30.1.3 The Purchaser gives no warranty as to the validity of any Purchaser Background IPR. The Contractor shall not do anything or act in any way which is inconsistent with or prejudicial to the ownership by the Purchaser of any Purchaser Background IPR.

30.2 ***Contractor Background IPR***

30.2.1 Any use of Contractor Background IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to Purchaser. The Contractor hereby grants to NATO a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Contractor Background IPR for the purpose of exploiting or otherwise using the Foreground IPR.

30.2.2 Any use of Contractor Background IPR is not limited to the number of users or the number of licenses required by the Contract for the use of system. The Purchaser reserves the right to use the Contractor Background IPR for any number of users and number of licenses as required, at no additional cost to the Purchaser.

30.3 ***Foreground IPR***

30.3.1 All Foreground IPR is the property of the Purchaser on behalf of NATO. Consequently, no statement shall be made restricting the rights of the Purchaser in the Foreground IPR.

30.3.2 The Contractor shall ensure that suitable arrangements are in place between its employees, agents, consultants and itself regarding Foreground IPR generated by said employees, agents, Subcontractors and consultants to allow the Contractor to fulfil its obligations under Clause 30.3.1 above.

30.3.3 The Contractor shall be entitled to use Foreground IPR on a non-exclusive, royalty free basis solely for the purpose of carrying out the Work.

30.3.4 The Contractor shall not use any Foreground IPR other than for the purpose of carrying out the Work without the Purchaser's prior written agreement. Any such agreement shall include terms relating to such use.

30.3.5 The Contractor shall provide the Purchaser, at the latest upon delivery of the Work and thereafter for the duration of the warranty and any purchased CLS agreement period, with full documented records of information in relation to the Work, including but not limited to, all drawings, specifications and other data that is necessary or useful to further develop, maintain and operate the Work.

30.3.6 The Contractor shall:

30.3.6.1 do all things necessary and sign all necessary or useful documents to enable the Purchaser to obtain the registration of the Foreground IPR as the Purchaser may require and select; and

30.3.6.2 to execute any formal assignment or other documents as may be necessary or useful to vest title to any Foreground IPR in the Purchaser.

30.3.7 The Contractor undertakes:

30.3.7.1 to notify the Purchaser promptly of any invention or improvement to an invention or any design conceived or made by the Contractor; and

30.3.7.2 to provide the Purchaser with such information as the Purchaser may reasonably request in order to: (i) determine the patentability of such invention or improvement; (ii) assess the need for registering such invention or improvement; and (iii) evaluate the potential value to the Purchaser of such a patent or registration if issued.

30.3.8 If the Purchaser determines that it wishes to apply for one or more patents for the disclosed invention or improvement or for a registration for the disclosed design, it will prosecute such application(s) at its own expense. The Contractor undertakes to provide the Purchaser, at the Purchaser's expense, with such information and assistance as the Purchaser shall reasonably require to prosecute such application(s).

30.4 ***Third Party IPR***

30.4.1 Any use of Third Party IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to the Purchaser. The Contractor hereby grants to NATO a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Third Party IPR for the purpose of exploiting or otherwise using the Foreground IPR.

30.4.2 With the exception of COTS items, any use of Third Party IPR is not limited to the number of users or the number of licenses required by the Contract for the use of system. With the exception of COTS items, the Purchaser reserves the right to use the Third Party IPR for any number of users and number of licenses as required, at no additional cost to the Purchaser.

30.4.3 For COTS items, the Contractor shall be responsible for obtaining licences from the Third Party in line with the requirements of the Statement of Work (including numbers and locations of licences).

30.4.4 Where Third Party IPR is the subject of a licence or other agreement between the third party and the Purchaser or the Contractor, the Contractor shall not use any Third Party IPR for the purposes of carrying out work pursuant to the Contract

without the prior written approval of the Purchaser. Contractor shall inform Purchaser in advance of any restrictions on the Purchaser's use.

30.4.5 If, after the award of the Contract, the Contractor becomes aware of the existence of any Third Party IPR which the Contractor is using or believes is needed for the performance of the Contract, the Contractor shall immediately give the Purchaser a written report identifying such IPR and if they are compliant with the other provisions in the contract. Any Third Party IPR under this clause is subject to the prior written approval by the Purchaser.

30.4.6 The Purchaser may consider open source solutions alongside proprietary ones in developments provided that such solutions are fully compliant with the requirements of this Contract. Contractor shall disclose in advance the open source license associated with the contemplated open source solution. The Purchaser reserves the right to refuse the incorporation of open source solutions that are deemed inadequate for incorporation in a NATO application (e.g. post-back obligations).

30.5 *Subcontractor IPR*

30.5.1 When placing a Sub-contract which is concerned with or involves the creation of IPR, the Contractor shall ensure that the Sub-contractor enters into the same agreement for the use of the IPR as stipulated in this Contract in such a way that the Purchaser will be entitled to use the IPR as agreed between the Purchaser and the Contractor. The Contractor shall include in the Sub-contract the content of the provisions of this Clause.

31. **SOFTWARE WARRANTY**

31.1 *Statement of the Warranties*

31.1.1 The Contractor warrants that each Software delivered under this Contract will conform to all requirements specified in the Contract. This will also include Software design specifications, including software configuration.

31.1.2 Regardless of the Purchaser initiation of or participation in developing Software design or specifications, each Software delivered under this Contract will conform to the essential Performance requirements set forth in this Contract, as those essential Performance requirements measured,

tested, and verified by tests and procedures set forth in this Contract.

31.2 *Notification Requirement*

31.2.1 The Contractor agrees to notify the Purchaser in writing immediately after he first discovers that a defect(s) may exist in Software delivered under this Contract, unless the Purchaser has first notified the Contractor, in writing, of the same defect(s).

31.2.2 The Purchaser shall notify the Contractor upon discovery that a defect(s) may exist in any Software accepted by the Purchaser under this Contract, unless the Contractor has first notified the Purchaser, in writing of the same defect(s).

31.3 Duration of the Warranty

31.3.1 For each Software delivered under this Contract, the Contractor Warranties stated in paragraph 31.1 above shall extend to all defects discovered within 12 months from the date of acceptance of the Software by the Purchaser.

31.4 Purchaser Remedies for Breach

31.4.1 The rights and remedies of the Purchaser under this Software Warranty:

31.4.2 Are in addition to any rights and remedies of the Purchaser under any other provision of this Contract, including, but not limited to, the Purchaser's rights in relation to latent defects, fraud, or gross mistakes that amount to fraud; and

31.4.3 Shall apply notwithstanding inspection, acceptance, or any other clauses or terms of this Contract;

31.4.4 In the event of any defect as defined herein with respect to a Software delivered under this Contract, the Purchaser, in its sole discretion may:

31.4.4.1 Require the Contractor to take such action as may be necessary to eliminate the defect, at no additional cost to the Purchaser for materials, labour, transportation, or otherwise;

31.4.4.2 Require the Contractor to supply, at no additional cost to the Purchaser, all materials and instructions necessary for the Purchaser to eliminate the defect and to pay costs reasonably incurred by the Purchaser in taking such action as

may be necessary to eliminate the defect, or;

31.4.4.3 Equitably reduce the contract price

31.4.5 The Purchaser may elect the remedies provided in paragraph 31.4.4.1 or 31.4.4.2 above notwithstanding any dispute respecting the existence of or responsibility for any alleged defect as defined herein with respect to any Software delivered under this contract, provided that the Contractor will not be required to pay costs incurred by the Purchaser under paragraph 31.4.4.2 until final determination of the defect. In the event that the alleged defect is subsequently determined not to be a defect subject to this warranty but the Contractor has incurred costs under paragraph 31.4.4.1 and 31.4.4.2 as required by the Contract by virtue of this paragraph 31.4.3, the contract price under this contract shall be equitably adjusted.

31.4.6 Election by the Purchaser of the remedy provided under paragraph 31.4.4.1 and 31.4.4.2 above shall not preclude subsequent election of a different remedy under paragraph 31.4.4 if the defect is not successfully eliminated under the prior election with one month of the notification under paragraph 31.4.2 above.

31.5 Limitations and Exclusions from Warranty Coverage

31.5.1 This Software Warranty shall not apply to alleged defects that the Contractor demonstrates to be in or otherwise attributable to the Purchaser furnished property as determined, tested, and verified by the tests and procedures set forth in this Contract. Notwithstanding this paragraph , a defect is not attributable to Purchaser furnished property if it is the result of installation or modification of Purchaser furnished property by the Contractor or of the integration of Purchaser furnished property into any Software delivered under this Contract.

31.5.2 Any Purchaser Furnished Property needs to be checked and approved by the Contractor. Approval is implied once the Contractor starts using the Purchaser Furnished Property.

31.6 Markings

31.6.1 All Deliverables under this Contract will identify the owner of the Deliverable and if applicable, will prominently include notice of the existence of its warranty, its substance, its duration, and instructions to notify the Purchaser promptly if the Software is found to be defective. The markings should also be included in

the operating and/or maintenance manuals or instructions accompanying such Software.

31.6.2 All Deliverables regardless of the media they are delivered onto and which are subject to export control restrictions shall be clearly marked indicating the type and nature of restriction as well as the national law imposing such restrictions. Nothing in this provision is intended to invalidate, void, or otherwise limit the rights of the Purchaser under this Contract.

32. NATO CODIFICATION

32.1 For the purposes of this Clause "Technical Data" means the drawings, specifications and technical documentation of those items designated by the Purchaser to support the equipment covered by the Contract, and required to fully identify the items and, if applicable, draft item identifications to the extent and in the form to be agreed between the Codification Authority and the Contractor.

32.2 In order to ensure the orderly identification of equipment, the Contractor shall furnish at the request of the Codification Authority the Technical Data required for the identification of the items of supply to the NATO codification system in the time scale stated in this Contract.

32.3 A recommended spare parts list or a similar data carrier prepared in accordance with instructions provided by the Purchaser as the basis for codification shall be supplied by the Contractor by the date established in this Contract.

32.4 The Contractor shall supply or require his Sub-contractor(s)/supplier(s) to supply on request for the period of time specified in the Contract the relevant Technical Data for all items and sub-contracted items to the Codification Authority and the Purchaser. The Contractor shall require that each Sub-contractor/supplier shall include identical conditions in any subsequent order which he may place.

32.5 The drawings, specifications, related documentation and, if applicable, draft item identifications, prepared when possible by the true manufacturer of the item, shall be supplied by the Contractor or his Sub-contractor(s)/supplier(s) direct to the Codification Authority and, if required, to the Purchaser as and when they become available or, at the latest within the time limits specified in the Contract. The Contractor shall inform the Codification Authority and Purchaser within 21 Days of receipt of the request if the required Technical Data are not immediately available, and shall impose a similar obligation upon his Sub-contractor(s)/supplier(s).

32.6 Except as hereinafter provided, the Contractor shall require the Sub-

contractor(s)/supplier(s) to furnish on request the information direct to the Codification Authority in the Sub-contractor(s)/supplier(s)' country, but the Contractor shall remain responsible for ensuring that the information is so furnished. In the event of a Sub-contract order being placed with a manufacturer in a non-NATO country, the Contractor shall be responsible for obtaining Technical Data from the Sub-contractor/supplier and furnishing it to the Purchaser.

32.7 Technical Data relating to any Sub-contractor's/supplier's items shall include but not be limited to the name and address of the true manufacturer(s), his/their true reference number(s), drawing or item Part number(s) and applicable data in addition to any Part or reference number(s) allocated by the Contractor, plus draft item identification(s) if required by the Codification Authority.

32.8 The Contractor shall provide the Technical Data required for codification of those items ordered with this Contract and also for the pertaining support items ordered with future contracts, including updating information regarding all agreed modifications, design or drawing changes made to the equipment or detailed Parts.

32.9 If the Contractor has previously supplied Technical Data (for the purpose stated in Clause 31.2), the Contractor is to state this fact and indicate to whom they were supplied and the Contractor shall not under normal circumstances be required to make a further supply of the Technical Data already provided. The Technical Data furnished by the Contractor and Sub-contractor(s)/supplier(s) are to be presented in accordance with the requirements for the preparation of item identification(s) as outlined in the Guide for Industry provided by the Codification Authority.

32.10 The Contractor should contact the Codification Authority for any information concerning the NATO codification system. This information is to be found at: "http://www.nato.int/structur/ac/135/ncs_guide/e_guide.htm"

32.11 Markings

32.11.1 All Deliverables under this Contract will identify the owner of the Deliverable and,if applicable, will prominently include notice of the existence of its warranty, its substance, its duration, and instructions to notify the Purchaser promptly if the Software is found to be defective. The markings should also be included in the operating and/or maintenance manuals or instructions accompanying such Software.

32.11.2 All Deliverables regardless of the media they are delivered onto

and which are subject to export control restrictions shall be clearly marked indicating the type and nature of restriction as well as the national law imposing such restrictions. Nothing in this provision is intended to invalidate, void, or otherwise limit the rights of the Purchaser under this Contract.

33. RELEASE FROM CLAIMS

33.1 Prior to final payment under this Contract, the Contractor and each assignee under this Contract shall execute and deliver a release discharging the Purchaser, its officers, agents and employees from all liabilities, obligations and claims arising out of or under this Contract subject only to the following exceptions:

33.1.1 specified claims in stated amounts or in estimated amounts where the amounts are not susceptible to exact statement by the Contractor;

33.1.2 claims for reimbursement of costs (other than expenses of the Contractor by reason of his indemnification of the Purchaser against patent liability) including reasonable expenses incidental thereto, incurred by the Contractor under the provisions of this Contract relating to patents.

33.1.3 a patent infringement resulting from specific written instructions from the Purchaser under this Contract.

33.1.4 a patent infringement resulting from changes or additions to the goods and services subsequent to final delivery and acceptance under this Contract.

34. ASSIGNMENT OF CONTRACT

34.1 The Purchaser reserves the right to assign this Contract, in whole or in part, to another NATO body, agency or representative within NATO or NATO Nations. In such a case, the Purchaser shall notify the Contractor accordingly in writing.

34.2 NATO shall remain responsible for its obligations under the Contract and for the actions of the body, agency or representative to which this Contract may be assigned.

35. TRANSFER AND SUB-LETTING

35.1 The Contractor shall not give, bargain, sell, assign, sub-let or otherwise dispose of the Contract or any part thereof or the benefit or advantage of the

Contract or any part thereof without the prior written consent of the Purchaser.

36. PURCHASER DELAY OF WORK

36.1 If the performance of all or any part of the Work is delayed or interrupted by an act of the Purchaser in the administration of this Contract, which act is not expressly or implicitly authorised by this Contract, or by the Purchaser's failure to act within the time specified in this Contract (or within a reasonable time if no time is specified), an adjustment shall be made for any increase in the cost of performance of this Contract caused by such delay or interruption and the Contract modified in writing accordingly.

36.2 Adjustment shall be made also in the delivery or performance dates and any other contractual provision affected by such delay or interruption. However, no adjustment shall be made under this Clause for any delay or interruption:

36.2.1 to the extent that performance would have been delayed or interrupted by any other cause, including the fault or negligence of the Contractor; or

36.2.2 for which an adjustment is provided or excluded under any other provision of this Contract.

36.3 No claim under this Clause shall be allowed:

36.3.1 if the Contractor has failed to notify the Purchaser in writing of the act or failure to act, indicating that this act or failure to act will result in a delay or increased costs;

36.3.2 for any costs incurred more than twenty (20) Days before the Contractor shall have notified the Purchaser in writing of the act or failure to act involved; and

36.3.3 unless the monetary claim, in an amount stated, is asserted in writing as soon as practicable after the termination of such delay or interruption, but not later than the date of final payment under the Contract.

37. CONTRACTOR NOTICE OF DELAY

37.1 In the event that the Contractor encounters difficulty in complying with the Contract schedule date(s) for whatever reason, including actual or potential labour disputes, the Contractor shall immediately notify the Contracting Authority in writing, giving pertinent details. This data shall be deemed to be informational in character and shall not be construed as a waiver by the Purchaser of any schedule or date, or of any rights or remedies provided by law or under this Contract.

37.2 Notwithstanding the above the Contractor shall be deemed to be in delay without notice from the Purchaser and only by simple expiry of the due date.

38. LIQUIDATED DAMAGES

38.1 If the Contractor:

38.1.1 fails to meet the delivery schedule of the Work or any performance milestones specified in the Schedule of Work to this Contract, or any extension thereof, or

38.1.2 fails to obtain acceptance of the delivered Work as specified in the Contract, or, if no time for acceptance is specified in the contract within a reasonable time after work is delivered.

the actual damage to the Purchaser for the delay will be difficult or impossible to determine. Therefore, in lieu of actual damages the Contractor shall pay to the Purchaser, for each day of delinquency in achieving the deadline or milestone, fixed and agreed liquidated damages of .1% (one tenth of per cent) per day of the associated payment set forth in the Schedule of Payments provided in the Contract Special Provisions. If no Schedule of Payments is specifically set forth in the Contract Special Provisions, the liquidated damages will be assessed against the price of the applicable contract line item (CLIN) of the Schedule of Supplies, Services and Prices.

38.2 In addition to the liquidated damages referred to above, the Purchaser shall have the possibility of terminating this Contract in whole or in part, as provided in Clause 39 (Termination for Default). In the event of such termination, the Contractor shall be liable to pay the excess costs provided in Clause 38.5.

38.3 The Contractor shall not be charged with liquidated damages when the delay arises out of causes beyond the control and without the fault or negligence of the Contractor as defined in Clause 39.6 (Termination for Default). In such event, subject to the provisions of Clause 41 (Disputes), the Purchaser shall ascertain the facts and extent of the delay and shall extend the time for performance of the Contract when in his judgement the findings of the fact justify an extension.

38.4 Liquidated damages shall be payable to the Purchaser from the first day of delinquency and shall accrue at the rate specified in Clause 38.1 to 20% of the value of each line item individually not to exceed 15% of the value of the total Contract. These liquidated damages shall accrue automatically and without any further notice being required.

38.5 The rights and remedies of the Purchaser under this clause are in addition to any other rights and remedies provided by law or under this Contract.

39. TERMINATION FOR DEFAULT

39.1 The Purchaser may, subject to Clause 39.6 below, by written notice of default to the Contractor, terminate the whole or any part of this Contract if the Contractor, inclusive but not limited to:

39.1.1 fails to make delivery of all or part of the Work within the time specified in the contract or any agreed extension thereof;

39.1.2 fails to make progress as to endanger performance of this Contract in accordance with its terms;

39.1.3 fails to meet the technical requirements or the Specifications of the Contract;

39.1.4 fails to comply with Clause 11 (Security);

39.1.5 transfer this Contract without the Purchaser's prior written consent;

39.1.6 breaches any provision of this Contract; or

39.2 In the case of any of the circumstances set forth in Clause 39.1 above, the Purchaser shall issue a letter to the Contractor stating that an actual or potential default exists and requiring a response from the Contractor within ten (10) Days that identifies:

39.2.1 in the case of late delivery of Work, when the Contractor shall deliver the Work and what circumstances exist which may be considered excusable delays under Clause 39.6.

39.2.2 in the case of the other circumstances identified in Clause 39.1 above, what steps the Contractor is taking to cure such failure(s) within a period of ten Days (or such longer period as the Purchaser may authorise in writing) after receipt of notice in writing from the Purchaser specifying such failure and identifying any circumstances which exist which may be considered excusable under Clause 39.6.

39.3 The Purchaser shall evaluate the response provided by the Contractor or, in the absence of a reply within the time period mentioned in Clause 39.2, all relevant elements of the case, and make a written determination within a reasonable period of time that:

39.3.1 sufficient grounds exist to terminate the Contract in whole or in part in accordance with this Clause and that the Contract is so terminated;

39.3.2 there are mitigating circumstances and the Contract should be amended accordingly; or

39.3.3 the Purchaser will enter a period of forbearance in which the Contractor must show progress, make deliveries, or comply with the Contract provisions as specified by the Purchaser. The Purchaser may apply other remedial actions as provided by this Contract during such period of forbearance. This period of forbearance shall in no event constitute a waiver of Purchaser's rights to terminate the Contract for default.

39.4 At the end of the period of forbearance, which may be extended at the Purchaser's discretion, the Purchaser may terminate this Contract in whole or in part as provided in Clause 39.1 if the Contractor has not made adequate progress, deliveries or compliance with the Contract provisions which were the terms of the period of forbearance.

39.5 In the event the Purchaser terminates this Contract in whole or in part, as provided in Clause 39.1, the Purchaser may procure, upon such terms and in such manner as the Purchaser may deem appropriate, Work similar to those so terminated, and the Contractor shall be liable to the Purchaser for any excess costs for such similar Work; however, the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this clause.

39.6 Except with respect to the default of Sub-contractors, the Contractor shall not be held liable for a termination of the Contract for default if the failure to perform the Contract arises out of causes beyond the control and without the fault or negligence of the Contractor.

39.6.1 Such causes may include, but are not restricted to, acts of God, acts of the public enemy, acts of the Purchaser in its contractual capacity, acts of sovereign governments which the Contractor could not reasonably have anticipated, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

39.6.2 If the failure to perform is caused by the default of a Sub-contractor, and if such default arises out of causes beyond the control of both the Contractor and Sub-contractor, without the fault or negligence of either of them, the Contractor shall not be held liable for a termination for default for failure to perform unless the Work to be furnished by the Sub-contractor were obtainable from other sources in sufficient time to permit

the Contractor to meet the required delivery schedule.

39.7 If this Contract is terminated as provided in Clause 39.1, the Purchaser, in addition to any other rights provided in this Clause and the Contract, may require the Contractor to transfer title and deliver to the Purchaser, in the manner and to the extent directed by the Purchaser:

39.7.1 any completed Work with associated rights ;

39.7.2 such partially completed Work, materials, Parts, tools, dies, jigs, fixtures, plans, drawings, information, and Contract rights (hereinafter called "Manufacturing materials") with associated rights as the Contractor has specifically produced or specifically acquired for the performance of such part of this Contract as has been terminated;

39.8 In addition to Clause 39.7, the Contractor shall, upon direction of the Purchaser, protect and preserve property in the possession of the Contractor in which the Purchaser has an interest.

39.9 Payment for completed Work delivered to and accepted by the Purchaser shall be at the Contract price.

39.10 Payment for manufacturing materials delivered to and accepted by the Purchaser and for the protection and preservation of property shall be in an amount agreed upon by the Contractor and Purchaser, failure to agree to such amount shall be a dispute within the meaning of Clause 41 (Disputes).

39.11 The Purchaser may withhold from amounts otherwise due to the Contractor for such completed Work or manufacturing materials such sum as the Purchaser determines to be necessary to protect the Purchaser against loss because of outstanding liens or claims of former lien holders.

39.12 If, after notice of termination of this Contract under the provisions of this Clause, it is determined for any reason that the Contractor was not in default under the provisions of this Clause, or that the default was excusable under the provisions of this Clause, the rights and obligations of the Parties shall be the same as if the notice of termination had been issued pursuant to Clause 40 (Termination for the Convenience of the Purchaser).

39.13 If after such notice of termination of this Contract under the provisions of this Clause, it is determined for any reason that the Contractor was not in default under the provisions of this Clause and that the Parties agree that the Contract should be continued, the Contract shall be equitably adjusted to compensate for such termination and the Contract modified accordingly. Failure to agree to any such adjustment shall be a dispute within the meaning of Clause 41 (Disputes).

39.14 The rights and remedies of the Purchaser provided in this Clause shall not be

exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

40. TERMINATION FOR THE CONVENIENCE OF THE PURCHASER

40.1 The performance of Work under this Contract may be terminated by the Purchaser in accordance with this Clause in whole, or from time to time in part, whenever the Purchaser shall determine that such termination is in the best interest of the Purchaser.

40.2 Any such termination shall be effected by delivery to the Contractor of a written notice of termination, signed by the Contracting Authority, specifying the extent to which performance of Work under the Contract is terminated, and the date upon which such termination becomes effective.

40.3 After receipt of a Notice of Termination and except as otherwise directed by the Contracting Authority, the Contractor shall:

40.3.1 stop the Work on the date and to the extent specified in the notice of termination;

40.3.2 place no further orders or Sub-contracts for Work, Parts, materials, services or facilities, except as may be necessary for completion of such portion of the Work under the Contract as is not terminated;

40.3.3 terminate all orders and Sub-contracts to the extent that they relate to the performance of Work terminated by the Notice of Termination;

40.3.4 assign to the Purchaser, in the manner, at the times and to the extent directed by the Purchaser, all of the right, title and interest of the Contractor under the orders and Sub-contracts so terminated, in which case the Purchaser shall have the right, in its discretion, to settle or pay any or all claims arising out of the termination of such orders and Sub-contracts;

40.3.5 settle all outstanding liabilities and all claims arising out of such termination of orders and Sub-contracts, with the approval or ratification of the Purchaser to the extent he may require, which approval or ratification shall be final for all the purposes of this Clause;

40.3.6 transfer title and deliver to the Purchaser in the manner, at the times, and to the extent, if any, directed by the Contracting Authority of:

40.3.6.1 the fabricated parts, work in process, completed work, Work, and other material produced as a part of, or acquired in connection with the performance of the Work terminated by the notice of termination, and

40.3.6.2 the completed or partially completed plans, drawings, information, and other property which, if the Contract had been completed, would have been required to be furnished to the Purchaser;

40.3.7 use his best efforts to sell, in the manner, at the times, to the extent, and at the price or prices directed or authorised by the Contracting Authority, any property of the types referred to in Clause 40.3.6 above. However, the Contractor:

40.3.7.1 shall not be required to extend credit to any Buyer; and

40.3.7.2 may acquire any such property under the conditions prescribed by and at a price or prices approved by the Purchaser; and provided further that the proceeds of any such transfer or disposition shall be applied in reduction of any payments to be made by the Purchaser to the Contractor under this Contract or shall otherwise be credited to the price or cost of the Work or paid in such manner as the Contracting Authority may direct;

40.3.8 complete performance of such part of the Work as shall not have been terminated by the Notice of Termination; and

40.3.9 take such action as may be necessary, or as the Purchaser may direct, for the protection and preservation of the property related to this Contract which is in the possession of the Contractor and in which the Purchaser has or may acquire an interest.

40.4 The Contractor may submit to the Purchaser a list, certified as to quantity and quality, of any or all items of termination inventory not previously disposed of, exclusive of items the disposition of which has been directed or authorised by the Purchaser, and may request the Purchaser to remove such items or enter into a storage agreement covering the same; provided that the list submitted

shall be subject to verification by the Purchaser upon removal of the items, or if the items are stored, within forty-five (45) Days from the date of submission of the list, and any necessary adjustment to correct the list as submitted shall be made prior to final settlement.

40.5 After receipt of a notice of termination, the Contractor shall submit to the Purchaser his termination Claim for the Work covered by the notice of termination, in the form and with certification prescribed by the Purchaser. Such claim shall be submitted promptly but in no event later than six (6) months from the effective date of termination, unless one or more extensions are granted in writing by the Purchaser, upon request of the Contractor made in writing within such six-month period or authorised extension thereof. However, if the Purchaser determines that the facts justify such action, the Purchaser may receive and act upon any such termination claim at any time after such six-month period or any extension thereof. Upon failure of the Contractor to submit his termination claim within the time allowed, the Purchaser may determine on the basis of information available to him, the amount, if any, due to the Contractor by reason of the termination and shall thereupon pay to the Contractor the amount so determined.

40.6 Subject to the provisions of Clause 40.5, the Contractor and the Purchaser may agree upon the whole or any part of the amount or amounts to be paid to the Contractor by reason of the total or partial termination of Work pursuant to this Clause, which amount or amounts may include a reasonable allowance for profit on work done; provided that such agreed amount or amounts exclusive of settlement costs shall not exceed total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of the Work not terminated. The Contract shall be amended accordingly and the Contractor shall be paid the amount agreed.

40.7 In the event of the failure of the Contractor and the Purchaser to agree as provided in Clause 40.6 upon the whole amount to be paid to the Contractor by reason of the termination of Work pursuant to Clause 40, the Purchaser shall pay to the Contractor the amounts determined by the Purchaser as follows, but without duplication of any amounts agreed upon in accordance with Clause 40.6 the total of:

40.7.1 for completed Work accepted by the Purchaser (or sold or acquired as provided in Clause 40.3 above) and not therefore paid for, a sum equivalent to the aggregate price for such Work computed in accordance with the price or prices specified in the Contract, appropriately adjusted for any saving of freight or other charges;

40.7.2 the costs incurred in the performance of the Work terminated including initial costs and preparatory expense allocable thereto, but exclusive of any costs attributable

to Work paid or to be paid for under Clause 40.7.1;

40.7.3 the cost of settling and paying claims arising out of the termination of work under Sub-contracts or orders, as provided in Clause 40.3.5, which are properly chargeable to the terminated portion of the Contract, exclusive of amounts paid or payable on account of Work or materials delivered or services furnished by Sub-contractors or vendors prior to the effective date of the notice of termination, which amounts shall be included in the costs payable under Clause 40.7.2; and

40.7.4 a sum, as profit on Clause 40.7.1 above, determined by the Purchaser to be fair and reasonable; provided, however, that if it appears that the Contractor would have sustained a loss on the entire Contract, had it been completed, no profit shall be included or allowed and an appropriate adjustment shall be made reducing the amount of the settlement to reflect the indicated rate of loss; and

40.7.5 the reasonable costs of settlement, including accounting, legal, clerical and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination and settlement of Sub-contracts there under, together with reasonable storage, transportation, and other costs incurred in connection with the protection, or disposition of property allocable to this Contract.

40.8 The total sum to be paid to the Contractor under Clause 40.7 shall not exceed the total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of Work not terminated.

40.9 Except for normal spoilage, and except to the extent that the Purchaser shall have otherwise expressly assumed the risk of loss, there shall be excluded from the amounts payable to the Contractor, as provided in Clause 40.7 above, the fair value, as determined by the Purchaser, of property which is destroyed, lost, stolen, or damaged so as to become undeliverable to the Purchaser, or to a buyer pursuant to Clause 40.3.7 above.

40.10 The Contractor shall have the right to dispute, under the Clause 41 (Disputes), any determination made by the Purchaser under Clauses 40.5 and 40.7, except that if the Contractor has failed to submit his claim within the time provided in Clause 40.5 and has failed to request extension of such time, the Contractor shall be foreclosed from his right to dispute said determination. In

any case where the Purchaser has made a determination of the amount due under Clauses 40.5 and 40.7, the Purchaser shall pay the Contractor the following:

40.10.1 if there is no right of appeal hereunder or if no timely appeal has been taken, the amount so determined by the Purchaser, or

40.10.2 if an appeal has been taken, the amount finally determined on such appeal.

40.11 In arriving at the amount due to the Contractor under this Clause there shall be deducted:

40.11.1 all unliquidated advance or other payments on account theretofore made to the Contractor, applicable to the terminated portion of this Contract;

40.11.2 any claim which the Purchaser may have against the Contractor in connection with this Contract; and

40.11.3 the agreed price for, or the proceeds of the sale of, any materials, Work, or other things acquired by the Contractor or sold, pursuant to the provisions of this Clause, and not otherwise recovered by or credited to the Purchaser.

40.12 If the termination hereunder is partial, prior to the settlement of the terminated portion of this Contract, the Contractor may file with the Purchaser, in accordance with Clause 16 (Changes), a request in writing for an equitable adjustment of the price or prices relating to the continued portion of the Contract (the portion not terminated by the notice of termination), and such equitable adjustment as may be agreed upon shall be made in such price or prices.

40.13 The Purchaser may from time to time, under such terms and conditions as it may prescribe, make partial payments and payments on account against costs incurred by the Contractor in connection with the terminated portion of this Contract whenever in the opinion of the Purchaser the aggregate of such payments shall be within the amount to which the Contractor will be entitled hereunder. If the total of such payment is in excess of the amount finally agreed or determined to be due under this Clause, such excess shall be payable by the Contractor to the Purchaser upon demand, together with interest calculated using the average of the official base rate(s) per annum of the deposit facility rate as notified by the European Central Bank or such other official source as may be determined by the Purchaser, for the period from the date the excess is received by the Contractor to the date such excess is repaid to the Purchaser, provided, however, that no interest shall be charged with respect to any such excess payment attributed to a reduction in the

Contractor's claim by reason of retention or other disposition of termination inventory until ten days after the date of such retention or disposition or such later date as determined by the Purchaser by reason of the circumstances.

40.14 Unless otherwise provided for in this Contract, the Contractor, from the effective date of termination and for a period of three years after final settlement under this Contract, shall preserve and make available to the Purchaser at all reasonable times at the office of the Contractor, but without direct charge to the Purchaser, all his books, records, documents, computer files and other evidence bearing on the costs and expenses of the Contractor under this Contract and relating to the work terminated hereunder, or, to the extent approved by the Purchaser, photographs, micro-photographs, or other authentic reproductions thereof.

41. DISPUTES

41.1 Except to the extent to which special provision is made elsewhere in the Contract, all disputes, differences or questions which are not disposed of by agreement between the Parties to the Contract with respect to any matter arising out of or relating to the Contract, other than a matter as to which the decision of the Contracting Authority under the Contract is said to be final and conclusive, shall be decided by the Contracting Authority. The Contracting Authority shall reduce his decision to writing and mail or otherwise furnish a copy thereof to the Contractor.

41.2 The Contracting Authority shall not proceed with the evaluation and decision in respect of any claim until and unless the Contractor has submitted the attestation as foreseen in Clause 18 (Claims), as well as the complete proof and evidence of the claim (either by submission or by identification of the relevant documentation).

41.3 The Contracting Authority's decision shall be final and conclusive unless, within 30 Days from the date of receipt of such copy, the Contractor mails or otherwise furnishes to the Contracting Authority his decision to open arbitration proceedings in accordance with the Clause 42 (Arbitration). The burden of proof for both receipt and delivery of such documentation shall be by signed and dated registered mail receipt or by hand receipt as acknowledged and signed by the Contracting Authority.

41.4 Pending final decision of a dispute, the Contractor shall proceed diligently with the performance of the Contract, unless otherwise instructed by the Contracting Authority.

42. ARBITRATION

42.1 Within a period of thirty days from the date of receipt of the notification referred to in Clause 41.3 above, the Parties shall jointly appoint an arbitrator. In the event of failure to appoint an arbitrator, the dispute or disputes shall be

submitted to an Arbitration Tribunal consisting of three arbitrators, one being appointed by the Purchaser, another by the other contracting party and the third, who shall act as President of the Tribunal, by these two arbitrators. Should one of the Parties fail to appoint an arbitrator during the fifteen days following the expiration of the first period of thirty days, or should the two arbitrators be unable to agree on the choice of the third member of the Arbitration Tribunal within thirty days following the expiration of the said first period, the appointment shall be made, within twenty-one days, at the request of the Party instituting the proceedings, by the Secretary General of the Permanent Court of Arbitration at The Hague.

42.2 Regardless of the procedure concerning the appointment of this Arbitration Tribunal, the third arbitrator will have to be of a nationality different from the nationality of the other two members of the Tribunal.

42.3 Any arbitrator must be of the nationality of any one of the member states of NATO and shall be bound by the rules of security in force within NATO.

42.4 Any person appearing before the Arbitration Tribunal in the capacity of an expert witness shall, if he is of the nationality of one of the member states of NATO, be bound by the rules of security in force within NATO. If he is of another nationality, no NATO classified documents or information shall be communicated to him.

42.5 An arbitrator, who, for any reason whatsoever, ceases to act as an arbitrator, shall be replaced under the procedure laid down in Clause 42.1 above.

42.6 The Contractor agrees to submit to the Arbitration Tribunal only such issues, facts, evidence and proof which the Contractor had beforehand identified and submitted to the Contracting Authority for decision in accordance with Clause 41 (Disputes). The jurisdictional authority of the Arbitration Tribunal shall be restricted to consider only those identical issues, facts, evidence and proof so identified and submitted to the Contracting Authority.

42.7 The Purchaser likewise agrees to restrict its submissions only to the information on which the Contracting Authority based its decision and not to introduce new information and arguments which cannot reasonably be deduced or inferred from the written decision of the Contracting Authority in response to the original dispute.

42.8 The Arbitration Tribunal will take its decisions by a majority vote. It shall decide where it will meet and, unless it decides otherwise, shall follow the arbitration procedures of the International Chamber of Commerce in force at the date of signature of the present Contract.

42.9 The awards of the arbitrator or of the Arbitration Tribunal shall be final and there shall be no right of appeal or recourse of any kind. These awards shall

determine the apportionment of the arbitration expenses.

42.10 Pending final decision of a dispute, the Contractor shall proceed diligently with the performance of the Contract, unless otherwise instructed by the Contracting Authority.

43. SEVERABILITY

43.1 If one or more of the provisions of this Contract is declared to be invalid, illegal or unenforceable in any respect under any applicable law, the validity, legality and enforceability of the remaining provisions shall not be affected. Each of the Parties shall use its best efforts to immediately and in good faith negotiate a legally valid replacement provision.

44. APPLICABLE LAW

44.1 This Contract shall be governed, interpreted and construed in accordance with the private contract law of the Kingdom of Belgium.

* *

ANNEX 1 TO GENERAL PROVISONS: PURCHASER'S PRICING PRINCIPLES

A. General

1. With regard to all actions included in Clause 19," Pricing of Changes, Amendments and Claims", the Parties agree that the Purchaser's Pricing Principles contained herein shall govern.

2. As may be requested by the Purchaser, the Contractor shall provide documentation. that the standards or principles employed in the submission of cost or pricing data are in conformance with governing national policies and regulation. The Contractor, when submitting a price proposal based upon national standards and regulations, shall provide a point of contact within the national body governing such standards and regulations in order to allow Purchaser verification and audit.

3. Where such conformance cannot be demonstrated to the satisfaction of the Purchaser, the Purchaser's Pricing Principles will govern.

4. The Contractor shall clearly state whether national standards and rules or the Purchaser's Pricing Principles and formats are the basis for the price proposal.

5. Whether national standards or Purchaser pricing principles are applied, all cost and pricing data shall be verifiable, factual and include information reasonably required to explain the estimating process.

6. The Contractor shall also incorporate provisions corresponding to those mentioned herein in all sub-contracts, and shall require price and cost analysis provisions be included therein.

B. Purchaser's Pricing Principles

1. Allowable cost

A cost is allowable for consideration by the Purchaser if the following conditions are fulfilled:

(a) it is incurred specifically for the Contract or benefits both the Contract and other work or is necessary to the overall operation of the business although a direct relationship to any particular product or service cannot be established and is allocated to them in respective proportion according to the benefit received;

i. Direct Costs
A direct cost is any cost which can be identified specifically with a particular cost objective as generally accepted. Direct costs are not limited to items which are incorporated in the end product as material or labour.

ii. Indirect Costs

An indirect cost is one which is not readily subject to treatment as a direct cost. When presented these costs shall be accumulated in logical cost groupings in accordance with sound accounting principles and the Contractor's established practices. An indirect cost may be allocated to more than one final cost objective. An indirect cost shall not be allocated to a final cost objective if other costs incurred for the same purpose, in like circumstances, have been included as a direct cost of that or any other final cost objective. Such costs shall be presented as overhead rates and be applied to each related direct cost grouping.

(b) The Contractor shall specify the allocation of costs to either of the cost groupings. The method by which costs are accumulated and distributed as part of direct or indirect costs cannot be modified during the duration of the Contract.

(c) it is reasonable and expedient in its nature and amount and does not exceed that which would be incurred by an ordinary prudent person in the conduct of competitive business;

(d) it is not liable to any limitations or exclusion as to types or amounts of cost items as set forth herein.

(e) The Purchaser will review other costs presented against the contract and will determine if they would be allowable.

2. Unallowable Costs

In general all costs which cannot be shown by the contractor to be directly or indirectly of benefit to the Contract are totally unallowable. =Examples of such costs are, among others:

(a) Advertising costs

(b) Costs of remuneration, having the nature of profit sharing.

(c) Costs of maintaining, repairing and housing idle and excess facilities.

(d) Fines and penalties as well as legal and administrative expenses resulting from a violation of laws and regulations.

(e) Losses on other contracts or on expected follow-on contracts

(f) Costs incurred for the creation of reserves for general contingencies or other reserves (e.g. for bad debts, including losses).

(g) Losses on bad debts, including legal expenses and collection costs in connection with bad debts.

(h) Costs incurred to raise capital.

(i) Gains and losses of any nature arising from the sale or exchange of capital assets other than depreciable property.

(j) Taxes on profits.

(k) Contractual penalties incurred.

(l) Commissions and gratuities.

(m) Interest on borrowings.

3. Rates and Factors

(a) The Contractor shall inform the Purchaser of his rates and factors the basis upon which they were computed.

(b) If the Contractor's rates and factors for similar contracts placed with national or international public services have not been established or approved by a government agency or an agency accepted by his government, the Contractor shall provide the necessary data to support the proposed rates.

(c) The term "provisional " used in the title of a rate or factor means a tentative rate established for interim billing purposes pending negotiation and agreement to the final rate or factor.

(d) A rate or factor is pre-determined if it is fixed before or during a certain period and based on (estimated) costs to be incurred during this period. An rate or factor is post-determined if it is fixed after a certain period and based on costs actually incurred during this period. Pre-determined rates or factors shall be agreed upon as final rates whenever possible; otherwise the provisions of paragraph 3c above shall apply pending agreement to post-determined rates or factors.

(e) Such rates or factors shall be determined on the basis of Contractor's properly supported actual cost experience.

(f) If the rates or factors of the Contractor for similar contracts placed by national or international public services have been established or approved by a government agency or an agency accepted by his government and the Contractor proposes the application of these rates, he shall state the name and address of the agency which has accepted or approved the rates and the period for which they were established. If he proposes rates which vary from the rates mentioned above, he shall furthermore provide a justification for the difference.

4. Profit/Benefit

(a) Over the entire life cycle of a given acquisition, Profit and/or Benefit may be subject to negotiation.

(b) Subcontracting profit/benefit amounts are dependent upon the size, nature and oversight needs of the subcontract(s) the prime contractor will use for work performance period.

(c) Profit/benefit is considered by the Purchaser to be directly related to the anticipated risk of the Contractor during the performance of the Contract.

RFQ-CO-115518-NPKI-M

PROVIDE NATO PUBLIC-KEY INFRASTRUCTURE CAPABILITY
NATO PKI – MITIGATION
WP 2 – DATA CENTRE INSTALLATION

BOOK II, PART IV
STATEMENT OF WORK (SOW)

DOCUMENT CONTROL PAGE

VERSION HISTORY

Version	Author	Date	Reason for Change	Superseded Document
0.1	NCIA	Nov 2021		N/A
0.2	NCIA	May 2022		V 0.1
0.3	NCIA	June 2023	Incomplete sections	V 0.2
1.0	NCIA	TBC	Pending release and baseline	

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1 Background

The NPKI Mitigation project is to provide NATO with a set of security services enabling confidentiality, integrity, authentication, and non-repudiation.

The overall aim of the NATO Public Key Infrastructure – Mitigation (NPKI-M) project is to create a new high availability resilient PKI Infrastructure to provide the key and information management functions to other Communication and Information Systems (CIS) security services by means of lifecycle certificate management.

Key to this is establishing the physical infrastructure at the various data centre locations – ensuring full resilience is realized, whilst observing the security compliance obligations, and delivering an adaptable and scalable solution.

1.2 Purpose

This Statement of Work (SOW) describes Purchaser's requirements for the deployment, configuration and operation of NPKI-M hosting capabilities in NATO Headquarters (NHQ) and Mons data centers.

[SOW 1] The Contractor shall observe the project milestones as a priority in its planning and execution of the work.

1.3 Scope

This project provides hosting infrastructures deployed across two datacenters which will support the NPKI-M system. These hosting infrastructures will be replicated to support both production and reference capabilties. The scope of the hosting infrastructures includes virtualization, and infrastructure services. Infrastructure services comprise of operating systems, and applications including databases and connections to existing security services as detailed in this SOW and in PRREF.1 NPKI-M High Level Design (HLD).

The Purchaser will provide all hardware, software and licences as Purchaser Furnished Equipment (PFE), apart from Red Hat which is in scope of the Contractor.

The Period of Performance is 62 weeks from the Effective Date of Contract, plus an additional 52 weeks warranty.

The place of performance is at NCIA facilities; deployments are to be performed at the datacentre locations of SHAPE, Mons (BE) and NHQ, Evere (BE); pre-staging configuration may occur at the CIS Sustainment Support Centre (CSSC), Brunssum (NL); meetings may also be held at additional NCIA facilities such as Braine L'Alleud (BE) and The Hague (NL).

There is no travel envisaged to any other NCIA locations. But all Contractor personnel must hold NATO Security Clearance

[SOW 2] Service provisioning, operations and maintenance shall take place at two NATO data centers; NATO HQ (Evere, BE), and SHAPE (Mons, BE).

[SOW 3] *The Contractor shall provide all necessary resources, including, but not limited to, services, personnel, data, documentation and Red Hat licences in order to discharge its obligations under this SOW.*

1.4 Standards for Interpretation of the SOW

Terminology conventions in this document:

- The term "**the Purchaser**" means the NCI Agency or its authorized representative(s).
- The term "**the Contractor**" means the selected bidder.
- The word "**shall**" in the text expresses a mandatory requirement. Departure from such a task is not permissible without formal written agreement between the Contractor and the Purchaser.
- The expression "**shall not**" means that the definition is an absolute prohibition of the specification.
- The word "**must**" in the text is used for legislative or regulatory requirements (e.g., Health and Safety) with which both the Purchaser and the Contractor shall comply.
- The word "**should**" in the text means something that is strongly encouraged but not mandatory.
- The word "**may**" indicates a permissible practice or action. It does not express a requirement of the Contractor.
- The word "**will**" in the text expresses a provision or service by the Purchaser or an intention by the Purchaser in connection with a requirement of the Contractor. The Contractor is implicitly authorized to rely on such service or intention.

Whenever requirements are stated herein to "**include**" a group of items, parameters, or other considerations, "**include**" means "**include but not limited to**".

Whenever reference is made to a document section, tasks, or paragraph, the reference includes all subordinate and referenced paragraphs.

This SOW invokes a variety of Standard NATO Standardisation Agreements (STANAG), Allied Publications, and Military Standards (MIL-STD). While these are NATO reference documents, there are national and international standards that are considered to be equivalent and are cited as such within these documents.

The Purchaser, however, reserves the right of review should any standards be proposed which had not been cited in the SOW .

2. APPLICABLE DOCUMENTS

2.1. Introduction

[SOW 4] The Contractor shall be aware and comply with the documents listed in Section 2 throughout the execution of its obligations under the Contract.

2.2. NATO Documents

2.2.1. Project specific reference documents

Reference ID	Abbreviation	Full document Name and Reference
PRREF.1	[NPKI-M High Level design]	NPKI-M High Level design, July 2023 , NATO Unclassified.

Table 1 Project specific reference documents

2.2.2. Reference documents for Quality Assurance

Reference ID	*Abbreviation*	*Full document Name and Reference*
QAREF.1	[STANAG 4107, Ed.12]	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications. Ed.12, 2022.
QAREF.2	[AQAP-4107, Ed.A, Ver.1]	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications (AQAP). Ed. A, Ver.1, 2018.
QAREF.3	[AQAP-2000, Ed.3]	NATO Policy on an Integrated System Approach to Quality Through the Life Cycle. Ed.3, 2009.
QAREF.4	[AQAP-2070, Ed.B, Ver.4]	NATO Mutual Government Quality Assurance (GQA). Ed.B, Ver.4, 2019.
QAREF.5	[AQAP-2105, Ed.C, Ver.1]	NATO Requirements for Quality Plans. Ed.C, Ver.1, 2019.
QAREF.6	[AQAP-2110, Ed.D, Ver.1]	NATO Quality Assurance Requirements for Design, Development and Production. Ed.D, Ver.1, 2016.
QAREF.7	[AQAP-2131, Ed.C, Ver.1]	NATO Quality Assurance Requirements for Final Inspection and Test. Ed.C, Ver.1, 2017.
QAREF.8	[AQAP-2210, Ed.B, Ver.!]	NATO Supplementary Software Quality Assurance Requirements to AQAP-2110 or AQAP-2310. Ed.B, Ver.1, 2022.
QAREF.9	[AQAP-2310, Ed.B, Ver.2]	NATO Quality Assurance Requirements for Aviation, Space and Defence Suppliers. Ed.B, Ver.2, 2022.
QAREF.10	[ISO/IEC/IEEE 29148]	Systems and software engineering - Life cycle processes - Requirements engineering, 01 Dec 2011.

Table 2 Quality Assurance Reference Documents

2.2.3. Reference documents for Configuration Management

Reference ID	Abbreviation	Full document Name and Reference
CMREF.1	[STANAG 4427, Ed.3]	Configuration Management in System Life Cycle Management. Ed.3, 2014.
CMREF.2	[ACMP-2000, Ed.A, Ver.2]	Policy on configuration management. Ed.A, Ver.2, 2017.
CMREF.3	[ACMP-2009, Ed.A, Ver.2]	Guidance on Configuration Management. Ed.A, Ver.2, 2017.
CMREF.4	[ACMP-2100, Ed.A, Ver.2]	The Core Set of Configuration Management Contractual Requirements. Ed.A, Ver.2, 2017.
CMREF.5	[ISO 10007:2017]	Quality Management System – Guidelines for Configuration Management. Third edition, 2017.

Table 3 Configuration Management Reference Documents

2.2.4. NATO Security Documents

Reference ID	Abbreviation	Full document Name and Reference
NSECREF.1	[NAC C-M(2002)49-REV1, 2020]	Security within the North Atlantic Treaty Organisation (C-M(2002)49-REV1), 2020
NSECREF.2	[NAC AC/35-D/2000-REV8, 2013]	Directive on Personnel Security (AC/35-D/2000-REV8), 2020
NSECREF.3	[NAC AC/35-D/2001-REV3, 2020]	Directive on Physical Security (AC/35-D/2001-REV3), 2020
NSECREF.4	[NAC AC/35-D/2002-REV5, 2020]	Directive on Security of NATO Classified Information (AC/35-D/2002-REV5), 2020
NSECREF.5	[NAC AC/35-D/2003-REV5-COR1, 2015]	Directive on Classified Project and Industrial Security (AC/35 – D/2003 –REV5-COR1), 2015
NSECREF.6	[NAC AC/35-D/2004-REV3, 2013]	Primary Directive on CIS Security (AC/35-D/2004-REV3), 2013
NSECREF.7	[NAC AC/322-D/0048-REV3 (INV), 2019]	Technical and Implementation Directive on CIS Security (AC/322-D/0048-REV3 (INV)), 2019
NSECREF.8	[NAC AC/35-D/2005-REV3, 2015]	Management Directive on CIS Security (CIS) (AC/35-D/2005-REV3), 2015
NSECREF.9	[NAC AC/35-D/1021-REV3, 2012]	Guidelines for the Security Accreditation of CIS (AC/35-D/1021-REV3), 2012
NSECREF.10	[NAC AC/35-D/1017 –REV3, 2017]	Guidelines for Security Risk Assessment Management (SRM) of Communication and Information Systems CIS (AC/35-D/1017 –REV3), 29 June 2017
NSECREF.11	[NAC AC/35-D/1015 –REV3, 2012]	Guidelines for the Development of Security Requirement Statements (SRSs) (AC/35-D/1015 –REV3), 2012
NSECREF.12	[NAC AC/35-D/1014-REV3, 2012]	Guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for CIS (AC/35-D/1014-REV3), 2012

Reference ID	Abbreviation	Full document Name and Reference
NSECREF.13	[NAC AC/322-N(2011)0130, 2011]	Guidance on the Marking of NATO Information (AC/322-N(2011)0130 Rev1), 2011
NSECREF.14	[NAC AC/322-D(2008)0002, 2008]	INFOSEC Technical and Implementation Supporting Document on Securing Domain Name System Services (AC/322-D(2008)0002), 2008
NSECREF.15	[AC/322-D(2019)0038(INV), 2019]	CIS Security Technical and Implementation Directive for the Secuirty of Web Applications (AC/322-D(2019)0038(INV)), 2019
NSECREF.16	[AC/322-D(2004)0024-REV3-COR1,30 April 2018]	CIS Security Technical and Implementation Directive on the NATO PKI Certificate Policy
NSECREF.17	AD 070-001	ACO Security Directive dated 28 Jan 2019
NSECREF.18	[AC/35-N(2015)0022 (CISS), 2015]	Rules of Engagement for Security Audits of NATO CIS, AC/35-N(2015)0022 (CISS), NATO CIS Security Accreditation Board (NSAB), dated 13 Nov 2015, NATO UNCLASSIFIED.
NSECREF.19	[AC/322-D/0047, 2009]	Infosec Technical and Implementation Directive on Cryptographic Security and Crytpographic Mechanisms, AC/322-D/0047-REV2 (INV), 8 Apr 2009, NATO RESTRICTED.
NSECREF.20	[AC/322-D (2004)0021, 2004]	INFOSEC Technical & Implementation Guidance for Electronic Labelling of NATO Information, 16 March 2004, NATO UNCLASSIFIED.
NSECREF.21	[AC/322-D(2015)0029]	CIS Security Technical and Implementation Guidance on Protecting Authentication Credentials, 27 November 2015, NATO RESTRICTED.
	[NAC AC/322-D(2011)0130 Rev1, 2011]	Guidance on the marking of NATO Information (AC/322-D(2011)0130 Rev1)

Table 4 NATO Security Reference Documents

2.2.5. Other NATO Reference Documents

Reference ID	Abbreviation	Full document Name and Reference
NREF.1	[NAC AC/322-D(2018)0002, 2018]	NATO Architecture Framework (NAF) V.4 (AC/322-D(2018)0002)
NREF.2	[NAC C-M(2009)0021, 2009]	North Atlantic Council Document C-M(2002), "Policy on the Retention and Disposition of NATO Information" 2009
NREF.3	[NAC C-M(2011)0043, 2011]	North Atlantic Council Document C-M(2002) NATO Records Policy, dated 17 June 2011
NREF.4	[NCIA AD 06.03.04, 2016]	Agency Directive AD 06.03.04 Test Verification and Validation - 13 July 2016
NREF.5	AI 16.31.03	Requirements for the Preparation of IPSP
NREF.6	AI 16.31.11	Requirements for the Preparation of TNA Reports
NREF.7	AI 16.31.04	Requirements for the preparation of TRNP
NREF.9	AI 16.31.04 Annex B	Training Feedback Form
NREF.10	AI 16.31.04 Annex C	Training Evaluation Report Form
NREF.11	AI 16.32.04	ABL Template
NREF.12	AI 16.32.05	PBL Template
NREF.13	AI 16.32.02	Preparation of ECP forms
NREF.14	AI 16.32.02 Annex A	ECP Form
NREF.15	AI 16.32.03	Preparation of RFC forms
NREF.16	AI 16.32.03 Annex A	RFC Form

Table 5 NATO Reference Documents

2.2.6. Non-NATO Reference Documents

	Abbreviation	Full document Name and Reference
NNREF.1	[ISO/IEC 15288, 2015]	Systems and software engineering -- System life cycle processes
NNREF.2	[ISO/IEC 12207, 2008]	Systems and software engineering -- Software life cycle processes
NNREF.3	[ISO/IEC 25010, 2011]	Systems and software engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
NNREF.4	[ISO/IEC 29119-1 to 4 2022]	Software and systems engineering — Software testing
NNREF.5	[IEC 60050]	International Electrotechnical Vocabulary (IEV). (www.electropedia.org)
NNREF.6	MIL-HDBK-470A	Designing and Developing Maintainable Products and Systems (1997)
NNREF.7	MIL-HDBK-338B	Electronic reliability design handbook (1998)
NNREF.8	IEC 61078:2016	Reliability block diagrams (2016)
NNREF.9	[AIA/ASD S3000L, 2014]	International Specification for Logistics Support Analysis – LSA. Issue 1.1, 2014.
NNREF.10	[ISO 9001, 2015]	ISO 9000 Series – Quality Management systems - Requirements
NNREF.11	[ISO 9000, 2015]	ISO 9000 Series – Quality Management Principles (Version 2015)
NNREF.12	[ISO 10012, 2003]	ISO 10012 (Version 2003) – Measurement Management Systems – Requirements for measurement processes and measuring equipment
NNREF.13	[IEEE 15288.2, 2014]	IEEE Standard for Technical Reviews and Audits on Defence Programs
NNREF.14	[IETF RFC 2119, 1997)]	Internet Engineering Task Force Request for Comments 2119, "Key Words for Use in RFCs to Indicate Requirement Levels", S. Bradner, IETF, Sterling, Virginia, US, March 1997
NNREF.15	[IETF RFC 5280,2008]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
NNREF.16	AR 700-82/ SECNAVINST 4410.23/ AFMAN 21-106	Joint regulation for SMR coding
NNREF.17	[ISO 9241-210:2019]	Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems
NNREF.18	[ISO/TS 18152:2010]	Ergonomics of human-system interaction — Specification for the process assessment of human-system issues

Table 6 Non-NATO Reference Documents

3. PROJECT MANAGEMENT

3.1. Project Organization

3.1.1. Purchaser Project Organization and Responsibilities

The Project will be managed and subject to review by the Purchaser who will be represented by the NCIA Project Management Team (PMT). The PMT will include NCIA functional elements, including the ACQ Contracting Officer and IPS Officer. It will be chaired by the NCIA Project Manager (PM).

The PMT will be responsible for reviewing the deliverables for the supervision of the implementation and for acceptance of the system. The PMT will constitute the interface with the Contractor.

3.1.2. Contractor's Responsibilities, Organization and Personnel

[SOW 5] *The Contractor shall establish a project management organization for the purpose of performing and managing the efforts necessary to satisfactorily discharge their responsibilities under this Contract.*

[SOW 6] *The Contractor shall also provide the necessary manpower and resources to conduct and support the management and administration of their operations to meet the overall objectives of the contract.*

[SOW 7] *The Contractor shall apply the PRINCE2 project management methodology to the planning and delivery of the capability under this Contract.*

[SOW 8] *Contractor shall provide highlight reports, minutes and attend all project meetings.*

Contractor

[SOW 9] *All of the Contractor resources proposed shall be fluent in English.*

[SOW 10] *Key Personnel are defined as: Project Manager, Technical Lead, Test Director, Quality Assurance Representative (QAR), Integrated Product Support Manager, Security Accreditation Manager and Configuration Manager.Contractor*

3.1.3. Contractor Project Manager (CPM)

[SOW 11] *The Contractor shall designate a CPM, who will direct and coordinate the activities of the Contractor's project team.*

[SOW 12] *The CPM shall be the Contractor's primary contact for the Purchaser's PM and shall conduct all major project design, test, and status reviews.*

[SOW 13] *The CPM shall be prepared at all times to present and discuss the status of Contract activities with the Purchaser's PM, Contracting Officer (CO), or Technical Lead (TL).*

3.1.3.1. Contractor PM Qualifications

[SOW 14] *The Contractor Project Manager shall have at least seven (7) years' experience as the Project Manager for an effort of similar scope, duration, complexity and cost.*

[SOW 15] *The Contractor Project Manager shall have as a minimum a Bachelor's degree in a relevant field such as computer science, information technology, or cybersecurity.*

[SOW 16] *They should hold Professional certifications related to project management methodology such as PRINCE2.*

3.1.4. Contractor Technical Team

[SOW 17] *The Contractor shall designate a Technical Lead (TL) for the project. The TL shall lead the analysis, design, development, integration, and follow-on efforts of the Contractor.*

3.1.4.1. Contractor TL Qualifications

[SOW 18] *The TL shall possess a Master's degree in engineering or computer science or shall have equivalent work experience. The TL shall: have at least seven (7) years' experience in engineering positions associated with the review, design, development, evaluation, planning and operation of networking and communication component parts similar to those being utilised for the purpose of this contract; be a member of a recognized engineering professional body.*

[SOW 19]

3.1.4.2. Contractor Technical Team

[SOW 20] *ContractorContractorContractorContractorThe Contractor shall designate a team of technical Subject Matter Experts (SME) for the installation, implementation, configuration and integration activities conducted under this Contract.*

[SOW 21] *SMEs designated by the Contractor shall demonstrate expert level of knowledge, capability and experience to meet the requirements of this contract mainly including but not limited to the below topics:*

a. *Complex TCP/IP based secure network infrastructure;*
b. *Virtualization techniques and technologies;*
c. *Windows Server, Linux (RHEL) and VMWare in HA configurations;*
d. *Development, enhancement and implementation of security settings relating to any of Cisco, Linux (RHEL), Unix, Microsoft operating systems;*
e. *Cisco switch installation, configuration and support including traffic flow and log analysis;*
f. *Palo Alto Firewall installation, configuration including IPsec VPN and support including traffic flow and log analysis;*
g. *SAN server installation, configuration and support;*
h. *VEEAM back up installation, configuration and support;*
i. *High availability (HA) deployment of PostgreSQL database services;*

j. *Red Hat Directory Servers installation, configuration and support;*

k. *Troubleshooting with flexibility and success across varying technology platforms such as Windows and Linux in both physical and virtual environments;*

l. *In depth understanding of network diagnostic, monitoring and analysis tools including but not limited to Solarwinds and Zabbix;*

m. *In depth understanding of SMC tools including but not limited to SCCM, SCOM and Trellix EPO;*

n. *Building hardware and software configurations and preparing system components for integration to the Purchaser's existing SMC, monitoring and logging capabilities;*

o. *Create and maintain detailed IT documentation;*

p. *Detailed understanding of NATO CIS security and/or NATO security services use across NATO Enterprise.*

3.1.5. Contractor Test Director

[SOW 22] *The Contractor shall designate a Test Director for all test activities conducted under this Contract. The Test Director shall direct test planning, design and tools selection, establish guidelines for test procedures and reports, and co-ordinate with the Purchaser on test support requirements and manage the Contractor test resources.*

3.1.5.1. Contractor Test Director Qualifications

[SOW 23] *The Contractor Test Director shall have at least Seven (7) years' experience in the design and execution of communication information systems tests.*

[SOW 24] *The Contractor Test Director shall have as a minimum a Bachelor's degree in a relevant field such as computer science, information technology, or cybersecurity.*

[SOW 25] *They should hold Professional certifications related to testing methodology such as ISTQB.*

3.1.6. Contractor Quality Assurance Representative

[SOW 26] *The Contractor shall designate a qualified individual to serve as the Contractor Quality Assurance Representative (CQAR), who will act as the Quality Assurance Manager for activities under this Contract. The CQAR shall report to a separate manager within the Contractor's organization at a level equivalent to or higher than the PM.*

3.1.6.1. Contractor Quality Assurance Representative Qualifications

[SOW 27] *The Quality Assurance Manager shall have at least four (4) years' experience in working with quality control methods and tools and ideally have a knowledge of NATO Standards (e.g. STANAG 4107 Ed. 11) or equivalent, processes and procedures applicable to Quality Assurance (QA) and Quality Control (QC) in the industry. The CQAR shall be independent from the project team and be involved in any project review, acceptance and delivery.*

[SOW 28] *The Quality Assurance Manager shall have as a minimum a Bachelor's degree in a relevant field such as computer science, information technology, or cybersecurity.*

3.1.7. Contractor Integrated Product Support (IPS) Manager

[SOW 29] *The Contractor shall designate an IPS Manager.*

[SOW 30] *The Contractor IPS Manager shall lead all Contractor's activities for the development of IPS deliveries as detailed in Section 5, and coordinate with Purchaser's IPS Officer on all decisions deliverables, templates and data pertinent to IPS processes, procedures and activities.*

3.1.7.1. Contractor IPS Manager Qualifications

[SOW 31] *The Contractor IPSM shall have a bachelor's degree or equivalent certification in supportability engineering.*

[SOW 32] *The Contractor IPSM shall have at least seven (7) years' experience in supportability engineering for hardware/software intensive products, preferably in the in defence and electronics sector.*

[SOW 33] *The Contractor IPSM shall have knowledge of the IPS related NATO standards (ALP-10, Allied Logistics Publications), handbooks, ISO standards and the ASD/AIA/ATA suite and tools.*

[SOW 34] *The Contractor IPSM shall have experience in all the fields of IPS – e.g. LSA (Logistics Support Analysis), RAM&T (Reliability, Availability, Maintainability and Testability), training, IETP (Interactive Electronic Technical Publications), supply support, PHST (Packaging, Handling, Storage and Transportation).*

3.1.8. Contractor Security Accreditation Manager

[SOW 35] *The Security Accreditation Manager shall have at least seven (7) years' experience in managing security accreditation processes within NATO or similar defense organizations.*

3.1.8.1. Contractor Security Accreditation Manager Qualifications

[SOW 36] *The Security Accreditation Manager shall have as a minimum a Bachelor's degree in a relevant field such as computer science, information technology, or cybersecurity. They should hold Professional certifications related to information security and accreditation, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or equivalent. They should have extensive knowledge of NATO security policies, standards, and procedures, including NATO Security Policy Manual (NSPM) and Allied Joint Publication (AJP)-33, or equivalent from other similar organizations.*

3.1.9. Contractor Configuration Manager

[SOW 37] *The Contractor shall designate a Configuration Manager for the project.*

[SOW 38] *The Contractor Configuration Manager shall be responsible for the preparation and execution of the entire set of configuration management processes and procedures*

(planning, identification, change management, accounting and verification & audit) in accordance with configuration management standards in Section 0, Table 3.

3.1.9.1. Contractor Configuration Manager Qualifications

[SOW 39] *The Contractor Configuration Manager shall have a Configuration Management Principles and Implementation Certification (CMPIC) courses 1-4 , or equivalent.*

[SOW 40] *The Contractor Configuration Manager shall have at least seven (7) years of proven experience in specifying configuration management requirements, standards, and evaluation criteria in acquisition documents, and in performing configuration identification, control, status accounting, and audits.*

ContractorContractorContractorContractor

3.2. Project Management Documentation

[SOW 41] *The Contractor shall provide a Project Management Plan (PMP) and control process to ensure management visibility and effective coordination from project startup through the cost-effective delivery of high quality services, contract transition and closeout, and shall adhere to all NATO regulations and directives. The Project Plan shall include all elements and processes to be used for successful execution of this project to include Startup, Schedule Management, SubContractor Management, Quality Control, Financial Control, Issue Escalation, Risk Management, Transition-Out, and Closeout.*

[SOW 42] *A draft Project Plan shall be submitted with the Contractor's proposal and a final version 30 calendar days after CAW.*

Deliverable: PMP

3.3. Integrated Master Schedule

[SOW 43] *The Contractor shall develop a single Integrated Master Schedule (IMS) to include each exercised task area that contains all of the technical and functional activities required to complete the tasking and deliver the first IMS within 14 calendar days of Effective Date of Contract (EDC) and updated each month thereafter to reflect the execution and completion of scheduled events.*

[SOW 44] *The Contractor shall deliver an IMS with at least three levels of definition sufficient to allow for tracking the completion of scheduled events, duration, and inter-relationships between events. The IMS will be baselined, through deliverable acceptance, within the first 30 days of award and changes cannot be made to baselines without concurrence from the Purchaser's PM in conjunction with other NPKI-M Project Leads. Any anticipated changes to the IMS shall be communicated within 24 hours of the identification of the change. This notification shall include identified impact factors and potential recovery mechanisms.*

[SOW 45] *The Contractor shall attend and be able to talk to the full IMS scope in a weekly PM Alignement IMS meeting to include risks to the schedule, recommended adjustments to the schedule as well as any external factors that have occurred that impacted the schedule. The Contractor shall provide meeting minutes from these meetings to include line changes, impact of change, and Purchaser acceptance date of the change.*

[SOW 46] *ContractorContractorContractorContractorThe Contractor shall produce an IMS Plan on a Page (IMSPOAP) representing the whole project as detailed in the IMS.*

[SOW 47] *The IMSPOAP shall be produced in Microsoft Visio Format, and be updated on a monthly basis as part of the Project Status Reporting cycle.*

Deliverable: IMS and IMSPOAP

3.4. Cyber Incident Management Plan

[SOW 48] *The Contractor shall be required to deliver a Cyber Incident Management Plan (CIMP) that is aligned to cyber security controls in line with NATO Security Policy and its supporting directives – see Annex C.3 for details.*

3.5. Documentation

[SOW 49] *The Contractor shall submit all documents listed in the following table based on the timelines defined provided.*

Serial	Name	Description	SOW Reference	To be completed by	Format
1	PMP	Project Management Plan	3.3	EDC+2 weeks	DOCX
2	MSR	Monthly Status Report	3.6.1	Monthly	DOCX
3	RISK*	Risk Log	3.8	EDC+2 weeks	XLSX**
4	ISSUE*	Issue Log	3.7	EDC+2 weeks	XLSX**
5	IMS*	Integrated Master Schedule	3.3	EDC+2 weeks Updated monthly	MPP
6	IMSPOAP*	Integrated Management Schedule Plan on a Page	3.30	EDC+2 weeks Updated monthly	VSDX
7	IPSP	Integrated Product Support Plan	5.2	EDC+4 weeks	DOCX XLSX
8	QAP	Quality Assurance Plan	90	EDC+4 weeks	DOCX
9	CMP	Configuration Management Plan	8	EDC+4 weeks	DOCX XLSX
10	TRNP*	Training Plan	5.6	Draft: EDC+4 weeks Final: CDR	DOCX XLSX
11	TNA	Training Needs Analysis	5.6	Draft: PDR Final: CDR	DOCX XLSX
12	ABL*	Allocated Baseline	8	Initial: PDR Final: CDR	CMDB dump XLSX
13	PBL*	Product Baseline	8	Initial: CDR First formal: CDR + 4W	CMDB dump XLSX
14	MTP	Master Test Plan	6.3 6.3.1	Initial: PDR Final: CDR	DOCX
15	ETP*	Event Test Plan	6.3 6.3.3	1 month before test event	DOCX
16	RTM	Requirements Traceability Matrix	6.3 6.3.4	First with MTP and update per test event	XLSX
17	IPS Case Report	IPS Case Report	5	CDR and revisions	DOCX XLSX
18	S3000L Tailoring	S3000L Tailoring	5.3	PDR	DOCX XLSX
19	TR-Templates	Training Templates and Formats	5.6	CDR and revisions	DOCX PPTX PDF
20	S3000L Data*	LSA/RMA Data (part of the IPS Case Report)	5.3	CDR + 4W and revisions	XML

Serial	Name	Description	SOW Reference	To be completed by	Format
21	Site inventory (includes SWDL)*	Site inventory (includes SWDL)	5.5.3	Initial: SiAT – 1W Final: PSA – 1W	XLSX DOCX
22	TR-MAT*	Training Material	5.6	Initial: Training Start – 8W Final: Training Start – 2W	DOCX PPTX PDF SCORM
23	ABDs and ICDs*	As Built Documentation (ABD) and Interface Control Documents (ICD)	5.5.4	PSA – 4W	DOCX XLSX VSD PDF
24	TR	Test Report	6.3 6.3.5	1 week after each test event	DOCX
25	SIP	Site Implementation Plan	4.5	4 weeks before each site deployment	DOCX
26	SIS	Site Installation Specification (updated and validated)	4.2.1	The (updated and validated) SIS will be submitted as a Draft 4 weeks before each site deployment. Final 2 weeks after each site deployment	DOCX
27	DP	Deployment Plan (in support of Change Requests)	4.5	4 weeks before each site deployment	DOCX
28	SDS	System Design Specification (Low Level Design)	4.4.1.1	CDR	DOCX
29	Dry Run Report/Engineering report	Dry Run Report/Engineering report (evidence documents)	6.4.1	1 week before TVVA Event	DOCX
30	PSA Protocol	PSA Protocol (collection of evidence documents)	4.2.2.1	PSA + 1W	Various formats
31	FSA Protocol	FSA Protocol (collection of evidence documents)	4.2.2.2	FSA – 1W	Various formats
32	Lessons Learned Report	Lessons learned and Identified report	4.4.2.2	FSA + 1W	DOCX
33	Test Completion Report	Test Completion Report (evidence documents)	6.3.5	1 week after TVVA event	DOCX
34	CISD	CIS Description	4.6.1.1	FSA – 1W	DOCX
35	SRA	Security Risk Assessment (SRA) input	4.6.1.2	FSA – 1W	DOCX
36	SSRS	System-specific Security Requirements Statement (SSRS)	4.6.1.3	CDR	DOCX
37	STVP	Security Test & Verification Plan (STVP) input	4.6.1.4	1 week before TVVA Event	DOCX
38	STVR	Security Test Verification Report (STVR) –test result recordings	4.6.1.5	1 week after TVVA Event	DOCX XLS

Serial	Name	Description	SOW Reference	To be completed by	Format
39	SecOps	Security Operating Procedures (SecOPs) input	4.6.1.6	CDR	DOCX
40	CIMP	Cyber Incident Mnagament Plan	Annex C.3	PSA	DOCX

Documents marked with an asterisk* are living documents and shall be updated throughout the life of the project.

[SOW 50] Documents shall be mastered in the SharePoint Portal provisioned by the Purchaser.

[SOW 51] All documents shall conform to the file naming and versioning standards identified in Section 8 of this SOW.

[SOW 52] Exceptions to the documents naming convention shall apply to S1000D data/exports and CMDB (Configuration Management Database) exports, based on the capabilities of the relevant Contractor data/product management tools.

Contractor

3.5.1. Documentation Review and Acceptance

[SOW 53] The Contractor shall submit all documentation in electronic format to the Purchaser for review and comments as applicable via the project portal.

[SOW 54] The Contractor shall not provide any documentation in a partial or gradual manner.

[SOW 55] The Contractor shall ensure that any documentation delivered to the Purchaser has been properly reviewed according to Contractor quality management process.

[SOW 56] Except otherwise stated for specific documents, the following provisions shall apply for any documentation to be provided by the Contractor under this Contract.

[SOW 57] The Contractor shall provide a first version (version 0.1) of each deliverable for Purchaser review. The first version shall be substantially complete and correct.

The Purchaser will provide questions, comments, corrections, and suggested changes to the Contractor within 10 (ten) working days of receipt. The Purchaser reserves the right to return without review a document that has significant deficiencies (e.g. a document only including a table of contents).

[SOW 58] The Contractor shall not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.

[SOW 59] The Contractor shall resubmit the document as a revised version (version 0.2) incorporating the modifications, additions and expansions required by the Purchaser, within 10 (ten) working days after receipt.

[SOW 60] The Contractor is encouraged to arrange a meeting during this period to discuss the findings if necessary and to better understand the Purchaser's expectations.

The Purchaser will provide comments, corrections, and suggested changes to the Contractor within 10 (ten) working days of receipt.

[SOW 61] The Contractor is encouraged to arrange a follow up meeting during this period to discuss the findings if necessary and to better understand the Purchaser's expectations.

[SOW 62] The Contractor shall provide a revised version (version 0.3) of the document within 10 (ten) working days of receipt of the Purchaser's comments on the revised version.

[SOW 63] *If the Purchaser is satisfied that a document is complete and correct, then the Contractor will be invited to update the document to version 1.0. This version will then be digitally signed in PDF format if applicable by the Contractor and Purchaser Project Managers.*

The Purchaser reserves to the right to exercise Articles defined in the Special Provisions should the second review cycle of a document be insufficient to a quality level deemed acceptable by the Purchaser.

[SOW 64] *Any delays to the project as a result of additional or delayed review cycles will be the responsibility of the Contractor – subject to agreement by the Purchaser Project Manager.*

The Purchaser reserves the right to require the Contractor to make further changes to any document, to correct any errors detected during the implementation or to reflect any technical or contractual changes necessary as a result of any supplemental agreement made to the contract.

[SOW 65] *If a document is anticipated to be updated throughout the duration of the project (such as the IMP or IMS), the Contractor shall remain responsible for updating the document in the course of the project (to correct errors, inconsistencies, omissions, and to reflect changes in the system design, system implementation, support arrangements) as part of its Configuration Management tasks. These documents, once accepted will not be subject to the review cycle process.*

[SOW 66] *The Purchaser reserves the right to request one additional cycle of review for each document should the Contractor not incorporate all the modifications, additions and expansions required by the Purchaser. Any delays to the project will be the responsibility of the Contractor.*

3.6. Project Controls

3.6.1. Monthly Status Reports

[SOW 67] *The Contractor shall provide a Monthly Status Report (MSR), five (5) working days prior to the Project Review Meeting (PRM).*

[SOW 68] *Failure to submit the MSR onto the project portal 5 working days prior to the PRM may result in a delay of the PRM – any additional costs or impacts as a result of this delay will be borne by the Contractor.*

[SOW 69] *The Contractor shall submit an MSR that addresses adherence to the Best Management Practices, in a format mutually agreed upon with the Purchaser. The MSR shall describe tasks, progress, quality, risks, customer feedback, any potential problems, accomplishments, and issues from the reporting period of the MSR for each of the exercised task areas against the IMS. At a minimum, this data shall include:*

[SOW 70] *A brief description of activities and deliverables performed during the reporting month by Task Area. This description shall include problem definition and recommendations for program resolution. Particular attention shall be given to risk management and cyber security activities.*

[SOW 71] *Rolling 90-Day Action plan*

[SOW 72] *Brief description of issues, challenges, or problems identified during the reporting period.*

[SOW 73] *Description of the outcome of any trips, technical visit, and related results for the reporting period.*

[SOW 74] *Identification of key personnel and personnel reassignments including personnel added or removed.*

[SOW 75] *The Contractor shall provide an updated Purchaser Furnished Equipment (PFE) list.*

[SOW 76] *Organizational report to include an overarching organization personnel hierarchy, and a subsequent page with an employee/personnel listing to show name, email, and phone number aligned to Labor Category and Prime vs Sub-Contractor (when applicable).*

[SOW 77] *The Contractor shall proactively identify and prioritize risks and alternative Course of Actions (COAs) sufficiently in advance to permit Purchaser intervention and action before a risk becomes an issue, as well as identify best practices and lessons learned.*

[SOW 78] *Process improvement recommendations – this can be related to the specific projects or just overall business improvements*

The Purchaser will by mutual agreement with the Contractor amend the content, format and regularity of the MSR throughout the life of the project.

3.6.2. Project Meetings

[SOW 79] *Except otherwise stated in the Contract, the following provisions shall apply to all meetings to be held under the Contract.*

[SOW 80] *The Contractor shall be required to attend recurring meetings in support of the NPKI-M project. These meetings will fall into 2 categories: participant and meeting support. Currently the NPKI-M project has 4-6 weekly recurring meetings that will need participation. Additionally, there are 1-2 monthly meetings and 1-2 quarterly meetings that are also expected to be supported.*

[SOW 81] *Meetings shall take place at NCI Agency premises in SHAPE (Mons), Braine L'Alleud, NHQ (Evere) or The Hague. However, at the discretion of the Purchaser PM, alternative locations (including Contractor or neutral locations), or virtual meetings may be permitted.*

[SOW 82] *The Contractor shall submit a meeting request and meeting agenda 5 working days prior to any meeting. However, at the discretion of the Purchaser PM, meetings may be arranged with shorter notice.*

[SOW 83] *When participating in meetings, the Contractor is expected to act in a professional manner. When the Contractor is providing meeting support, the Contractor will need to prepare the meeting agenda, briefing materials, coordinate participants and venue (in person or virtual) prior to the meeting.*

[SOW 84] *The Contractor shall take meeting minutes with action item tracking, submit them in draft version to the Purchaser for approval within 3 working days of the meeting, on the Project Portal, as well as notifying the Purchaser PM and relevant Purchaser SME as appropriate (such as Test Director or QAR) by email.*

[SOW 85] *The Purchaser will respond within 3 working days of receipt of the draft minutes, and subject to Purchaser approval, the Contractor shall finalise the minutes in the project portal.*

[SOW 86] *The participants shall not regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract, or as a vehicle to alter the design or configuration of equipment or systems.*

[SOW 87] *Any documentation, even in draft format, that may be useful to the Purchaser in preparing for meetings and ensuring efficient discussions during the meetings shall be provided to the Purchaser no later than 2 working days before the meeting.*

3.6.2.1. Project Kick-Off Meeting

[SOW 88] *The CPM shall participate in the NPKI-M project kick-off meeting with the Purchaser's Project Team no later than two weeks after EDC. The meeting shall be arranged by the Purchaser, and shall be held at an appropriate NCIA facility (subject to discretion by the Purchaser PM).*

[SOW 89] *The Contractor shall propose which resources shall be in attendance (including Sub-Contractor personnel). This shall be agreed by the Purchaser PM in advance 2 weeks prior to the meeting.*

[SOW 90] *The Contractor (and Sub-Contractor) Project personnel shall introduce themselves, and explain which project deliverables they are accountable for and what work they are responsible for.*

[SOW 91] *The CPM shall explain how the Contractor intends to manage the project delivery approach for all project aspects.*

[SOW 92] *The Contractor's Technical Lead shall introduce how the Contractor intends to fulfil the technical design and implementation work (as described in Section 4).*

[SOW 93] *The Contractor's IPS manager shall introduce how the Contractor intends to fulfil the IPS scope of work (as described in Section 5).*

[SOW 94] *The Contractor's Test Director shall introduce how the Contractor intends to fulfil the Testing scope of work (as described in Section 6).*

[SOW 95] *The Contractor's Quality Assurance Representative shall introduce how the Contractor intends to fulfil the Quality Assurance scope of work (as described in Section 7).*

[SOW 96] *The Contractor's Configuration Manager shall introduce how the Contractor intends to fulfil the Configuration Management scope of work (as decribed in Section 8).*

3.6.2.2. Design Review Meetings

[SOW 97] *The Contractor shall co-ordinate the Design Reviews.*

[SOW 98] *Meetings shall take place at NCI Agency premises. However, at the discretion of the Purchaser PM, alternative locations or virtual meetings may be permitted.*

[SOW 99] *In addition to the scope and requirements for design reviews as described in Section 4, the Contractor shall provide the following, if applicable, at all design reviews:*

- *Changes to the IMS*
- *Risk assessment of proposed changes, and an update of the Risk Log*

and Issue Logs

3.6.2.3. Project Review Meetings

[SOW 100] *The Contractor shall coordinate and host the Project Review Meetings (PRM) with the Purchaser.*

[SOW 101] *The PRM shall be held at least once a month throughout the Period of Performance, and once every three (3) months during the warranty period.*

[SOW 102] *The Contractor shall provide an MSR, five (5) working days prior to each PRM, as per Section 3.5.2.3.*

[SOW 103] *The Contractor shall submit a meeting request no later than 5 working days prior to the PRM.*

[SOW 104] *Project delivery problems shall be identified, discussed and escalated with the Purchaser PM promptly, and shall not be backed up until the next PRM.*

[SOW 105] *The PRMs shall be conducted at NCI Agency premises. However, at the discretion of the Purchaser PM, alternative locations or virtual meetings may be permitted. SHAPE (Mons) shall be considered the primary location to conduct the PRMs. However, the location of PRMs may vary and, where possible, be scheduled with other project meetings.*

[SOW 106] *The PRM shall be held on the first Tuesday of each month. Deviation from this is subject to approval by the Purchaser PM.*

[SOW 107] *The Contractor shall conduct a PRM once a month throughout the Contract period of performance and once a quarter during the warranty period (if required). This cadence may increase or decrease if deemed necessary by the Purchaser.*

3.6.2.4. Other Meetings

The Purchaser will host all other meetings unless there is a specifically agreed need to review material, witness technical demonstrations or testing, or perform any other activity outside of the Purchaser's premises, as part of the meeting.

[SOW 108] The Contractor shall identify to the Purchaser's PM any other meetings with NATO personnel required to support this Contract.

[SOW 109] Upon approval by the Purchaser's PM, the Contractor shall schedule, organize, and conduct such meetings.

3.7. Risk Management

[SOW 110] The Contractor shall establish and maintain an overall Risk Management process for the project.

[SOW 111] This Risk Management process shall identify all risks (management, technical, schedule, and cost risks), evaluate each risk, and select a proposed response for each risk.

[SOW 112] Evaluating each risk shall result in the risk being rated as High, Medium, or Low, based on its probability and impact.

[SOW 113] For each risk, the proposed response shall be selected from the following list:

- ***Prevention**: Terminate the risk by doing things differently and thus removing the risk, where it is feasible to do so. Countermeasures are put in place that either stop the threat or problem from occurring or prevent it from having any impact on the project or business.*
- ***Reduction**: Treat the risk by taking action to control it in some way where the action either reduces the likelihood of the risk developing or limits the impact on the project to acceptable levels.*
- ***Acceptance**: Tolerate the risk – e.g. if nothing can be done at a reasonable cost to mitigate it or the likelihood and impact of the risk occurring are at an acceptable level.*
- ***Contingency**: plan and organize actions to come into force as and when the risk occurs.*
- ***Transference**: Pass the management of the risk to a third party (e.g. insurance policy or penalty clause), such that the impact of the risk is no longer an issue for the health of the project.*

3.8. Risk Log

[SOW 114] The Contractor shall create a Risk Log in the SharePoint Portal, and shall be responsible for maintaining the log throughout the project.

[SOW 115] The Risk Log shall be a table listing the risks, and shall include the following information:

- *Risk identifier: unique code to allow grouping of all information on this risk*
- *Description: brief description of the risk*
- *Risk category (e.g. commercial, legal, technical)*

- *Impact: effect on the project if this risk were to occur*
- *Probability: estimate of the likelihood of the risk occurring*
- *Proximity: how close in time is the risk likely to occur*
- *Countermeasure(s): what actions have been taken/will be taken to counter this risk*
- *Owner: who has been appointed to keep an eye on this risk*
- *Author: who submitted the risk*
- *Date identified: when was the risk first identified*
- *Date of last update: when was the status of this risk last checked*
- *Status: e.g. dead, reducing, increasing, no change*

3.9. Issue Management

An issue is anything that has already been realised, but may not have been previously identified in the Risk Log.

An issue will have an impact on the Project or dependent projects, either detrimental or beneficial (change request, problem, error, anomaly, risk occurring, query, change in the project environment).

[SOW 116] The Contractor shall create an Issue Log in the SharePoint Portal, and shall be responsible for maintaining the log throughout the project.

[SOW 117] The Issue Log shall be a table and shall comprise the following information:

- *Project Issue Number*
- *Project Issue Type (Request for change, Off-specification, general issue such as a question or a statement of concern)*
- *Author*
- *Date identified*
- *Date of last update*
- *Description*
- *Action item*
- *Responsible (individual in charge of the action item*
- *Suspense date (Suspense date for the action item)*
- *Priority*
- *Status*

[SOW 118] The Issue Log can be combined with the Risk Log for ease of administration.

3.10. Independent Verification, Validation and Quality (IVVQ)

[SOW 119] The Contractor will engage with the Purchaser's IVVQ team for this project. The main objective of the IVVQ activities will be the evaluation of the performance of the

Contractor and the verification of the work being performed under the related effort, in particular evaluation of Contractor deliverables and testing activities.

[SOW 120] *IVVQ will also monitor, assess, and report on the Contractor's performance in order to identify, as early as possible, perceived problem areas.*

[SOW 121] *The Contractor shall transfer to IVVQ all information deemed necessary to perform the IVVQ activities, on their own initiative or on request by the Purchaser.*

3.11. Project Portal

[SOW 122] *The Contractor shall utilise a Project Portal, provided by the Purchaser, on which all relevant (classified up to NATO RESTRICTED) project documentation and datasets shall be maintained.*

[SOW 123] *The Contractor shall be able to access the Portal using the Purchaser provided REACH.*

[SOW 124] *The portal shall be used as the master repository for all project documentation, in all versions of completion.*

[SOW 125] *The documents posted to the portal shall clearly indicate the version number inside the document.*

[SOW 126] *The Contractor shall keep the portal up to date, in support of access by the users, or the Purchaser, through the project period of performance, the warranty period as appropriate, and any subsequent extensions, subject to approval from the Purchaser.*

3.12. Co-ordination with other NATO projects and Operational capacity

The NATO CIS environment is under continual development by other NATO projects that are being implemented in parallel with the project. Potential changes for example could include, but are not limited to, firewall version updates, switch vendor changes, version updates to the software baselines in the SRS or HLD. These changes are not expected to increase the scope or complexity of tasks for the Contractor to perform.

The Purchaser will inform the Contractor and provide information concerning the changes to the operational environment that may emerge as a result of these projects (as relevant).

[SOW 127] *The Contractor shall attempt to accommodate any related changes at no additional cost or schedule impact to the project. Contractor*

4. TECHNICAL SCOPE

4.1. Technical Requirements

4.1.1. The NPKI-M project will deliver a public key infrastructure system covering:

- Two datacenters (DC) in Belgium; NATO Headquarters (NHQ), Evere and SHAPE, Mons for production environments
- Two separate production infrastructures to cover NATO Secret (NS) and NATO Unclassified (NU)/NATO Restricted (NR) security domains in each datacenter (4 production installations)
- Each installation consists of a layered Infrastructure with firewalls separating the Front End PKI services from multiple back end PKI service zones and a second layer of firewalls separating front end PKI services from external systems
- Two reference environments fully replicating the functionality and installations of the two production infrastructures and two security domains; to be located in Mons (4 Reference installations)

4.1.2. This work package provides for the following elements to be installed within each installation:

- Racking and cabling of all equipment required to implement the NPKI-M system
- Provision of cabling where not already available in the rack
- Establishment of Virtual LANs (VLAN)
- Build and configure of Hosting Platform services consisting of two physically separate VMWare infrastructures per installation
- Establishing High availability (HA) for all components between datacenters
- Installation and configuration of two HA PostgreSQL services and configuration of automated failure detection and HA failover and recovery (2 sets of 2 PostgreSQL servers per installation)
- Installation and configuration of Red Hat Enterprise Linux (RHEL) 389 Directory Servers and configuration of automated failure detection and HA failover and recovery for each of the two VMware infrastructures per installation
- Installation and configuration of infrastructure services, proxies and other applications covering the entire installation
- Establishment of all virtual machines described in this HLD
- Installation of specific set of network interconnections which will provide services across the NATO enterprise
- Validating the firewall rulesets for required communications between all VLANs, Operating systems, and applications identified in the NPKI-M HPS SOW and HLD

[SOW 128] *The Contractor shall procure the necessary Red Hat Enterprise Linux (RHEL) 389 Directory Server Software and Licences required to create the necessary platform to support the automated failure detection and HA failover and recovery for each of the two VMware infrastructures per installation. All Red Hat procurements must include a lifetime including warranty until FSA+12 months.*

4.1.3. Each installation consists of two physically separated virtualization infrastructures providing the following services.

4.1.3.1. Core PKI VMware infrastructure consisting of the following virtualized zones:

- Management, Control, and Production zones (Core Zones);
- Physical Hardware Security Module (HSM) zone;
- Physical Out of Band (OOB) management switch for the Management Zone.

4.1.3.2. Front End services consisting of the following virtual domains:

- Externally accessible Front End service zone;
- Second Externally accessible Front End (limited) NU services zone. This zone is not applicable to the NS security domain;
- Connection to Core Management zone, via the OOB switch.

Annex A – System Requirements Specifications (SRS) details the scope of project requirements.

4.2. Milestones

The project is split into six key deliverable milestones to cover the whole project delivery phase, plus a final milestone for the conclusion of the warranty period.

[SOW 129] The Contactor shall adopt a flexible deployment planning approach to accommodate for any changes in the order of the implementation milestones, under the discretion of the Purchaser PM.

[SOW 130] The Contractor shall explore opportunities to execute the implementation milestones in parallel, to accelerate the completion. However, deployment activities that require to be run in parallel shall be approved by the Purchaser PM to ensure that the Purchaser resources can support the approach.

[SOW 131] The Contractor shall deliver the milestones as per the delivery dates detailed in the table below.

Milestone	Description	Delivery Date
0	Design Reviews (CDR)	EDC + 16 weeks
1	Reference Environment High Side (PSA-1)	EDC + 22 weeks
2	Reference Environment Low Side (PSA-2)	EDC + 28 weeks
3	Production Environment High Side (PSA-3)	EDC + 43 weeks
4	Production Environment Low Side (PSA-4)	EDC + 58 weeks
5	Final System Acceptance (FSA)	EDC + 62 weeks
6	System Warranty	FSA + 52 weeks

Table 7 Milestone Dates

4.2.1. Milestone 0 – Design Reviews

This milestone may only be regarded as complete once the Critical Design Review (CDR) has been electronically signed as approved by the Purchaser PM as per the document review process detailed in Section 4.3.1.2.

[SOW 132] *Acceptance of the CDR shall be absolute – no caveats are to be granted by the Purchaser in the interests of maintaining the schedule.*

[SOW 133] *The Contactor may not initiate any subsequent implementation milestone deployment activities until such time as Milestone 0 has been approved by the Purchaser PM.*

4.2.2. Milestone 1 – Preliminary Site Acceptance (PSA-1) – Reference environment (High Side)

[SOW 134] *The PSA-1 Acceptance Criteria shall have been achieved without exception, as per SOW section 4.3.2.1. This will include the conclusion of the test cases and that no critical, high, or medium defects remain un-remediated.*

[SOW 135] *The completion of the Reference environment (High Side) PSA-1 milestone represents the transition of the capability from project development to Operational capability, and as such the early warranty for this environment initiates at this milestone. Therefore the aspects of service transition are also included in the PSA acceptance criteria – which shall also include training and other associated IPS documentation.*

4.2.3. Milestone 2 – Preliminary Site Acceptance (PSA-2) – Reference environment (Low Side)

[SOW 136] *The PSA-2 Acceptance Criteria shall have been achieved without exception, as per SOW section 4.3.2.1. This will include the conclusion of the test cases and that no critical, high, or medium defects remain un-remediated.*

[SOW 137] *The completion of the Reference environment (Low Side) PSA-2 milestone represents the transition of the capability from project development to Operational capability, and as such the early warranty for this environment initiates at this milestone. Therefore the aspects of service transition are also included in the PSA acceptance criteria – which shall also include training and other associated IPS documentation.*

4.2.4. Milestone 3 – Preliminary Site Acceptance (PSA-3) – Production environment (High Side)

[SOW 138] *The PSA-3 Acceptance Criteria shall have been achieved without exception, as per SOW section 4.3.2.1 This will include the conclusion of the test cases and that no critical, high, or medium defects remain un-remediated.*

[SOW 139] *The completion of the Production environment (High Side) PSA-3 milestone represents the transition of the capability from project development to Operational capability, and as such the early warranty for this environment initiates at this milestone. Therefore the aspects of service transition are also included in the PSA acceptance criteria – which shall also include training and other associated IPS documentation.*

4.2.5. Milestone 4 – Preliminary Site Acceptance (PSA-4) – Production environment (Low Side)

[SOW 140] *The PSA-4 Acceptance Criteria have been achieved without exception, as per SOW section 4.3.2.1. This will include the conclusion of the test cases and that no critical, high, or medium defects remain un-remediated.*

[SOW 141] *The completion of the Production environment (Low Side) PSA-4 milestone represents the transition of the capability from project development to Operational capability, and as such the early warranty for this environment initiates at this milestone. Therefore the aspects of service transition are also included in the PSA acceptance criteria – which shall also include training and other associated IPS documentation.*

4.2.6. Milestone 5 – Final Site Acceptance

Final Site Acceptance (FSA) can only be achieved after all PSA milestones (1-4) have been achieved and approved by the Purchaser PM.

[SOW 142] *The FSA shall be achieved no later than 4 (four) weeks after the final PSA has been approved.*

[SOW 143] *Approval of the FSA shall be absolute – no caveats are to be granted by the Purchaser in the interests of maintaining the schedule – subject to the discretion of the Purchaser PM.*

4.2.7. Milestone 6 – System Warranty

[SOW 144] *The scope of the overall warranty is defined in Section 0.*

[SOW 145] *The period of System Warranty is defined as FSA plus fifty two (52) weeks from the date of the FSA approval signature by the Purchaser PM.*

4.3. Delivery Gates

[SOW 146] *The Contractor shall observe the Delivery Gates throughout the project.*

The objective of the gates are to formally collate all deliverables and ensure they are completed and accepted by the Purchaser PM.

Every Delivery Gate will have acceptance criteria.

[SOW 147] *The Contractor shall ensure that all acceptance criteria for a Delivery Gate have been completed or validated before the Contractor can formally state their readiness for the gate review to the Purchaser PM. Validation implies that the Contractor has fully collaborated with the Purchaser on all deliverables, and no outstanding actions exist.*

[SOW 148] *The Contractor shall expedite the request for a Gate review when the product is deemed complete and ready for assessment by the Purchaser, which may be earlier than stated in the SSS of milestone tables in Section 4.2.*

The Purchaser will reject a Delivery Gate as incomplete if the Acceptance criteria are not fully met.

[SOW 149] *The Contractor shall ensure that all relevant documentation is approved (PDF digitally signed by the Purchaser PM as appropriate) with the correct naming convention, classification and version control, and that the documentation is achieved in the project portal.*

There are two types of Delivery Gates in scope of the NPKI-M project.

- Design Gates
- Implementation Gates

4.3.1. Design Gates

There are two Design Gates in scope of the NPKI-M project.

4.3.1.1. Preliminary Design Review

[SOW 150] The Preliminary Design Review (PDR) shall include the following:

- *Draft System Design Specification (SDS)*
- *Draft Site Implementation Plan (SIP)*
- *Draft Site Installation Specification (SIS)*
- *Draft Requirements Traceability Matrix (RTM)*
- *Draft CI breakdown (ABL)*
- *Initial tailoring of S3000L specification*
- *Draft Training Needs Analysis (TNA)*
- *Draft Security Accreditation Documentation:*
  - *SRA*
  - *SRSS*
- *Draft Master Test Plan (MTP)*
- *Draft Test Cases*
- *QAP*
- *CMP*
- *IPSP*

[SOW 151] The PDR is a Design Gate which seeks to evaluate the completeness of the Contractor's deliverables in anticipation of the Critical Design Review. However, all deliverables shall be of a sufficient quality and completeness to progress.

4.3.1.2. Critical Design Review

[SOW 152] The Critical Design Review (CDR) shall include the following:

- *System Design Specification (SDS)*
- *Requirements Traceability Matrix (RTM)*
- *Site Implementation Plan (SIP)*
- *Site Installation Specification (SIS)*
  - *Service Request Tracking System (SRTS)*
- *Detailed CI breakdown*

- *Final Allocated Baseline - ABL*
- *Initial Product Baseline - PBL*

- *Training templates and formats*
- *Training Needs Analysis (TNA)*
- *Tailored S3000L specification*
- *Draft Security Accreditation Documentation:*
  - *SRA*
  - *SRSS*
- *Master Test Plan (MTP)*
- *Test Cases*

[SOW 153] The Contractor shall ensure that all CDR deliverables are of an acceptable quality and completeness prior to requesting the CDR.

The Purchaser PM will declare that the CDR has been approved, when all deliverables are accepted.

[SOW 154] The Contractor shall not progress to the next phase of the project until the CDR Design Gate has been successfully passed.

[SOW 155] If any deliverables are not approved, then the CDR Design Gate will not have been achieved and the Contactor may not progress to the next phase of the project. Any delays to the project will be the responsibility of the Contractor.

4.3.2. Implementation gates

4.3.2.1. Provisional System Acceptance

[SOW 156] The Provisional Site Acceptance (PSA) Implementation Gate shall include the following (which shall be complete and accepted):

- *Installation, Integration and testing of the specific milestone in scope*
- *SOW and SRS requirements*
- *Requirements Traceability Matrix*
- *Site Implementation Specification*
- *Site Acceptance Test Report*
- *Security and Vulnerability Testing Report*
- *Product Breakdown List*
- *Site Inventory (including the Software Distribution List and Physical Configuration Audit)*
- *All equipment and cables are labelled*
- *Interactive Electronic Technical Publications (S1000D)*
- *Training and training material*
- *As-Built Documentation and Interface Control Documentation delivered and accepted*

- *Configuration Management Database*
- *Logistic Support Analysis and Reliability, Maintainability and Availability (RMA) data (S3000L)*
- *Relevant Security Accreditation documentation*

[SOW 157] *The Contractor shall ensure that all elements of the PSA are completed, however only minor deficiencies (equipment, software, licences, and documentation) may be permitted to be carried over until the Final System Acceptance Implementation Gate – subject to the discretion of the Purchaser PM.*

4.3.2.2. Final System Acceptance

[SOW 158] *The Contractor shall commence Final System Acceptance (FSA) upon the acceptance of all four PSA milestones (1-4).*

[SOW 159] *The time elapsed between the last PSA and the FSA shall not be more than four (4) weeks.*

[SOW 160] *The FSA Implementation Gate shall include the following (which shall be complete and accepted):*

- *All known deficiencies resolved (equipment, software, licences, and documentation)*
- *All Engineering Change Proposals*
- *Final Product Baseline*
- *All project documentation*
- *All Security Accreditation documentation*
- *Outstanding Change Control activities*

[SOW 161] *The Contractor shall conduct a two-day FSA Project Service Performance Review (SPR), to be conducted on the Production and Reference systems. The location of the review is subject to the discretion of the Purchaser PM.*

[SOW 162] *The Contactor shall demonstrate via scenarios that the delivered services are functioning as per the Requirements, and that training is completed such that transition to operational capability can be accepted.*

[SOW 163] *The Contractor shall deliver a SPR report one week after the completion of the SPR for Purchaser review.*

[SOW 164] *The Contractor shall conduct a one (1) day FSA meeting, where acceptance evidence of all activities, deliverables and services of the project will be provided for final review to the Purchaser for final Acceptance. The meeting shall also include a collaborative element to capture Lessons Identified and Learned.*

4.4. Purchaser Furnished Equipment

The Purchaser will provide all equipment as Purchaser Furnished Equipment (PFE), and will be responsible for all logistics to NHQ and SHAPE and Tempest testing of those components.

[SOW 165] *The Contractor shall install the Purchaser-provided hardware identified as PFE according to the requirements and in compliance with the approved low level design document as verified by the Purchaser.*

[SOW 166] *The Contractor shall inform the Purchaser immediately upon identification of any PFE items found not to be in accordance with the SOW and SRS in ANNEX A.*

[SOW 167] *The Contractor shall inform the Purchaser immediately upon identification of any defective equipment.*

[SOW 168] *The Contactor shall be responsible, when necessary, for the local site logistics of equipment beyond the warehouse storage facuilities in NHQ and SHAPE .*

[SOW 169] *The Contractor shall perform pre-configuration of all equipment in the Purchaser provided facilities at the CIS Service Support Centre (CSSC) in Brunssum, NL. This configuration is prior to deployment of the equipment to the respective sites (SHAPE and NHQ) – the logistics is the responsibility of the Purchaser. Should the facility not be available, then under the discretion of the Purchaser PM, alternative locations may be proposed within the NCI Agency footprint.*

[SOW 170] *The timing of the pre-configuration is subject to agreement between the Purchaser and Contractor PMs. Equipment for NHQ may require Tempest testing at the CSSC facilities before shipping to site. These activities shall be scheduled so as to not impact the delivery milestones.*

4.5. Design Activities

This section outlines the System Engineering, Integration, Tests, and Implementation of NPKI-M Hosting Platform Services.

[SOW 171] *The Contractor shall be responsible for the implementation of the Purchaser provided overall design throughout the Contract period of performance. When needed, the Purchaser will provide reasonable effort for the integration with other services necessary to allow the NPKI-M applications to function.*

[SOW 172] *The Purchaser will provide the NPKI-M Hosting Platform Services High-Level Design (HLD). The Contractor shall update the Purchaser provided version of the HLD and produce the detailed System Design Documentation.*

[SOW 173] *The active components used for the NPKI-M Hosting Platform Services shall be physically separated and be used exclusively for the NPKI-M Hosting Platform Services.*

[SOW 174] *The Contractor shall integrate all necessary components to establish the NPKI-M Hosting Platform Services Baseline, and plan and execute a series of tests to confirm that this baseline meets its requirements, in accordance with Section 6.*

[SOW 175] *The Contractor shall be responsible for integration of the various products that constitute the NPKI-M Hosting Platform Services.*

The Purchaser will provide reasonable effort to assist with the integration of the NPKI-M Hosting Platform Services with other NATO systems.

[SOW 176] *The Contractor shall deliver and activate the NPKI-M Hosting Platform Services.*

4.5.1. System Design

The NPKI-M hosting solution is leveraging the core networks infrastructure design principles and access switching with VLAN and VRF separation principles, with dedicated Firewalls. Monitoring and Management connections will be available from the dedicated switch to the NPKI authorized clients.

[SOW 177] *The Contractor shall conduct the necessary activities and develop its own complete design of the NPKI-M Hosting Platform Services at the Preliminary and Critical levels, including all interfaces to other systems to meet the SOW requirements.*

[SOW 178] *The Contractor shall keep the system design documentation package (including security accreditation documentation) up to date throughout project execution, in particular in order to obtain the security accreditation.*

[SOW 179] *The Contractor shall establish, deliver and maintain up to date the NPKI-M Hosting Platform Services Design Documentation Package, comprising of:*

- *The System Design Specification (SDS)*
- *The Security Accreditation Documentation Package*
- *The Requirements Traceability Matrix (RTM)*
- *The Master Test Plan (MTP)*

[SOW 180] *The Contractor shall prove the design through the regime of testing set forth in the Contract and the Contractor shall be responsible in the event that the system proves deficient in meeting the Contractual requirements.*

[SOW 181] *The Contractor shall ensure that in order to maintain clear consistency throughout all documents in the System Design Documentation Package, any update of any of the documents comprised in the System Design Documentation Package shall result in re-delivery of a new version of the complete System Design Documentation Package.*

4.5.1.1. System Design Specification

[SOW 182] *The Contractor's System Design Specification (SDS) shall describe the NPKI-M Hosting Platform Services to a level of detail that is sufficient for the Purchaser to be able to ensure that the requirements in the SRS in ANNEX A are implemented.*

[SOW 183] *Updated Low Level Design (LLD) details from the Contractor shall be included within the SDS.*

[SOW 184] *The Contractor shall include, at a minimum, the following information in the SDS document which shall serve as LLD.*

- *System Architecture:*
  - *Diagrams: logical architecture, physical architecture, external interfaces, network etc.*
  - *Topology for the system*
  - *Routing, Transport, and connectivity to NPKI-M components*
- *Administration model design (Administrative groups and permissions, administrative roles)*
- *System Functionalities*

- *Functional breakdown of the NPKI-M Hosting Platform Services*
- *System internal interfaces: physical interfaces between components, data flows*
- *Performance*
- *Equipment*
  - *Physical breakdown of the operational NPKI-M Hosting Platform Services, into hardware/software CIs (including the number of licenses for each software CI)*
  - *Identification of all COTS included in the system.*
  - *CSA reports addressing all system CIs*
  - *All configuration information (parameters, settings, security, etc.) for all components*
- *LLD documentation showing the implementation of elements from the HLD*
- *Step by step deployment and failover recovery documents for the deployed PostgreSQL Database services*
- *Description of how the system complies with SRS requirements in ANNEX A*
- *Description of how the Segregation Requirements are met*

4.5.1.2. Security Accreditation Documentation Package

[SOW 185] *The Contractor shall ensure that the Security Accreditation Documentation Package comprises all documentation identified in Section NN.*

4.5.1.3. Requirements Traceability Matrix (RTM)

[SOW 186] *The Contractor shall develop and maintain a Requirements Traceability Matrix (RTM) that establishes a complete cross-reference between the requirements stated in the SRS, the System Security Requirements Statement (SSRS), and the detailed contents of the SDS in terms of SDS statements and lowest-level Configuration Items (CIs) with the Master Test Plan.*

4.5.1.4. Master Test Plan

[SOW 187] *The Contractor shall ensure that the Master Test Plan (MTP) is created and maintained as per Section 6.*

4.5.2. Design Review

[SOW 188] *The Contractor shall organize a System Requirements Review (SRR) for NPKI-M Hosting Platform System Design Documentation Package to be delivered in MS0 in Table 7. The SRR shall be held immediately after the Project Kick-Off meeting, and should be expected to last for a minimum of two (2) days. The location of the SRR should be in the same facility, primarily to be at SHAPE – but subject to the discretion of the Purchaser PM.*

[SOW 189] *The Contractor shall include all of the following areas in the Design Review:*

- *NPKI-M Hosting Platform Services overall system architecture and interactions*
- *System functionality, modularity and interfaces, breakdown into lowest-level CIs*
- *Off-the-shelf products to be used in the system: the Contractor shall identify the intended product and version, and note if any additional elements (such as macros or plug-ins) are required*
- *Interfaces with other relevant systems*
- *System security design: Presentation of the Risk Assessment Methodology that the Contractor intends to use for the Project, Results of the Risk Analysis, Definition and implementation of the Security measures to counter the risks identified in the Security Risk Assessment (SRA) and in compliance with the SRS in ANNEX A.*
- *Sequence and scope of system tests of the ABL and any requirements for Purchaser support and participation*
- *Any change request or off-specification*
- *Any changes to the PBS*
- *Any changes to the IMS*
- *Cost considerations, as applicable*
- *Risk assessment*
- *MTP traceable to system system/component requirements and acceptance criteria.*

[SOW 190] *The Contractor shall provide an SRR Report within five (5) days after the SRR.*

4.6. Implementation

[SOW 191] *The Contractor shall ensure the implementations are planned and achievable as per the milestones in Section 4.2.*

The Purchaser reserves the right to suspend the Contractor's installation and/or or activation work for up to ten (10) working days to avoid interfering with or disrupting other activities with no cost impact.

[SOW 192] *The Contractor shall produce a Site Implementation Plan (SIP) for each installation – which details all aspects required to perform the implementation in advance of deployment.*

[SOW 193] *The Contractor shall include in the SIP, a list of all equipment, hardware, software and licences that are required.*

[SOW 194] *The Contractor shall include in the SIP the details of the Contractor's personnel that will be involved in site installation and activation work.*

[SOW 195] *The Contractor shall provide a Request For Visit (RFV) from the individuals' respective National Security Agency to the Purchaser's Security Office for these personnel – no less than two (2) weeks before the actual site deployment.*

[SOW 196] *The Contractor shall ensure that the Draft SIS is completed and that the SRTS elements are completed and approved prior to initiating implementation.*

[SOW 197] *The Contractor shall provide a simple Deployment Plan to support the Change Control and Approved Service Interruption (ASI) requests necessary before authorisation is granted to rack any equipment.*

[SOW 198] *The Contractor shall monitor the progress of any required Site facilities preparations, and the progress of any required provision of input by the Purchaser and the Site, to ensure timeliness and quality of the preparatory work required from the Purchaser.*

[SOW 199] *The Contractor shall ensure that anything that may delay installation is brought to the attention of the Purchaser PM immediately.*

4.6.1. Implementation activities

[SOW 200] *The Contractor shall perform site installation and activation, which comprises of the following activities:*

- *Perform site installation of any NPKI-M Hosting Platform Services elements (Hardware, Software), including establishment of network connectivity between all required components, in accordance with PRREF.1 (HLD).*
- *Perform amendments as appropriate to deployed NPKI-M Hosting Platform Services elements (Hardware, Software), including establishment of network connectivity between all required components, in accordance with PRREF.1 (HLD).*
- *Perform site activation.*
- *Execute all activities related to Security Accreditation.*
- *Execute Physical Configuration Audit (PCA).*
- *Deliver all documentation associated to site installation and activation.*

[SOW 201] *The Contractor shall coordinate the start date of the planned installation no later than three weeks before that start date.*

[SOW 202] *Although the Purchaser will provide the facilities in which the NPKI-M Hosting Platform Services will be installed and the external systems to which it will be interfaced, the Contractor shall be responsible for timely requests to complete logistics and installation of all relevant supplies.*

[SOW 203] *The Contractor shall unpack all NPKI-M Hosting Platform Services equipment at the installation location and dispose of packing materials as directed by the Purchaser's Site POC. Due to site constraints, the Contractor may be required to pre-configure all equipment at the Purchaser's logistics facility CSSC in Brunssum, Netherlands – subject to the discretion of the Purchaser PM.*

[SOW 204] *The Contractor shall connect all equipment to electrical power and communications interfaces provided by the Purchaser.*

[SOW 205] *The Contractor shall provide and install all the pre-made cabling and ancillary items which are not already included within the Purchaser's rack infrastructure.*

[SOW 206] *The Contractor shall turn on all equipment and configure hardware and software settings in compliance with the HLD and the SRS in Annex A..*

[SOW 207] *The Contractor shall install and configure all Purchaser-provided equipment, e.g. switches, firewalls and virtualized networking components for each security classification domain.*

[SOW 208] *The Contractor shall provide Red Hat Enterprise Linux (RHEL) Licences with smartmanager add-on based on the list of VMs specified in PRREF.1 (HLD).*

[SOW 209] *The Contractor shall install and configure all NPKI-M Hosting Platform Services equipment (hardware, software, hosting platform and workstations), in accordance with the PRREF.1 (HLD) and SRS in ANNEX A.*

[SOW 210] *The Contractor shall conduct the site activation tests as per the testing process detailed in section 6.*

4.7. Security Accreditation

[SOW 211] *The NPKI-M Hosting Platform Services are to deliver the underlying infrastructure for the NPKI-M CIS. The NPKI-M CIS needs to achieve security accreditation in order to be granted the authorisation for operational use at its final operational environment. Therefore, the Contractor shall follow the security accreditation process established by the Security Accreditation Authority (SAA) for the NPKI-M CIS with respect to the NPKI-M Hosting Platform Services.*

[SOW 212] *The NPKI-M Hosting Platform Services shall be provisioned in a way to support achieving of the security accreditation for the NPKI-M CIS to be granted before NPKI-M CIS will be authorized to go live.*

[SOW 213] *The NPKI-M Hosting Platform Services as the critical component of the NPKI-M CIS shall demonstrate compliance with the NATO relevant Security Policy, supporting directives and the NPKI-M system-specific documentation (e.g., System Security Requirement Statements (SSRS)).*

The overall Security Accreditation Authority (SAA) for the NPKI-M CIS is the NATO CIS Security Accreditation Board (NSAB). Coordination with the SAA will be conducted by the Purchaser.

The primary objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the NPKI-M CIS. This includes ensuring that the NPKI-M Hosting Platform Services, being part of the NPKI CIS, conforms to NATO Security Policies and Directives identified in the NPKI-specific security-related documentation (SRD) described in Section 2..

A verification that security measures (personnel security, physical security, security of information, CIS security controls), including security baselines identified in the respective System-specific Security Requirement Statements (SSRS) and SecOPs have been properly implemented in accordance with the requirements of the SAA is one of the primary bases for the security accreditation for the NPKI-M.

This verification is carried out by the SAA and typically supported by appropriate results of security testing conducted based upon agreed Security Test and Verification Plan (STVP) which is to cover all security requirements identified and approved in form of System-specific Security Requirement Statement (SSRS).

The SAA might require a “Type 3 Security Audit” (SA) to be conducted against the NPKI-M to include the NPKI-M Hosting Platform Services.

[SOW 214] *The Contractor shall support the Purchaser in performing a security vulnerability analysis (A "Type 3 Security Audit" as per the "Rules of Engagement for Security Audits of NATO CIS") of all Contractor-delivered components in each solution in each domain prior to acceptance. This is also covering development of the remediation plan and fixture of deficiencies/vulnerabilities relevant to the NPKI-M Hosting Platform Services discovered and reported in the Type 3 SA Report.*

[SOW 215] *The Contractor shall take action to follow, carry out the necessary work, and to implement the advice, instructions and changes required by the SAA and/or resulting from the security audit(s) in order to support achieving security accreditation for the NPKI CIS at no additional cost.*

[SOW 216] *The Contractor shall designate Security Subject Matter Experts (SMEs) as points of contact for Security Accreditation and security-related issues.*

4.7.1. Security Accreditation Documentation

[SOW 217] *The achievement of the security accreditation for the NPKI-M will require a contribution to development of the prescribed set of security-related documentation (SRD) from the Contractor. This documentation will be developed by using security accreditation documentation templates. The templates will be made available to the Contractor after the Contract Award (CAW).*

[SOW 218] *The Contractor shall contribute to the development of the SRD regarding the NPKI-M Hosting Platform Services in support of the security accreditation of the NPKI CIS.*

The documentation to be developed to support the NPKI CIS security accreditation process is listed in the table below; which also summarizes responsibilities related to the development of each document; Column "Baseline/Guidance" lists available templates, relevant NATO Security Directives and Guidance, and similar documentation.

[SOW 219] *The Contractor shall undertake the work identified in the column "Contractor Responsibility".*

Document	Baseline/ Guidance	Contractor Responsibility	Purchaser Responsibility
Generic documentation			
Security Accreditation Plan (SAP)	SAP template	1. Provide necessary information, which might result in the update to SAP. 2. Adhere to security accreditation activities as described in the SAP. 3. All activities related with the security accreditation process (as per SAP) shall be included in the SIP, IMP, and the IMS	1. Develop and update SAP. 2. Provide SAP to the Contractor (after Contract Award). 3. Coordination with the SAA.

Document	Baseline/ Guidance	Contractor Responsibility	Purchaser Responsibility
CIS Description	CIS Description template	1. Update the Initial version of the CIS Description. 2. The update shall cover all technical aspects within the scope of the SOW (i.e. NPKI-M Hosting Platform Services) and shall be coherent with information provided in the LLD.	1. Develop the initial version of the CIS Description. 2. Review of the updated version of the CIS Description. 3. Coordination with the SAA.
Security Risk Assessment (SRA)	AC/35-D/1015, AC/35-D/1017, SRA Report template, Tool for formal SRA: NATO PILAR	1. Support the Purchaser in conducting SRA (to include participation in the SRA workshops as required) regarding technical aspects included in the SOW. 2. Address additional technical security requirements from the SRA.	1. Conduct SRA (based on CIS Description). 2. Develop SRA Report. 3. Coordinate with the SAA.
System specific Security Requirement Statement (SSRS)	AC/35-D/1015, SSRS template	Provide necessary inputs to the SSRS related to system design within the scope of the SOW (NPKI-M Hosting Platform Services).	1. Develop SSRS. 2. Review relevant inputs provided by the Contractor. 3. Coordinate with the SAA.
Security Operating Procedures (SecOPs)	AC/35-D/1014, SecOPs	Provide necessary inputs to the SecOPs, especially to cover security requirements related with the system design within the scope of the SOW (NPKI-M Hosting Platform Services).	1. Develop SecOPs. 2. Review relevant inputs provided by the Contractor. 3. Coordinate with the SAA.

Document	Baseline/ Guidance	Contractor Responsibility	Purchaser Responsibility
Security Test & Verification Plan (STVP)	AC/35-D/2005, STVP template	1. Provide inputs to STVP, to include detailed Security Implementation and Verification Procedures (SIVP) covering all technical aspects within the scope of the SOW. 2. STVP/SIVP shall define a complete sequence of steps to be followed to prove that the security mechanisms designed into the NPKI-M CIS enforce the security requirements identified in the NPKI-M SSRS. 3. The STVP/SIVP shall cover all security mechanisms of the NPKI-M as defined in the SSRS which are related to the scope of the SOW.	1. Develop STVP. 2. Review relevant inputs provided by the Contractor. 3. Coordinate with the SAA.
Security Test Verification Report (STVR)	STVR template	1. Execute relevant tests out of STVP (related with security measures required for NPKI-M Hosting Platform Services) during security testing. 2. Record test results relevant to the NPKI-M Hosting Platform Services in the STVR template.	1. Provide STVR template. 2. Supervise/witness testing to be conducted by the Contractor for the NPKI-M Hosting Platform Services. 3. Coordinate with the SAA.
Approval for Test (AfT) request	AfT Request Template	Support the Purchaser in developing AfT Request(s) by providing necessary technical details and/or testing specific information related with the NPKI-M Hosting Platform Services.	1. Develop AfT Request(s) as per SAP. 2. Coordinate with the SAA.

Table 8: Security Accreditation Documentation and Contractor Responsibility

[SOW 220] *In support of producing the SRD the Contractor shall closely engage directly with representatives of the Purchaser and the Security Accreditation Authority (as necessary) in order to discuss particular security-related requirements but also to clarify and/or enhance inputs to the documentation required in support of the Security Accreditation Process.*

[SOW 221] *The Contractor should expect a number of review rounds per document before it will be approved.*

[SOW 222] *The Contractor may be invited to provide briefings and/or technical expertise for meetings with the Purchaser and the SAA in support of the review of the security-related documentation.*

[SOW 223] *The SAA may provide advice and instructions to the Contractor (through the Purchaser) on any security implication or any proposed change based on the findings and results of the assessments or security tests. The Contractor shall consider the advice, instructions and guidance from the SAA. The Contractor shall take actions to follow, carry out the necessary work and to implement the advice, instructions and guidance given by the SAA in relation to the NPKI-M Hosting Platform Services architecture and configuration.*

[SOW 224] *The Contractor shall recognize the NATO Security Policies and supporting Directives in order to take into account all related requirements in the resulting NPKI-M Hosting Platform Services design and installation thereof.*

[SOW 225] *The Purchaser might receive comments from the SAA towards any security-related document. The Contractor shall support the Purchaser in updating this document or update the document (relevant to the CIS Description) as many times as necessary in order to obtain SAA approval.*

All inputs to the Security Accreditation documents will be subject to Purchaser and SAA approval.

4.7.1.1. CIS Description

An initial CIS Description for the NPKI-M Hosting Platform Services will be developed by the Purchaser. This document will be made available to the Contractor after Contract Award (CAW). The initial CIS Description will describe the Hosting Platform Services (HPS) information derived from the initial HLD.

[SOW 226] *The Contractor shall update the CIS Description document based on the CIS Description template provided by the Purchaser, and maintain the CIS description during the project, including all relevant information taken from the System Design Documentation Package as required to understand the content of the CIS Description document. The CIS Description shall be a standalone document.*

[SOW 227] *The CIS Description document shall at a minimum include the following information:*

- *Detailed technical description showing the main components and the high level as well as detailed information flows,*
- *Description of all internal and external connections of the system,*
- *List of hardware and software components used,*
- *Overview of the security mechanism which are going to be implemented in the NPKI-M Hosting Platform Services.*

[SOW 228] *The Contractor developed CIS Description shall be submitted to the Purchaser for review before it will be provided to the SAA for approval.*

[SOW 229] *The Contractor shall take into account any comments from the reviewers and SAA and shall update the CIS Description document as many times as necessary in order*

to obtain SAA approval for the portion related with the NPKI-M Hosting Platform Services.

4.7.1.2. Security Risk Assessments

[SOW 230] The Contractor shall support the development of the Security Risk Assessments (SRA), including risks related to modern CIS technologies and NPKI-M Hosting Platform Services specific risks.

The Purchaser will organise SRA workshop(s) at Purchaser or Contractor facilities as necessary.

[SOW 231] The Contractor's Subject Matter Experts (SMEs) shall attend these workshops to support proper assessment. It has been anticipated that at least two (2) and up to five (5) days for each SRA workshop will be required.

[SOW 232] Based on the results of the Security Risk Assessment SRA, the Contractor shall support to identify areas of NPKI-M Hosting Platform Services requiring safeguards and countermeasures to comply with NATO Security Policy and supporting Directives. The decision on specific security mechanisms shall be based on evidence(s) and results produced by the Security Risk Assessment.

[SOW 233] Where the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components, the Contractor shall consider these changes to be within the technical and financial scope of this Contract; no Engineering Change Proposal (ECP) shall be generated.

[SOW 234] Where the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, an ECP shall be raised by the Contractor.

4.7.1.3. System-Specific Security Requirements Statement

The System-specific Security Requirement Statement (SSRS) is a complete statement of the security principles to be observed and of the detailed security requirements to be met.

[SOW 235] The SSRS will be developed, as directed by the SAA in form of the SAP, defining the security requirements for the NPKI-M CIS to include the NPKI-M Hosting Platform Services.

[SOW 236] The Contractor shall support the development of the SSRS to include the minimum levels of security deemed necessary.

[SOW 237] The Contractor shall provide inputs to the overall SSRS for the NPKI-M CIS related to the NPKI-M Hosting Platform Services.

[SOW 238] To provide inputs to the SSRS the Contractor shall adhere to the template provided by the Purchaser (after Contract Award).

[SOW 239] The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of relevant part of the SSRS document as many times as necessary in order to obtain SAA approval.

4.7.1.4. Security Test and Verification Plan (STVP)

A Security Test and Verification Plan (STVP) is a description of the security testing and verification of the CIS Security measures to be implemented for the NPKI-M.

[SOW 240] The overall STVP for the NPKI-M will be generated by the Purchaser with support provided by the Contractor.

[SOW 241] The Contractor shall provide inputs to the overall STVP for the NPKI-M CIS related to the NPKI-M Hosting Platform Services.

[SOW 242] To provide inputs to the STVP the Contractor shall adhere to the template provided by the Purchaser (after Contract Award).

The inputs to the STVP shall describe in details the tests which will demonstrate compliance with the security requirements for the NPKI-M identified in the respective SSRS and SecOPs against the NPKI-M Hosting Platform Services.

[SOW 243] The Contractor shall ensure that the inputs to STVP covering tests for the NPKI-M Hosting Platform Services defines a complete and detailed sequence of steps to be followed to prove that designed security mechanisms enforce the security requirements identified in the NPKI-M SSRS.

[SOW 244] For each security test to be developed by the Contractor the following details shall be identified:

- *The objective of the security test*
- *An outline description of the security test*
- *A description of the execution of the security test (too include technical instructions how to conduct the test)*

The pass criteria for the security test.

[SOW 245] The Contractor shall ensure that each and every security test is cross-referenced to the corresponding security requirements from the NPKI-M SSRS (identified by the unique identifier) related with the NPKI-M Hosting Platform Services.

[SOW 246] The Contractor shall ensure all security requirements identified in the SSRS for the NPKI-M Hosting Platform Services are planned for testing.

[SOW 247] The Contractor shall execute the test out STVP relevant to the NPKI-M Hosting Platform Services, under Purchaser's supervision.

[SOW 248] The Contractor shall also develop, provide and maintain the initial and any updated Security Implementation Verification Procedures (SIVP) for the NPKI-M Hosting Platform Services specific Security Tests.

[SOW 249] These procedures shall consist of a set of software scripts and inspection procedures that shall allow a CIS Security Officer to verify that all components of the NPKI-M Hosting Platform Services have been installed and configured property and comply with the SSRS and SecOPs.

4.7.1.5. Security Test and Verification Report (STVR)

A Security Test and Verification Report (STVR) is a description of the results for the every instance of security testing conducted based on STVP.

[SOW 250] The Contractor shall record test results relevant to the NPKI-M Hosting Platform Services in the STVR template provided by the Purchaser.

[SOW 251] *The Contractor shall ensure security test identifiers are preserved in the Report as defined in the STVP.*

4.7.1.6. Security Operating Procedures (SecOPs)

Security Operating Procedures (SecOPs) are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel.

[SOW 252] *The overall SecOPs for the NPKI-M will be generated by the Purchaser with support provided by the Contractor.*

[SOW 253] *The Contractor shall provide inputs to the SecOPs related with the NPKI-M Hosting Platform Services.*

[SOW 254] *To provide inputs to the SecOPs the Contractor shall adhere to the template provided by the Purchaser (after Contract Award).*

[SOW 255] *Contractor's inputs to SecOPs shall specifically cover all security requirements identified in the SRA and SSRS (relevant to the NPKI-M Hosting Platform Services) which are not fully fulfilled by technical countermeasures. For example, the following security procedures should be addressed (not exhaustive list):*

- *System configuration and maintenance*
- *System backup*
- *System recovery, etc.*

[SOW 256] *The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of relevant part of the SecOPs as many times as necessary in order to obtain SAA approval.*

4.7.1.7. Approval for Testing / Approval for Pilot

When there will be a requirement to test the NPKI-M Hosting Platform Services or its element(s) before this is used in its final operational environment, the SAA may grant an Approval for Testing (AfT) by identifying specific conditions for the AfT including, for example, the scope of tests, the classification of information involved in the testing, the test plan and the timeframe for the AfT.

[SOW 257] *The Contractor shall coordinate with the Purchaser for Approval for Testing (AfT) before initiating any testing activity in the final environment.*

[SOW 258] *The Contractor shall support the Purchaser in developing AfT requests by providing necessary technical details and/or testing specific information related with the NPKI-M Hosting Platform Services.*

[SOW 259] *The Contractor may need to request Approval for Pilot (AfP) before the Interim Security Accreditation (ISA) can be requested to the SAA. The AfP will have to be agreed by the Purchaser with the SAA, in order to define to what extent the solution may be operated during a period of time and until ISA is requested and granted.*

4.8. Physical Configuration Audit

[SOW 260] *The Contractor shall perform a Physical Configuration Audit (PCA) for every PSA milestone.*

[SOW 261] *The Contractor shall schedule and chair the PCA.*

[SOW 262] *The Contractor shall co-ordinate the PCA with the Purchaser's IPS Manager.*

[SOW 263] *The Contractor shall produce and deliver a PCA Report for each PSA milestone.*

5. INTEGRATED PRODUCT SUPPORT

5.1. Introduction

[SOW 264] *This Section details all Integrated Product Support (IPS) requirements covering the through-life supportability aspects that the Contractor shall implement for the NPKI-M Hosting Platform Services capability.*

[SOW 265] *The Contractor shall implement the requirements of this section by using the IPS templates and instructions made available by the Purchaser in accordance with ANNEX B.*

[SOW 266] *Although the Contractor's work defined in Section 4 will rely on PFEs provided by NCI Agency for installation, integration and testing in the listed sites/locations, the Contractor shall be fully responsible for the design of operation, maintenance and support tasks for all the implemented locations, in accordance with the requirements set in this Section 5, and shall develop and deliver the relevant artefacts and services as defined in the next paragraphs in accordance with the Contractor developed LLD.*

5.2. IPS Plan (IPSP)

[SOW 267] *The Contractor shall deliver an IPSP as part of the PMP describing all aspects of support and how the Contractor proposes to meet the IPS requirements, following the requirements set in the Agency Instruction (AI) 16.31.03 – Requirements for the Preparation of IPSP.*

[SOW 268] *The IPSP shall include details that demonstrate how the Contractor proposes to meet all IPS requirements of the contract including the warranty period as detailed in Section 5.14 below.*

The Purchaser will verify that the activities, deliveries, analyses and documentation delivered by the Contractor(s) are integrated, coherent and consistent with the contractual requirements and do not degrade the operational availability of the existing systems and services.

5.3. Maintenance and Support Concept

[SOW 269] *The maintenance and support definitions detailed in ANNEX C shall be applicable to this project.*

[SOW 270] *In order to allow the Purchaser to fully operate the provided capability (including initial solution configuration), to perform HL1/2 and SL1/2 maintenance, and to support the capability at SUPL3 (centralized) from each completed environment (MS 2 to 5) for the relevant site(s), the Contractor shall:*

a. *Perform supportability analysis and studies;*

b. *Design and deliver maintenance and support documentation and instructions;*

c. *Design and execute training sessions.*

[SOW 271] *The maintenance and operational support instructions shall specify the procedures, the tasks and the resources required at each maintenance and support level, including the interaction/coordination between maintenance and operational support activities.*

From each completed environment (MS2 to 5) for the relevant site(s), the HL1/2 and SL1/2 maintenance and operational support activities up to SUPL3 included (centralised) of the capability will be executed by Purchaser's personnel.

[SOW 272] *From each completed environment (MS2 to 5) for the relevant site(s), up to the end of the warranty period, the Contractor shall be responsible of:*

a. *Performing HL3/4 and SL3/4 maintenance tasks;*

b. *Performing SUPL4 operational support tasks;*

c. *Providing all resources (skills and tools and test equipment)[1] required to support a. and b. above;*

d. *Fixing software bugs and releasing required patches; and*

e. *Provisioning of remote and onsite technical assistance beyond the scope and capabilities of the Purchaser – i.e. HL1/2, SL1/2 and SUPL1/2/3.*

[SOW 273] *The Contractor shall document the detailed maintenance and support concept of the capability within the IPS Case Report.*

5.4. Logistic Support Analysis (LSA)

[SOW 274] *The Contractor shall develop and document a detailed LSA in accordance with the ASD S3000L Specification.*

[SOW 275] *The Contractor shall propose for Purchaser's approval the project-specific tailoring of the ASD/AIA S3000L specification.*

[SOW 276] *The Contractor shall perform the Operational and Maintenance Task Analysis (OMTA) of the product to include, for each maintenance and operational support task:*

a. *General information, such as preconditions for task performance, training requirements or criticality information;*

b. *Assignment of maintenance tasks to the identified events (e.g. failures, damages, interval or thresholds for preventive maintenance tasks)*

c. *Concise task description, including the sequence of subtasks;*

d. *Identification of required task resources (e.g. personnel, support tools, spares);*

e. *Time estimations;*

f. *Task frequencies;*

g. *Consideration of required pre- and post-work (e.g. gaining access, final operational test).*

[SOW 277] *The proposed ASD/AIA S3000L tailoring at [SOW 278] shall include the project-specific data dictionary, and the formats used for LSA data and documentation deliveries.*

---

[1] Any spare parts required for the accomplishment of the maintenance tasks will be provided by the Purchaser.

[SOW 278] *The ASD/AIA S3000L data set shall contain as at a minimum the following information, in accordance with the maintenance and support levels defined in ANNEX C and the high level maintenance and support concept described in MAINTENANCE AND SUPPORT CONCEPT:*

a. *Detailed hierarchical LSA Breakdown Structure (LBS) down to the Maintenance Relevant/Significant Item (MRI/MSI), as per definition of MIL-HDBK-470A, Appendix D;*

b. *Configuration Management data (identification of Configuration Items - CI, type of CI, relationships, dependencies) in accordance with STANAG 4427 Ed.3 (see Section 8);*

c. *Software and relevant licenses data, as required to provide the Software Distribution List (SWDL) in [SOW 286];*

d. *MRI/MSIs category (Line Replaceable Unit - LRU, Insurance Item - II, Attaching Part - AP, Technical and/or non-Technical consumable, Next Higher Assembly - NHA, not-MRI/MSI) as per definitions in ANNEX C.*

e. *For each non-volatile storage media devices of the product (e.g. hard disk drives, solid-state drives, M.2 drives, CompactFlash memory cards, micro SD cards, multimedia cards): detailed information for the identification of both the hosting device and the storage media device, that include*

   (1) For both: Part Number (PNR), NATO Commercial and Government Entity Code (NCAGE), Serial Number (SNR) and Reference Designator (REFDEF);

   (2) For the hosting device: NCIA stock number and NCIA Asset Tag (both assigned by the Purchaser);

   (3) For the storage: Capacity and Position.

f. *For each individual item identified in the LBS: full and detailed range of maintenance and operational support tasks, including troubleshooting, and relevant durations, periodicities, resources (skills/trades, tools, materials), safety data/procedures;*

g. *Maintenance Level (preventative, corrective, troubleshooting) associated to each individual item identified in the LBS;*

h. *MTBF (Mean Time Between Failure) from each element at MRI/MSI aggregated up to the system level, and relevant calculation method (predicted, allocated, field data, specification) and conditions (e.g. temperature, environment);*

i. *MTTR (Mean Time to Repair) from each element at MRI/MSI level aggregated up to the system level;*

j. *Preventative Maintenance periodicities and durations (Mean Time Between Preventative maintenance - MTBP - and Mean Time To Preventive - MTTP - as per guidelines given by MIL-HDBK-338B);*

k. *Skills/Trades and numbers (e.g. Electronic, Electro-Mechanic, Mechanic);*

l. *Population at each MRI/MSI level and QEI (Quantity per End Item);*

m. *SMR (Source, Maintenance, Recoverability) coding down to MSI level in accordance with AR 700-82/SECNAVINST 4410.23/AFMAN 21-106;*

n. *Safety instructions.*

[SOW 279] *The ASD/AIA S3000L data set deliverable shall be delivered at MS1 – three (3) working weeks in accordance with the Purchaser provided template.*

[SOW 280] *LSA deliveries shall be fully consistent with the applicable Product Baseline (PBL) and include:*

a. *Summary reports, which address applicable standards and handbooks, implemented methodology and mathematical models, calculations, and outcomes of the analysis;*

b. *Detailed list of all tasks as per the results of the OMTA; and*

c. *Raw data as either MS Excel tables and/or S3000L XML dumps.*

[SOW 281] *The Contractor shall document the results of the LSA in the IPS Case report.*

[SOW 282] *The LSA data shall be used as input to the development of the technical publications and the development of training courseware to the maximum extent possible.*

5.5. Software Distribution List (SWDL)

[SOW 283] *The Contractor shall provide a detailed SWDL, which details comprehensively all Configuration Software Configuration Items (CSCI) and associated software, firmware and licenses (including PFE), as installed on the deployed capability.*

[SOW 284] *The SWDL shall contain as at a minimum the following information:*

a. *CSCI identification data (i.e. PNR, nomenclature, NCAGE, version);*

b. *CSCI hosting device identification data;*

c. *CSCI End Of Life (EOL, as applicable);*

d. *CSCI End Of Support (EOS, as applicable);*

e. *For each licensed CSCI, the following software license data as applicable:*

(1) *Licensing authority;*

(2) *Description;*

(3) *Type – e.g. perpetual, subscription-based;*

(4) *Key code;*

(5) *Date of deployment;*

(6) *Current date of expiration;*

(7) *Contractual date of expiration;*

(8) *License renewal date;*

(9) *Renewal periodicity (e.g. quarterly, Six-monthly, annual);*

(10) *Distribution media (e.g. hardware key, dongle, software key, simple key)*

(11) *Price per yearly maintenance.*

The Purchaser will make available all licenses required for the deployment of the capability.

[SOW 285] *The Contractor shall verify that all software licenses are registered with the NCI Agency service desk as end-user, and promptly report to the Purchaser any issues that may occur.*

[SOW 286] *The SWDL shall be delivered, as part of each site's inventory list, at Site Acceptance Test (SiAT) start – 1W and final version at each completed environment (MS 2 to 5) – one (1) working week.*

5.6. Reliability, Availability, Maintainability and Testability (RAM&T)

[SOW 287] *The Contractor shall perform RAM&T analysis to calculate and predict the Inherent Availability (Ai) and Operational Availability (Ao) of the capability.*

[SOW 288] *The Contractor shall develop RBDs (Reliability Block Diagrams) in accordance with IEC 61078:2016, and use mathematical models for Ai and Ao to demonstrate that the provided product and support solution allow the requirements in compliance with the PRREF.1 (HLD).*

[SOW 289] *The Contractor shall provide evidence of the RAM&T analysis in the IPS Case Report, such as applicable standards and handbooks, implemented methodology and mathematical models, RBDs, calculations, and outcomes of the analysis.*

[SOW 290] *RAM&T analysis data shall be used to feed the LSA dataset (ref. [SOW 281]).*

5.7. Interactive Electronic Technical Publications (IETP)

[SOW 291] *The Contractor shall develop and deliver, in accordance with the ASD/AIA/ATA S1000D Issue 4.0.1 specification as per the tailoring provided by the Purchaser with the following agency instructions:*

a. *AI 16.31.07 – GD (Guidance Document) for ASD-AIA-ATA S1000D TechPubs*

b. *AI 16.31.12 – WSG (Writing Style Guide) for ASD-AIA-ATA S1000D TechPubs*

c. *AI 16.31.13 – ISG (Illustration Style Guide) for ASD-AIA-ATA S1000D TechPubs.*

[SOW 292] *The IETP delivery shall include:*

a. *Installations instructions;*

b. *Safety instructions;*

c. *Operating instructions, including initial solution configuration;*

d. *HL1/2 and SL1/2 maintenance instructions, including:*

1) *System description, controls and indicators,*

2) *Corrective, preventative and troubleshooting procedures down to MRI/MSI level,*

3) *Illustrated Parts Catalogue,*

e. *Support Levels 1, 2 and 3 instructions, including:*

1) *Hardware and software monitoring,*

2) *Network integration description and management,*

3) *SW installation, policies management and fine tuning,*

4) *SW troubleshooting, debugging, patching and re-installation;*

5) *SW performance improvement procedures;*

6) *System Administrator instructions;*

f. *COTS/OEM Manuals (in their original format, PDF) encapsulated in the IETP Data Modules (DM) as required in the AI 16.31.07 (GD).*

[SOW 293] *IETP content, structure and layout, and usability on a ASD/AIA/ATA S1000D fully compliant browser[2] shall be verified both Table Top (TT) and On Object (OO) in accordance with AI 16.31.07.*

[SOW 294] *The Contractor QA shall approve TT and On Object OO first verified IETP before such IETP are delivered to the Purchaser.*

[SOW 295] *First verified IETP shall be ready, approved by Contractor QA, when the relevant training sessions will occur.*

The Purchaser will validate first verified IETP and provide either confirmation of 'Validation pass' or request for re-delivery (in case of 'Validation fail') of first verified IETP as per Purchaser's comments.

[SOW 296] *If 'Validation fail', follow on deliveries of first verified IETP shall be provided by the Contractor as required to achieve 'Validation pass' as early as possible.*

The Purchaser will distribute first verified IETP to all stakeholders for second verification and collect comments to the IETPs in different stages (including the training sessions).

[SOW 297] *The Contractor shall support IETP OO second verification activities, by attending in person on-site Combined Verification Process (CVP) event.*

[SOW 298] *The Purchaser will submit formal IETP comments to the Contractor at the end of the on-site CVP event.*

[SOW 299] *The Contractor shall attend virtual consolidation meetings held between Contractor & Purchaser, and stakeholders aimed to address all pending comments, as required.*

[SOW 300] *IETP final version delivered by the Contractor shall include the implementation of all second verification comments as agreed at CVP event.*

[SOW 301] *The IETPs delivery shall be in the form of a "bundle" comprising:*

a. *All the required source files i.e. collection of all required DMs, illustrations,*

---

2 The ASD/AIA/ATA S1000D browser is not part of the provision and any available ASD/AIA/ATA S1000D browser can be used by the Contractor for the IETPs verification.

referenced publications (e.g. COTS) etc.;

b. *An interactive PDF of the Publication Module (PM) in the form of an editable & printable technical manual; and*

c. *A release notice in standard office or pdf format listing the content of the bundle and the exact version of each entity (DDN, PMC, referenced publications).*

[SOW 302] The Contractor shall provide updates of the IETP final version not later than each completed environment (MS 2 to 5) – one (1) working week.

[SOW 303] The Contractor shall provide updates of the IETP final versions at the end of each Operational Acceptance testing

[SOW 304] Further updates of the IETP final versions shall be provided by the Contractor in accordance with the warranty requirements.

5.8. Training

[SOW 305] *The Contractor shall deliver a full training programme including training needs analysis, planning, design, delivery and assessment of the training activities.*

[SOW 306] *The training programme shall cover all capability management (operation and maintenance) aspects in accordance with the Maintenance and Support Concept defined above.*

[SOW 307] *The Contractor shall deliver a project-specific Training Plan (TRNP) to describe in detail the training programme that the Contractor will implement including the proposed duration for each session, sequence of the sessions, daily planning and any other information deemed important for the correct planning and execution of the trainings.*

[SOW 308] *The Contractor shall develop and deliver the TRNP in accordance with the Purchaser provided AI 16.31.04 – Requirements for the preparation of TRNP.*

[SOW 309] *The Contractor shall deliver a draft Training Plan with the PMP and a final Training Plan at MS1 including the resolution of all the comments provided by the Purchaser on the draft version.*

[SOW 310] *The Contractor's proposed duration of the trainings shall be subject to acceptance by the Purchaser and be adequate to the contents, complexity and required knowledge to be transferred to the trainees in accordance with the requirements of this SOW, the maintenance and support levels defined in ANNEX C and the support concept described above, and the results of the TNA required (see below).*

[SOW 311] *The Contractor shall design and develop the training data and courseware on the basis of the maintenance and support above, specialities (maintenance, operational support, operation), levels and requirements defined in this SOW*

[SOW 312] *The Contractor shall propose for Purchaser'approval the formats and templates for the training data and course material at MS1.*

[SOW 313] *The Contractor shall conduct a Training Needs Analysis (TNA) in accordance with BiSC D-075-007, 2015.*

[SOW 314] *The TNA shall include:*

a. *Target audience analysis;*

b. *Performance gap analysis;*

c. *Difficulty, Importance and Frequency (DIF) analysis;*

d. *Training delivery options analysis.*

[SOW 315] *The Contractor's TNA shall be based on the tasks resulting from OMTA (see [SOW 279]) and on the possible gaps highlighted during the site surveys (so called Target Audience Analysis).*

[SOW 316] *The Contractor's TNA shall consider all assigned staff roles involved in the operation, administration, maintenance and support of the delivered capability.*

[SOW 317] *The Contractor shall deliver a TNA Report that captures the results of the TNA, not later than MS1 – three (3) working weeks and a final version not later than MS1.*

[SOW 318] *The TNA Report shall be delivered in accordance with the Purchaser provided AI 16.31.11 – Requirements for the Preparation of TNA Reports to include:*

a. *A description of the TNA approach and activities;*

b. *An account of the operation, support, corrective and preventive maintenance tasks considered in the TNA;*

c. *The results of the Target Audience Analysis, the Performance Gap Analysis the DIF Analysis and the training delivery options analysis;*

d. *The final list of Performance Objectives in accordance with Annex J of BiSCD 75-7, 2015;*

e. *The final list of Learning Objectives in accordance with Annex N of BiSCD 75-7, 2015;*

f. *Course Proposals in accordance with the Course Control Document II form annexed to Annex L of BiSCD 75-7, 2015.*

[SOW 319] *The Contractor provided training shall include training sessions covering the complete product overview, concepts at a high level, targeted to managers of technical teams operating, managing and supporting the delivered solution.*

[SOW 320] *When not available from the Contractors in-house capability, the Contractor shall procure, organise and provide standard commercial vendor training courses available on the market to fulfil the training requirements identified in the TNA as part of the Contractor provided training.*

[SOW 321] *The number of sessions required shall be defined in the TNA Report.*

[SOW 322] *The Contractor's provided training shall include operation training sessions to allow the attendees to fully operate the provided product.*

[SOW 323] *The Contractor's provided training shall include technology awareness training sessions for any new technologies to be implemented as part of the solution.*

[SOW 324] *The training at [SOW 322] shall take place before installation commences to allow the personnel to understand and follow the implementation.*

[SOW 325] *The Contractor's delivered training shall include maintenance and support training sessions to allow the attendees to perform maintenance at HL1/2 and SL12 and operational support at SUPL3 on the provided capability, in accordance with the maintenance and support levels defined in ANNEX C and the support concept described above.*

[SOW 326] *The Contractor's delivered training shall include administrator training sessions to allow the attendees to fully install, re-install, set-up, customize, troubleshoot, patch, update, upgrade, test and release and administer the provided product, including automation, scripting and adaptations that may be required in the life of the product, in line with the maintenance and support levels defined in ANNEX C and the support concept described above.*

[SOW 327] *The Contractor shall deliver each training session to a maximum of ten (10) trainees (per session) that will have at least a basic starting knowledge on products similar to the one in the scope of this project and at the same maintenance and operational support levels.*

[SOW 328] *The Contractor's delivered training shall be based on a combination of classroom and hands-on Instructor Led Training (ILT) sessions.*

[SOW 329] *Where possible training should be conducted off-site to avoid work based distractions for the attendees.*

[SOW 330] *The Contractor shall be responsible for the timely provision on the training site/location of the following training data and courseware for each trainee:*

a. *Trainee guidebook;*

b. *Training courseware, properly structured and organized, including video/audio, drawings and procedures, slides/presentations, COTS documentation etc.;*

c. *IETPs;*

d. *Final training test questionnaire;*

e. *Completion certificates (upon successful completion of the final test).*

[SOW 331] *The Contractor shall propose and, upon Purchaser concurrence, make available the system or reference system or reference environment where the training will be executed in order to maximize the effectiveness of the training.*

[SOW 332] *The Contractor shall be responsible for the instructor courseware and tools (instructor's guidebook, laptop, portable projector etc.).*

[SOW 333] *The Contractor shall be fully responsible for the quality, content, completeness and correctness of the training courseware and shall implement the modifications, corrections and improvements required by the Purchaser to achieve acceptance and deliver the training accordingly.*

[SOW 334] *The training and training courseware shall be delivered in simplified English language and the instructor shall be English mother tongue or proficient and certified in English language (STANAG 6001 level 4333 at least).*

[SOW 335] *Any training session/course shall be delivered by an instructor with a minimum of 2 (two) years' experience on the provided product, or similar to.*

[SOW 336] *The Contractor shall deliver and complete (achieving full Purchaser acceptance) all the training sessions before each PSA is granted.*

[SOW 337] *The HL1/2 and SL1/2, and the SUPL3 training sessions shall not be run in parallel.*

[SOW 338] *At training start, the Contractor shall make available the first verified version of the IETPs to be used as integral part of the training courseware and data during each session.*

5.9. Packaging, Handling,Storage, Transportation (PHST)

The Purchaser will be responsible for the PHST of all PFE to the destination locations.

The application of the requirements [SOW 338] to [SOW 345] **is only limited to the PHST of any additional equipment to the PFE**, provided by the Contractor to support the scope of supply of this SOW.

[SOW 339] *The Contractor shall PHST the provided equipment to/from the destination locations (e.g. building, warehouse), including Tempest Testing facility (if required), within the deadlines established by the SSS.*

[SOW 340] *All provided equipment, including items being returned for warranty repair, shall be shipped Delivered Duty Paid (DDP) to the destination locations in accordance with INCOTERMS 2020 published by the International Chamber of Commerce.*

[SOW 341] *The Contractor shall define the best method for the packaging of the provided equipment, fulfilling as a minimum the requirements of STANAG 4280 "NATO Levels of Packaging", NATO packaging level 4.*

[SOW 342] *If the provided equipment is shipped to the destination locations by means original OEM/Vendors commercial packaging, the Contractor shall be responsible for either:*

a. *Demonstrating to the Purchaser that such packaging fulfils the requirements of STANAG 4280 Level 4; or*

b. *Re-packing the equipment in accordance with STANAG 4280 Level 4.*

[SOW 343] *The Contractor shall be fully responsible for the decision and the selection of the proper packaging, marking and transportation means (air, sea, land), making proper considerations about and including vibrations, shocks, management of Electrostatic Discharge (ESD) sensitive devices, altitude/pressure, temperature and humidity limits not to be exceeded during the PHST activities.*

[SOW 344] *The Contractor shall be responsible for resolving any loss incurred in shipping the provided equipment.*

[SOW 345] *The Contractor shall unpack and install the provided equipment in the Purchaser facilities*

[SOW 346] *Any malfunction/failure/defect of the procured equipment, identified during the incoming inspection shall be full responsibility and fixed by the Contractor, in accordance with General Provisions clause "Inspection and Acceptance of Work"*

[SOW 347] *The Contractor shall also unpack and install the PFE NPKI equipment in the Purchaser facilities.*

Any malfunction/failure/defect of PFE NPKI equipment at destination (e.g., site/location or Tempest testing facility) assessed at incoming inspection, inventory or testing level will be full responsibility of the Purchaser.

[SOW 348] *In case of malfunction/failure/defect of PFE NPKI equipment at destination locations assessed at incoming inspection, the Contractor shall immediately notify the Purchaser of the defect for Purchaser's relevant action.*

[SOW 349] *PHST costs of PFE NPKI equipment will be under the sole responsibility and cost of the Purchaser, except for Contractor's induced failures that shall fall under costs and responsibilities of the Contractor.*

[SOW 350] *The Contractor shall coordinate with the Purchaser and with the local authorities the access to the sites and the proper safety and security procedures to be put in place for the PHST activities, for installation, integration and testing.*

5.10. 302 Forms

The 302 is a customs declaration to enable applicable authorities to permit the import or export of supplies between NATO/EU and NATO/Non-EU countries free of duties, taxes and excise charges.

Customs 302 documents have to be originals duly signed and stamped by the NCI Agency. They have to be originals and can therefore not be faxed but have to be mailed or sent by mail/express courier.

Although the Contractor is not expected to purchase and deliver any material to the destinations sites, should this become necessary the following requirements are applicable.

[SOW 351] The Contractor shall be responsible for the timely request of Customs Forms 302.

The Purchaser will provide the template, with relevant instructions, to be used for the submission of the Forms 302.

Following receipt of the request, the Purchaser will normally require a maximum of 3 (three) days for the issuance and shipment (e.g. via DHL) of the Forms 302, unless missing or incomplete documents (e.g. Packing List) are required by the Purchaser to be amended by the Contractor.

[SOW 352] In case that an express courier has to be used to ensure that the form is available in time before shipment, the Contractor shall create an account with a Contractor's designated freight forwarder (e.g. DHL, FEDEX) that the Purchaser can use for this purpose.

[SOW 353] Forwarding agents shall be informed of the availability of Form 302 and how this form is utilised to avoid the payment of customs duties.

[SOW 354] The Contractor shall add the Form 302 to the shipping documentation to be provided to the carrier.

[SOW 355] The Contractor shall have two copies of the Form 302 signed by the Purchaser representative at the final destination and return signed form to the Purchaser IPS Manager.

The 302 is provided by the Purchaser to facilitate the import or export free of duties, taxes and excise charges, but not always guaranteed since it can be declined by national customs authorities.

[SOW 356] If a country refuses to accept the Form 302 and requires the payment of customs duties, the Contractor immediately inform the Purchaser by the fastest means available and providing a written statement from the Custom Officer establishing that the subject Country refuses to accept the Custom Form 302.

[SOW 357] In case such an event occurs, the Contractor shall immediately inform the Purchaser by the fastest means available and before paying, obtain from the Customs officer a written statement establishing that his Country refuses to accept the Form 302.

[SOW 358] Only after having received Purchaser's approval, the Contractor shall pay these customs duties and shall claim reimbursement from either the Contractor's government or (only if denied by the government) the Purchaser, in accordance with the relevant procedure within the contract General Provisions.

5.11. Notice of Shipment

Although the Contractor is not expected to purchase and deliver any material to the destinations sites, should this become necessary the following requirements are applicable.

[SOW 359] At least ten days before each shipment of supplies, the Contractor shall provide the Purchaser with a Notice of Shipment comprising the following details:

a. *Shipment Date;*
b. *Purchaser Contract Number;*
c. *CLIN (Contract Line Item Number) as per SSS;*
d. *Consignor's and Consignee's name and address*
e. *Number of boxes, pallets, crates, containers or transit cases;*

f. *Gross weigh*

g. *Overal cubic meters;*

h. *Final/Partial Shipment;*

i. *Mode of Shipment (e.g. road, sea, land);*

j. *Number of 302 Forms used;*

k. *Packing List (see below).*

[SOW 360] *When 302 custom declarations are required, the Contractor shall combine the delivery of the Notice of Shipment together with the delivery of the Forms 302, so that the Purchaser can promptly prepare and send the required documentation and allow the Contractor to ship the equipment in the expected time window.*

[SOW 361] *The Purchaser will review for approval each request of shipment after receipt of the relevant Notice of Shipment.*

[SOW 362] *The Contractor shall not execute any shipment without the approval of the relevant Notice of Shipment by the Purchaser.*

[SOW 363] *Purchaser's approval of request of shipment will depend on granting of access and availability of storage space.*

[SOW 364] If no storage space can be allocated and assigned by Purchaser, then Contractor shall organise on-site or off-site storage at no additional cost to the Purchaser.

5.12. Packing Lists

Although the Contractor is not expected to purchase and deliver any material to the destinations sites, should this become necessary the following requirements are applicable.

[SOW 365] *The Contractor shall establish the packing lists in such a way as to permit easy identification of the procured equipment to be delivered to destinations.*

[SOW 366] *These packing lists shall accompany the shipment.*

[SOW 367] *Each individual box, pallet, container or transit case from a consignment shall have one packing list in weather-proof envelope affixed to the outside of each container/box which indicates exactly what is contained inside.*

[SOW 368] *One copy of the same packing list shall also be put inside each box, pallet, crate, container or transit case.*

[SOW 369] *The Contractor shall await for the Confirmation from the Purchaser of the availability of the destination location before shipment of the procured equipment takes place.*

[SOW 370] *The Packing list shall include the following general data:*

a. *Purchaser's contract number;*

b. *Purchaser's project number;*

c. *Names and addresses of the Contractor and the Purchaser;*

d. *Names and addresses of the Carrier, Consignor and Consignee (if different from Contractor or Purchaser);*

e. *Final destination address and POC;*

f. *Method of shipment;*

g. *List and number of boxes, pallets, crates, container or transit case.*

[SOW 371] *The Packing List shall include, for each box, pallet crate, container, or transit case shipped:*

a. *Box, pallet, crate, container or transit case identification number (assigned by the Contractor);*

b. *Weight (metric);*

c. *Dimensions (LxDxH, metric);*

d. *List of the items in each box, pallet, crate, container or transit case.*

[SOW 372] *The Packing List shall include, for each item shipped:*

a. *CLIN number as per the SSS;*

b. *Nomenclature;*

c. *PNR;*

d. *NCAGE (coherent with the PNR);*

e. *SRN (if applicable, for serailized items);*

f. *Quantity (for each line item);*

g. *Price (each and total).*

[SOW 373] *The Contractor shall be responsible to verify the correctness and completeness of the Packing Lists that will be referenced in the customs Forms 302, if required.*

5.13. Material Data Sheet (MDS)

Although the Contractor is not expected to purchase and deliver any material to the destinations sites, should this become necessary the following requirements are applicable.

[SOW 374] *The Contractor shall provide the product inventory of all the provided equipment delivered under this contract by filling out the Material Data Sheet (MDS) template provided by the Purchaser.*

[SOW 375] *The Contractor shall provide the MDS at least 10 (ten) days before each shipment of supplies.*

The Purchaser will not accept deliveries without the support of a complete and accurate MDS data.

5.14. Physical Labelling

[SOW 376] *The Purchaser will provide labels required for Purchaser's internal asset management process – compliant with STANAG 4329 "NATO Standard Bar Code Handbook" and AAP-44(A) "NATO Standard Bar Code Handbook" – which the Contractor shall attach to the equipment before its installation inside NATO locations.*

[SOW 377] *The Purchaser will also provide label for non-volatile storage media devices (see [SOW 281]) to be installed on NS environment, which the Contractor shall attach – directly on the device or, where the label is incompatible with the physical properties of the device, on its proximity – before their first installation.*

5.15. Warranty services

The warranty services of the provided NPKI-M Hosting Platform Services capability are based on:

- Hardware/software warranty services for the equipment used on the capability[3];
- Professional services to warrant all the activities required to accomplish the requirements of this SOW.

The Purchaser will be responsible for the hardware/software warranty services of all PFE.

The Contractor is required to provide both:

- Hardware/software warranty services **only for the additional equipment to the PFE**, provided by the Contractor to support the scope of supply of this SOW – if any;
- Professional services to warrant all the activities required to accomplish the requirements of this SOW.

[SOW 378] The Contractor shall provide resources and services required by this section during the warranty period.

[SOW 379] The warranty period shall start immediately after completion of each environment (milestones MS2 to 5)

[SOW 380] The warranty period shall complete for all entire capability – all environments aligned – after 12 months from MS6, except for extensions due to the Contractor' induced delays.

Milestones 2 to 5 are granted after all the installations, integration and testing activities are completed and accepted, the relevant training is completed and the required documentation is delivered and accepted.

MS6 will be granted once all sites have been completed (milestones 2 to 5), all major and minor deficiencies dragged from MS 2 to 5 have been solved and Operational Testing and Evaluation is completed.

[SOW 381] The time between the last MS5 and MS6 shall not be more than four (4) working weeks to provide the Contractor with enough time to rework hardware, software and/or documentation as required.

At each completed environment (MS 2 to 5) , the Purchaser will take title of the equipment and will perform the operation, maintenance and support activities defined in the MAINTENANCE AND SUPPORT CONCEPT.

All materials required to keep the provided environment operational will be under the responsibility of the Purchases until the end of warranty, excluding the equipment directly provided by the Contractor for the execution of the work defined in this SOW.

---

[3] It should be noted that the hardware/software warranty of the equipment might require to extend – in terms of both: duration and content – the legal warranty guaranteed by the OEM/Vendors, in order to comply with the requirements of this section.

[SOW 382] The Contractor shall provide hardware/software warranty services for all the equipment specifically provided by the Contractor to support the scope of supply of this SOW – if any.

[SOW 383] The Contractor shall provide professional services to warrant all the activities provided to accomplish the requirements of this SOW (e.g. installation, integration and testing activities; activities for the development of documentation or provision of data).

In the warranty period, the Purchaser will inform the Contractor of any defect on the services (labour, activities) delivered by the Contractor to accomplish the requirements of this SOW, through the issuance of warranty claims.

[SOW 384] Contractor shall have to solve any defect on the services (labour, activities) delivered by the Contractor to accomplish the requirements of this SOW i.a.w. the given timelines.

[SOW 385] The Contractor shall issue the entire set of warranty claims raised in each quarter from start of warranty in the form of warranty claims report.

The report will be analyzed by the Purchaser to assess the performance of the Contractor in the warranty phase and will be discussed by both parties during the Project Review Meetings for acceptance or rejection of the relevant warranty milestone.

[SOW 386] Before each completed environment (MS 2 to 5) and prior to the system warranty start, the activities, equipment, artefacts (including COTS hardware/software) and documentation shall remain under full responsibility of the Contractor and shall be delivered to NCI Agency, free of major deficiencies.

[SOW 387] The Contractor shall manage and correct all major deficiencies as formal class I changes in accordance with the requirements defined in Section 8, starting from the Purchaser's approval of the first Contractor's issued PBL.

[SOW 388] The Contractor shall manage and correct all minor deficiencies as formal class II changes in accordance with the requirements defined in Section 8, starting from the Purchaser's approval of the first Contractor's issued PBL.

[SOW 389] The Contractor shall warrant that all procured equipment and software specifically provided by the Contractor for the purposes of this SOW and which have been installed, integrated and tested under the Contract are genuine and free of any malicious components, firmware and software to ensure overall security of the capability and its supply chain.

[SOW 390] The Contractor shall warrant that documentation and training provided in the scope of the project reflects the system delivered and the MAINTENANCE AND SUPPORT CONCEPT.

[SOW 391] If the documentation does not reflect the product, the Contractor shall provide the updated documentation within ten (10) working days upon Purchaser's request.

[SOW 392] In case of failures of PFE items due to the execution of this project or failures of Contractor delivered items, the Contractor shall repair/replace the faulty items, at its own expenses and under its responsibility, with the highest priority allocated and shall be responsible to return the item to the destination site.

[SOW 393] If the updated/upgraded systems/services are unserviceable for a period of time, during the implementation of this Project, due to Contractor induced failures/delays, the warranty period shall be extended accordingly for all the sites and for the amount

of time the system has been unserviceable without any cost to be incurred by the Purchaser.

[SOW 394] *If the Contractor becomes aware at any time before each completed environment (MS 2 to 5) and during warranty that a defect exists in any supplies or services or documentation, the Contractor shall promptly correct the defect.*

[SOW 395] *The Contractor shall provide software patches and software/hardware/firmware upgrades, if applicable, whenever a specific issue is reported by the Purchaser until the expiration of the warranty, at no additional cost for the Purchaser.*

[SOW 396] *The Contractor shall install new software/firmware (e.g. through upgrades or patches) only after testing in the Reference System (RS) and only after accreditation in the NCI Agency Approved Field Product List (A2SL).*

[SOW 397] *The Contractor shall support the Agency with activities, data and documentation required to obtain A2SL approval for all software and firmware delivered in the frame of the project and requiring uplifting (upgrades, patches) w.r.t. the initially approved baseline.*

[SOW 398] *All the software and firmware changes (in addition to the hardware ones) shall follow the mandatory CM standards, processes and procedures required in Section 8.*

[SOW 399] *The Contractor shall provide Technical Assistance to the Purchaser or his representatives until the end of the warranty.*

[SOW 400] *Technical assistance information details shall be provided at MS1.*

[SOW 401] *Technical Assistance shall be provided from assistance centers located strictly within NATO countries boundaries and by staff who are nationalized citizens of NATO member nations.*

[SOW 402] *The Technical Assistance shall provide support in English for requests that correspond to information demands limited to the perimeter of delivered products, evolution proposals, problem reports, or any information needed by the Purchaser or its representatives, which are not included in the supplied technical documentation.*

[SOW 403] *Under the warranty arrangements (from each completed environment (MS 2 to 5)), the Contractor shall provide 24/7 reactive maintenance/support to the Purchaser based on a combination of:*

a. *Full access (credentials) to the KEDB/patches/firmware-software updates/firmware-software upgrades portal of the Contractor relevant to the procured HW/SW/SW products by NCIA*

b. *Full access to live helpdesk (chat, video, phone call) for instructions, documentation, troubleshooting, help on support and maintenance, configuration issues, patching and fixing of any HW/SW problem/failure under purchaser responsibilities (see maintenance/support concept)*

c. *Technical Assistance as per [SOW 402] to [SOW 405].*

[SOW 404] *Under the warranty arrangements (from each completed environment (MS 2 to 5)), the Contractor shall provide continuous advice and pro-active Support/Maintenance to the Purchaser based on a combination of:*

a. *Full access (credentials) to the Knowledge Base (or similar DB) portal of the OEM's/Vendors relevant to the HW/SW products procured by the Purchaser through the Contractor relevant to the procured HW/SW/SW*

products by NCIA.

b. *Periodic (e.g. weekly) bulletins/information/notices/recommendations for the improvement of the settings/security of the procured HW/SW/FW by NCIA*

c. *Active monitoring and both periodic and urgent notification of security alerts with temporary workarounds (including fixes and instructions) and follow-on release of security patches or new SW/FW releases*

d. *Support for HW/SW/FW inventories management (CMDB and LBS/PBS management)*

e. *Support, through a Single Point of Contact (SPOC) for HW/SW/FW settings/improvements to increase Security and Performance of the delivered equipment.*

[SOW 405] *Defect magnetic, solid state and electronic media storage devices (e.g., CD-ROM's, DVD's, Universal Serial Bus (USB) sticks, solid state storage drives, hard drives) will remain NATO property, at no additional cost, and not be returned to the Contractor when being replaced.*

[SOW 406] *All activities and issues arising before and during the warranty period shall be reported in the PRM minutes and Action Items List (AIL) for tracking and closure purposes.*

6. TESTING

6.1. General Requirements for Testing

This section defines the generic requirements to be applied by the Supplier to the Test, Verification and Validation (TVV) process, which is required for verification and validation of the requirements set forth under this Contract by the Purchaser.

NPKI-M Hosting Platform Services requires a set of TVV activities to verify its compliance with the Contractual requirements.

All Contract-related deliverables supplied by the Contractor will be verified and validated to ensure they meet the requirements of this Contract. Both fitness-for-use and fitness-for-purpose will be assessed using a quality-based approach.

The verification and validation approach will not only involve delivered equipment, but also interfaces and interoperability with existing NATO and/or national equipment, here considered as Purchaser Furnished Equipment (PFE).

The verification and validation of PFE is out of the scope of the Contract.

[SOW 407] For each requirement, the Contractor shall select a verification method, which shall be approved by the Purchaser.

6.2. TVV Activities

[SOW 408] All information items used during the verification and validation activities are to be handled according to their security classification, in accordance with AD 070-001 (Ref. 002)

[SOW 409] The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities. This includes the development of all TV&V documentation required under the Contract, the conduct of all independent verification and validation as well as the evaluation and documentation of the results

[SOW 410] All Contract-related deliverables supplied by the Contractor shall be verified and validated to meet the requirements of this Contract.

[SOW 411] All document-based deliverables shall be produced in a manner compliant with the templates provided by the Purchaser.

[SOW 412] The Contractor shall be responsible for the planning, execution and follow-up of all TVV events.

The Purchaser will assist in preparations by reviewing and providing feedback on all Contractor produced Configuration Items.

The Purchaser will also provide testing and engineering Subject Matter Expertise (SME) during all TVV events to witness and assist with these events.

[SOW 413] The Contractor shall support the Purchaser during TVV events as describe in this Product Baseline (PBL).

[SOW 414] The Contractor shall demonstrate to the Purchaser that there is a testing process in place for the development stages of this project.

[SOW 415] The Contractor shall identify and communicate to the Purchaser which best practices and international standards will be applied by them during all stages of the project.

[SOW 416] The Contractor shall strictly follow the TVV process, document templates and guidance provided by the Purchaser unless officially agreed otherwise by the Purchaser.

[SOW 417] *The Contractor shall ensure that rigorous testing, including regression testing when required, is performed at every stage of the project lifecycle to identify and correct defects as early as possible and minimise the impact on cost and schedule.*

[SOW 418] *The Contractor shall provide the Purchaser with all TVV material developed and used under this contract.*

[SOW 419] *The Contractor shall provide an overall project Test Director, who will work closely with the Purchaser's assigned Test Manager.*

[SOW 420] *Progress and result measurement shall be approved by the Purchaser and focused on items identified in MTP.*

[SOW 421] *The Contractor shall define and make use of Key Performance Indicators (KPIs) as identified in MTP, to measure process execution and identify opportunities for quality improvement, provide solutions and update the plans the achievement of defined objectives like coverage of risks, requirements, supported configurations, supported operational scenarios, etc.*

[SOW 422] *For each event supporting a test phase, the Contractor shall follow TVV process defined in MTP to perform the following activities:*

a. *Planning and management of the test event*
b. *Design and development of all tests cases and associated documentation required under this Contract*
c. *Test Readiness Review (TRR)*
d. *Conduct all testing*
e. *Event Review Meeting (ERM) to report and agree on the results*
f. *Closure of the of test events (including the final version of all test artefacts created during the test event)*
g. *Possible event re-run or amalgamated fix cycle to correct non-compliances and defects.*

Test Phases	Scope	Purchaser Involvement
Engineering Phase	Internal tests executed during development phase of the system to ensure the system/software conforms to their design specifications.	**Review**: Test Reports

Test Phases	Scope	Purchaser Involvement
Qualification Phase	Tests executed to verify the design and manufacturing process, ensure the system meets necessary design requirements, and provide a baseline for subsequent acceptance tests. *Possible tests:* *Electro-Magnetic Compatibility (EMC) Testing* *General Environmental Testing* *Water/Dust Ingress Testing* *Operational Robustness Testing* *Mechanical Environmental Testing* *Environmental Control Testing* *Biological & Chemical Testing* *Transportation Testing* *Physical Functional System Testing* *Product Safety Testing*	**Review**: Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects. **Participate**: Test Readiness Review (TRR), Test Execution, Event Review Meeting (ERM) **Provide**: Test Event Assurance Reports
IVVQ Assessment Phase	To determine whether or not a system satisfies user needs, functionality, requirements, and user workflow processes etc. before it gets into operation. To ensure verification of quality criteria, for the following tests shall be performed during the IVVQ Assessment: - **System Integration Test (SIT)** – Requirements based testing, focused on verifying integration of the different components together and with any external interface as defined by the SOW - **Security Tests** – Tests focused on ensuring the security criteria are met. - **System Acceptance Test (SAT)** – Tests focused on ensuring compliance with the requirements outlined in the SOW. These events may be merged into fewer events, subject to Purchaser approval.	**Review**: Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **Participate**: TRR, Test Execution, Event Review Meeting (ERM)

Test Phases	Scope	Purchaser Involvement
Site Acceptance Phase (SiAT)	To ensure that the specific site/node is installed properly per site/node installation plan and the service meets the requirements stated in the SRS. Site Acceptance Testing is also to ensure compatibility and integration of the product with the site environment. Migration related tests are also covered under this tests. This includes integration with PFE. This event may also be merged into the IVVQ Assessment event, subject to Purchaser approval.	**Review**: Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **Participate**: TRR, Test Execution, Event Review Meeting (ERM)
Operational Test and Evaluation	To ensure that all the Operational Sites are successfully integrated and tested on the network level. Demonstrate that all components of the System/Application have been integrated (including other systems) to meet all the requirements of the SRS as well as all security requirements defined in the Security Accreditation Documentation Package. Ensure end to end delivered system works as expected and can interoperate with other Purchaser equipment. This event will involve the end users. This event may also be merged into the IVVQ Assessment event, subject to Purchaser approval.	**Review**: Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **Participate**: TRR, Test Execution, Event Review Meeting (ERM)

Table 9: Test Categories for Independent Testing

[SOW 423] The Contractor shall only proceed to the next formal TVV activity, after the successful completion of the previous TVV activity and after the agreement and approval by the Purchaser.

6.3. Deliverables

[SOW 424] The Contractor shall provide a System Test Documentation Package, following documentation templates provided by the Purchaser, that is comprised of the following documents.

Work Product Name	Sent to Review/Approve
The Master Test Plan (MTP)	*with the System Design Documentation Package*

Work Product Name	Sent to Review/Approve
Event Test Plans (ETP) for individual test events	*1 month before test event*
The Security Test & Verification Plans (STVP)	*as required per NSAB*
Any submitted test Waivers together with supporting material	*4 weeks before test event*
The Test Cases/Scripts/Steps	*4 weeks before test event. First draft 4 weeks after CAW.*
Status Reports	*Periodically (to be set in MTP)*
The Test (Completion) Reports	*1 week after test event*
The Requirements Traceability Matrix (RTM) updated with test-related information	*First with MTP and update per test event*
Verification Cross Reference Matrix (VCRM)	*First with MTP and update per test event*

Table 10: System Test Documentation Package

[SOW 425] *The following timeline indicates by when the deliverables need to be provided to the Purchaser (and approved by the Purchaser) for each Test Event (dates follow the timelines of the previous table):*

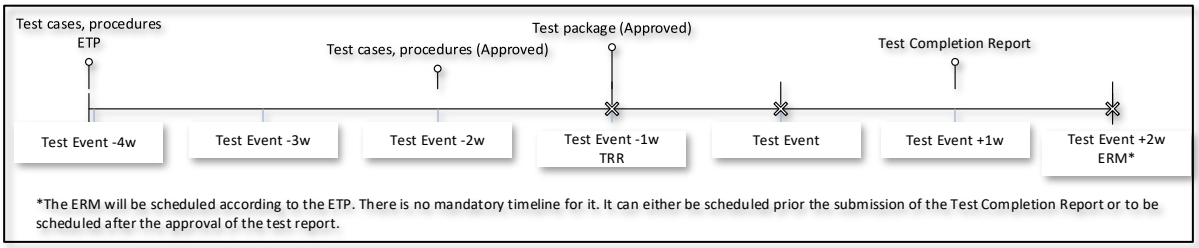

Figure 1 -Test Event timeline

[SOW 426] *All deliverables shall undergo as many review cycles are required, and shall be approved once all deficiencies have been corrected.*

6.3.1. Master Test Plan (MTP)

[SOW 427] *The Contractor shall produce a Master Test Plan (MTP) to address the plans for each TVV activities listed in this document.*

[SOW 428] *The Contractor shall describe how the Quality Based Testing is addressed and implemented in the MTP. The following figure is based on ISO 25010 and should be used as product quality criteria model.*

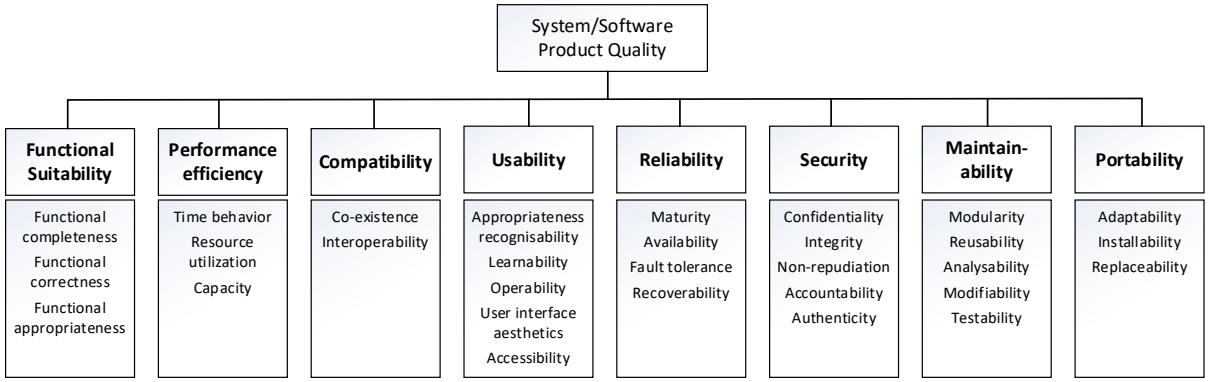

Figure 2 - Product Quality Criteria

[SOW 429] *The Contractor shall describe all formal test, verification and validation activities in the MTP with a testing methodology and strategy that fit the development methodology chosen by the project. The methodology shall also be fit-for-use and appropriate for the size and complexity of the Contractor's proposed solution.*

[SOW 430] *The Contractor proposed testing methodology shall describe the method of achieving all the test phases.*

[SOW 431] *The Contractor shall describe in the MTP how the following objectives will be met:*

- *a. Compliance with the requirements of the Contract*
- *b. Verification that the design produces the capability required*
- *c. Compatibility among internal system components*
- *d. Compliance with the SRS requirements*
- *e. Compliance with external system interfaces and/or systems*
- *f. Confidence that system defects are detected early and tracked through to correction, including re-test and regression approach*
- *g. Compliance with Purchaser policy and guidance (i.e security regulations, etc)*
- *h. Operational readiness and suitability*
- *i. Product Quality Criteria*
- *j. Identify which platform(s) to be used for the test events and the responsibilities for operation and maintenance of the environment*

[SOW 432] *The Contractor shall describe in the MTP:*

- *a. the Contractor's test organization and its relationship with the Contractor's Project Management Office and Quality Assurance (QA) functions*
- *b. "Entry", "Suspension", "Resumption" and "Exit" criteria for each of the formal test events. The Contractor shall seek approval of all criteria related to an event not later than the TRR of the event.*
- *c. Schedule for the provision of the test related deliverables and detail the conduct of testing*
- *d. The Contractor shall provide in the MTP the schedule, location and scope for all the events to be run, specifying to which phase they belong to. When*

the Contractor identifies that multiple events are required for a phase, this shall also be specified in the MTP.

e. *defect/non-conformances reporting and management process during the performed tests*

f. *Contractor's approach to Test Reviews including Test Readiness Reviews and Test Results Reviews for each test event*

6.3.2. Test Cases and Test Procedures

[SOW 433] *Any updates required from the execution of test cases during each phase shall be incorporated into the relevant test cases by the Contractor for use during independent verification, validation and acceptance. If only certain sections are affected, then it shall be sufficient to up-date and re-issue those section plus cover sheet with amendment instructions. Should major changes in contents or page re-numbering be needed, then the complete section shall be re-issued by the Contractor. All changes shall be made with the agreement and approval of the Purchaser*

[SOW 434] *The Contractor shall submit the draft test cases for the TVV event to the Purchaser for approval no later than four (4) weeks prior to the execution of the tests, unless differently stated in a work package.*

The Purchaser will provide comments or approval within four (4) weeks of receipt.

[SOW 435] *The Contractor shall make available to the Purchaser the final version of the test cases and Event Test Plan available one (1) week prior to the TRR for a specific TVV event.*

[SOW 436] *The Contractor shall develop test and use cases to verify and validate all requirements in the SoW, requirements specifications and final design. The test cases shall follow the template provided by the Purchaser*

6.3.3. Event Test Plan

[SOW 437] *The Contractor shall create an Event Test Plan (ETP) per each event detailing all the information required for that event. The ETP shall follow the template provided by the Purchaser.*

[SOW 438] *The Contractor shall describe in the event test plan what training (if any) will be provided prior to formal TV&V events.*

[SOW 439] *The ETP shall describe when an agreement shall be reached between the Contractor and the Purchaser on the defect categorization and defect priority of failures encountered, as well as a way forward (if either at the end of each day of a TVV event or at the Event Review Meeting). If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Management functions.*

[SOW 440] *The Contractor shall describe in the event test plan what training (if required) will be provided to test event participants prior to formal TVV events.*

6.3.4. Requirements Traceability Matrix (RTM)

[SOW 441] *The Contractor shall produce and maintain the Requirements Traceability Matrix (RTM) to include all functional and non-functional requirements from ANNEX A, to track the TVV status of all requirements throught the contract execution (especially*

during the TVV activities). The RTM shall reflect the results of all previous test sessions, and show how the tests and any test Waivers relevant to the test session demonstrate the associated requirements.

[SOW 442] *The RTM shall also trace the requirements to the design. It shall also define how the requirements will be validated or verified at each of the TVV activities:*

a. *The verification method: Inspection, Analysis, Test or Demonstration*
b. *Correspondent TVV phase(s) for each requirement*
c. *Coverage Status*

[SOW 443] *The Contractor shall extend the RTM to ensure that the Purchaser can verify compliance throughout the project.*

[SOW 444] *The Contractor shall ensure that the testable and non-testable requirements are linked to the Requirements Traceability Matrix*

[SOW 445] *In the RTM, the Contractor shall maintain full traceability between the functional, the developmental and the product baselines, so that the Purchaser can verify their compliance throughout the Contract.*

[SOW 446] *The RTM shall guarantee the two-way link between requirements (SRS) and technical specifications.*

[SOW 447] *The RTM shall be kept up to date by the Contractor during the project lifecycle in order to reflect any changes during the implementation of the project, in a timely manner (i.e., within one (1) week of change occurring).*

[SOW 448] *The Contractor shall provide the Purchaser with updates (via the tools) to the RTM daily during the execution of an event, and following the conclusion of each event defined in the MTP. A workflow for updating the RTM shall be proposed by the Contractor and approved by the Purchaser*

[SOW 449] *The Contractor shall verify each requirement using a verification method as defined in Annex A. Selected verification method for each requirement is subject to Purchaser approval.*

[SOW 450] *If the verification method per requirement is not provided beforehand, the verification method shall be either test or demonstration. Any deviation to this requirement is subject to Purchaser approval.*

[SOW 451] *The Contractor shall trace all test cases in the Requirements Traceability Matrix.*

[SOW 452] *The Contractor shall update the RTM to provide traceability from tests completed to contracted requirements and provide the updated Matrix to the Purchaser in soft copy format.*

6.3.5. Test Report/ Test Completion Report

[SOW 453] *The Test Report or Test Completion Report provides a summary of the testing performed during the Test Event.*

[SOW 454] *The Contractor shall provide, in the Test Completion Report, a log/record of the event, including but not limited to individual test results, defects found (with a way forward for the ones remaining open), requirement coverage (planned and executed), test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.*

6.3.6. Tools

[SOW 455] *The Contractor shall generate and deliver automated test procedures/cases compatible with Purchaser test management and automation tools.*

[SOW 456] *The Contractor shall make use of automated testing and supporting testing tools (test management, requirement coverage, defect management, etc.) to the maximum applicable extent, for all system development, implementation, internal and formal tests. The process and proposed supportive tools shall be described in the Master Test Plan (MTP). In areas where the Purchaser already uses specific tools, the Contractor shall make use of the tools in use by the Purchaser.*

[SOW 457] *Tools supporting requirements coverage, defect management and test management shall be selected and hosted by the Purchaser and used by the Contractor. For any internal work, the Contractor may use their own internal tools, but the tools used for the Contractor's internal work shall be able to natively interface with the tools selected and hosted by the Purchaser in order to keep all TV&V related data for the project in the Purchaser tools.*

6.4. TVV Events and results

[SOW 458] *The Contractor shall conduct testing during the Project lifecycle compliant with the following requirements:*

[SOW 459] *The Contractor is responsible for conducting all testing during the Project lifecycle. The Contractor shall provide evidence to the Purchaser of the results of these testing activities. The Contractor shall respond to any Purchaser clarification requests regarding test results or performance within two working days*

[SOW 460] *The Contractor shall conduct all testing activities for any architectural changes.*

[SOW 461] *The Contractor shall support post go-live activities during the Operational Acceptance phase, to evaluate the project capability performance and establish benchmarks for future enhancements, including any changes made to fulfil the requirements.*

[SOW 462] *The Contractor shall provide status reports to the Purchaser regarding verification and validation activities during the planning/design and development phases, via the use of a dashboard report within the test management tool set and through meetings. The Contractor shall provide report(s) to the Purchaser following the completion of any TVV event.*

The Purchaser will approve the report and its findings within two business days

[SOW 463] *Progress and results measurement shall be approved by the Purchaser and focused on KPIs.*

[SOW 464] *Test results shall be recorded in the test management tool set. All results of all formal acceptance testing performed during a given day shall be recorded in the test management tool. The Contractor shall provide these test results for any given day by the starting of the next business day (0800 AM), but as a minimum not later than 24 hours following the execution of any test*

6.4.1. Test Readiness Review (TRR)

[SOW 465] *The Contractor shall conduct a Test Readiness Review (TRR) at least one week prior to the events defined in the MTP. The TRR shall ensure that all entry criteria for events have been met. Documentation that requires review by the Purchaser prior to a TRR shall be provided no less than 2 weeks prior to TRR.*

[SOW 466] *The Purchaser has the right to cancel the TRR and/or formal test event if the evidence demonstrates that execution of the test event will not be effective.*

[SOW 467] *The Contractor shall demonstrate that all the internal tests and dry runs are successful with test reports and results delivered to the Purchaser at least 2 weeks prior to start of any Contractual test activities.*

[SOW 468] *Formal acceptance testing, including installation testing, shall be performed always on an environment with the up to date security settings, latest approved patches and antivirus applied and on a solution that has followed the security guidelines and policies.*

6.4.2. TVV Event

[SOW 469] *An event starts with the Test Readiness Review (TRR) and finishes off with the Event Review Meeting (ERM).*

[SOW 470] *The start and/or ending of any test session shall be subject to the Purchaser approval. In the event that critical issues are encountered which impact the process of the testing or if the other functions depends on the failed test cases, the Purchaser has the right to stop the testing for Contractor's investigation. The tests can only re-start if Purchaser agrees to continue testing from the point of failure or re-start testing from the beginning.*

[SOW 471] *During formal TVV phases, a daily progress debrief shall be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.*

[SOW 472] *For each TVV event, the Contractor shall provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.*

[SOW 473] *At the end of the project, the Contractor shall provide the final version of all artefacts (regardless of format) created during the execution of all TV&V activities*

6.4.3. Event Review Meeting

[SOW 474] *The Contractor shall convene a EventReview Meeting (ERM) as defined in the ETP. The ERM shall ensure that the event results, defect categorization and a way forward to fixing the defects (if required) is agreed between the Contractor and the Purchaser. If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Management functions.*

[SOW 475] *The Contractor shall use the Purchasers' categorization nomenclature for all defects and non-compliances.*

[SOW 476] *At the end of the project, the Contractor shall provide the final version of all artefacts (regardless of format) created during the execution of all test, verification and validation activities.*

6.4.4. Test Waivers

[SOW 477] *The Contractor may request a Test Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. The Purchaser, after review of test waivers and analysis of their impact, reserves the right to require test and certification of the modified equipment at no cost to the Purchaser. The Purchaser has the right to reject any test Waiver.*

[SOW 478] *In respect to a requested Test waiver, the Contractor shall certify that the test environment to be implemented is identical to that which was originally used for testing, or inform the Purchaser of design/construction changes which affect form, fit or function.*

[SOW 479] *The Contractor shall record and log all waiver requests along with their resolution submitted for the Purchaser's approval.*

a. *If the Purchaser grants the waiver, the Contractor shall execute the Testing in accordance with the waiver.*

b. *With respect to a requested waiver, the Contractor shall certify that the test environment to be implemented is identical to that which was originally used for testing, or advice the Purchaser of design/construction changes which affect form, fit or function.*

c. *The Contractor shall record and log all waiver requests along with their resolution submitted for the Purchaser's approval.*

6.4.5. Failed Events

[SOW 480] *In the event of failed TV&V event and the need to return to a site for re-testing; travel and per diem expenses of NATO personnel shall be borne by the Contractor.*

6.5. Test Defect Categorization

[SOW 481] *The Contractor shall use the Purchasers' categorization nomenclature for all defects and non-compliances*

[SOW 482] *Should a failure be identified during a TV&V event/activity, a defect shall be recorded in the Agency's' test management and defect management systems. Once the event has concluded, the defect shall be reviewed during the event review meeting to agree on the severity, priority and category. The event test report shall then report the disposition of all defects recorded during the event and the defect management system shall be updated accordingly. Classification shall follow the definitions below:.*

Category	Definition
Severity	The severity of a defect is the degree of impact that the failure has on the development or operation of a component or system or user function. The severity shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached the Purchaser's PM will set the severity.
Priority	The priority of a defect defines the order in which defects shall be resolved. The priority of the defect shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached the Purchase's PM will set the priority.
Category	The type of observation identified during the execution of a test case.

Table 11: Definitions for Defect Categorization

6.5.1. Severity

[SOW 483] *According to their severity, failures shall be classified as one of the following.*

Critical	• The failure of testing of a requirement • The failure results in the termination of the complete system or one or more component of the system. • The failure causes extensive corruption of data.

	• The failed function is unusable and there is no acceptable alternative method to achieve the required results •
Major	A significant failure that causes severely impaired functions but does not prevent operational processing. Applies to conditions under which the complete system or one or more component of the system are partially inoperative, but are still usable by the users. A work around may be available, but it may require manual intervention. Examples: * Absence of expected modules/ object or Unit * failure of business operational process that affects a large group of users * complete failure of a module
Moderate	• The failure does not result in the termination and all functions are available but causes the system to produce incorrect, incomplete or inconsistent results. When resources are available and budgeted, should be resolved.
Minor	The failure does not result in termination and does not damage the functioning of the system. The desired results can be easily obtained by working around the failure
Cosmetic	The failure is related to the look and feel of the application, typos in a document or user interfaces (amongst others), and not part of the immediate usability or contractual requirements. The failure does not adversely affect the overall system operation.

Table 12 Classification of defects based on severity

6.5.2. Priority

[SOW 484] According to their priority, defects shall be classified as one of the following:

Priority Class	Description
Urgent	The defect shall be resolved as soon as possible.
Medium	The defect shall be resolved in the normal course of development activities. It can wait until a new build or version is created.
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.

Table 13: Priority Classes for Defect Classification

6.5.3. Category

[SOW 485] According to their category, defects shall be classified as one of the following:

Category	Description
Defect	An imperfection or deficiency in a work product where it does not meet its requirements or specifications. This category of defect could drive to the creation a Class II (Product Correction) Engineering Change Proposal (ECP).
Enhancement	This type of defect is used to record an Improvement to the product baseline. This category of defect would typically drive to the creation of a Class I (Product enhancement) ECP.
Document	This category is used to record defects encountered in the system documentation (test cases, test procedures, RTM, test plan, manuals, design, procedures…).
Clarification	This category is used to record deficiencies encountered during the test execution, which shall be clarified.
Waiver	This category is used to record when a waiver is required to address a specific observation or defects.

Table 14: Defects Categories

7. QUALITY ASSURANCE

7.1. Definitions

[SOW 486] *Unless otherwise specified in the SoW, QAREF.1 and underpinning AQAPs in Table 2 Quality Assurance Reference Documents NNREF.10 in Table 6 Non-NATO Reference DocumentsTable 6, PRINCE2 and ITIL definitions shall apply.*

Quality Assurance (QA) is a process and set of procedures intended to ensure that a product or service, during its definition, design, development, test and deployment phases will meet specified requirements.

Quality Control (QC) is a process and set of procedures intended to ensure that a manufactured product or performed service adheres to a defined set of quality criteria and meets the requirements of the customer.

Under the Contract, the terms “QA process” will also include Quality Control process.

A “Project document” is a document developed and maintained to help in the management of the project. Typically the plans (amongst which, the Quality Assurance Plan (QAP)) are project documents.

[SOW 487] *The term "NATO Quality Assurance Representative" (NQAR) shall apply to any of the Purchaser appointed Quality Assurance Representative.*

[SOW 488] *The term "Contractor Quality Assurance Representative" (CQAR) shall apply to any of the Contractor appointed Quality Assurance Representative.*

7.2. Introduction

[SOW 489] *The Contractor shall establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the Contract’s lifetime.*

[SOW 490] *The QA programme shall apply both the contractual requirements and the NATO requirements for quality identified by QAREF 2, QAREF.5, QAREF.6 and QAREF.8 and QAREF.9 in Table 2 to provide confidence in the Contractor’s ability to deliver products that conform to the Contractual requirements.*

[SOW 491] *If any inconsistency exists between the SoW requirements and the references, the SoW requirements shall prevail.*

[SOW 492] *The Contractor‘s QA effort shall apply to all services and products (both management and specialist) to be provided under the Contract. This includes all hardware, software, firmware and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract (including deliverable and non-deliverable items like test and support hardware and software), without limitation.*

[SOW 493] *The Contractor‘s QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.*

7.3. Roles and Responsibilities

During the entire Contract implementation, the NQAR(s) assures the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirements. The Purchaser, through its NQAR(s), is the authority concerning all Quality related matters.

[SOW 494] *The Contractor shall be responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the life-cycle of the Contract.*

[SOW 495] *The CQAR shall be accountable for the provision of the QA Plan and the compliance to the defined QA process.*

[SOW 496] *The CQAR(s) shall define the major quality checkpoints that will be implemented while executing the project and the quality process to be used at each checkpoint.*

[SOW 497] *The CQAR(s) shall be responsible for assessing that the Contractual requirements have been complied with, prior proposing the Contractual services and products.*

[SOW 498] *The CQAR shall report to a distinct manager within the Contractor's organisation at a level equivalent to or higher than the Project Management function.*

[SOW 499] *The CQAR shall be the point of contact for interface with and resolution of quality matters raised by the NCI Agency or its delegated NQAR.*

[SOW 500] *The Contractor shall support any NCI Agency or its delegated NQAR activity focused on monitoring Contractor activities at Contractor's facilities or other sites related to the development, testing and implementation. In particular, the Contractor shall:*

a. *Make himself/herself available to answer questions and provide information related to the project*,
b. *Allow the Purchaser representatives to inspect and monitor testing activities, and management, technical and quality processes applicable to the project*.
c. *Transfer to the Purchaser representatives all information deemed necessary to perform the QA activities, on his/her own initiative or on request by the Purchaser representative*.

[SOW 501] *The Contractor shall ensure that CQAR(s) have the required qualifications, knowledge, skills, ability, practical experience and training for performing their tasks.*

[SOW 502] *The CQAR(s) shall have sufficient responsibility, resources, authority and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective actions.*

[SOW 503] *The CQAR(s) shall participate in the early planning and development stages to ensure that all quality related requirements are specified in plans, standards, specifications and documentation.*

[SOW 504] *After establishment of attributes, controls and procedures, the CQAR(s) shall ensure that all elements of the QA Process are properly executed, including inspections, tests, analysis, reviews and audits.*

[SOW 505] *The Contractor, through its CQAR(s), shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services which conform to contractual requirements only.*

[SOW 506] *The Contractor shall maintain and, when required, deliver objective evidence of this conformance.*

[SOW 507] *The Contractor shall give written notice to the NQAR(s) at least four weeks in advance that the services and/or products are being presented for review, testing, verification, validation and acceptance.*

[SOW 508] *The Contractor shall demonstrate to the Purchaser that there is a Test Process in place for the project, supported by Contractor Quality Assurance (QA).*

[SOW 509] *Testing shall only be permitted by using test procedures and plans approved by the Purchaser.*

7.4. Quality Management System (QMS)

[SOW 510] *The Contractor shall establish, document and maintain a Quality Management System in accordance with the requirements of NNREF.10 in Table 6 Non-NATO Reference DocumentsTable 6.*

[SOW 511] *The Contractor's and Sub-Contractor's QMS relevant to performance under the Contract shall be subject to continuous review and surveillance by the cognizant NQAR(s).*

[SOW 512] *The Contractor shall include in orders placed with its Sub-Contractor(s) and Supplier(s), the QMS requirements necessary to ensure the supplies and services covered by the Sub-Contract(s) and/or Purchase Orders conform to the requirements of the prime Contract.*

[SOW 513] *The Contractor shall specify in each order placed with its Sub-Contractor(s) and Supplier(s), the Purchaser's and its NQAR(s) rights of access to all premises where contractual work is performed, in order to carry out audits, inspections, tests and other functions as may be required by the NQAR(s).*

[SOW 514] *If sub-contracted quality resources are used, the Contractor's Quality Management process shall describe the controls and processes in place for monitoring the Sub-Contractor's work against agreed timelines and levels of quality.*

7.5. Quality Assurance Process

[SOW 515] *The Contractor's QA process shall ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.*

[SOW 516] *The requirements for these processes shall be derived from the Contract, the QMS, the applicable AQAPs and referenced best practices, in that sequence of priority.*

[SOW 517] *The Contractor shall prepare, perform and document System Requirements Review (SRR), Preliminary Design Review (PDR) and Critical Design Review (CDR) according to the contractual requirements and NNREF.1 in Table 6.*

[SOW 518] *The Contractor shall prepare the testing process according to the contractual requirements and NNREF.4 in Table 6*

[SOW 519] *The Contractor shall prepare the test documentation in accordance to the contractual requirements and NNREF.4 in Table 6.*

[SOW 520] *The Contractor shall perform verification and validation of the Contractual deliverables before proposing them for the Purchaser review and approval.*

[SOW 521] *The Contractor's QA process shall be described in the QA Plan as outlined below. The process is subject to approval by the Purchaser.*

[SOW 522] *The Contractor shall demonstrate, with the Quality Assurance process, that the processes set up for design, develop, test, produce and maintain the product will assure the product will meet all the requirements.*

[SOW 523] *The Contractor shall assure that all the test and procedure used to demonstrate the requirements will be monitored and controlled under the QA process.*

[SOW 524] *On request, the Contractor shall provide the Purchaser with a copy of any Sub-Contracts or orders for products related to the Contract.*

[SOW 525] *The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser NQAR(s).*

[SOW 526] *The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.*

7.6. Quality Assurance Plan (QAP)

[SOW 527] *The Contractor shall provide a Quality Assurance Plan (QAP) for review to the Purchaser in accordance with the requirements identified in the* QA*REF*.5 in Table 2 *and the SoW requirements.*

[SOW 528] *The initial version of the QAP shall be delivered not later than 4 weeks after the signing of the contract.*

[SOW 529] *The Contractor's QAP shall be compatible and consistent with all other plans, specifications, documents and schedules, which are utilised under the Contract.*

[SOW 530] *All Contractor procedures referenced in the QA Plan shall either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.*

[SOW 531] *The QA Plan and all related QA procedures, and all their versions/revisions, shall be subject to NQAR(s) approval based on an agreed checklist.*

[SOW 532] *The acceptance of the QAP by the Purchaser only means that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.*

[SOW 533] *The Contractor shall review his QA programme periodically and audit it for adequacy, compliance and effectiveness.*

[SOW 534] *The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.*

[SOW 535] *The Contractor shall inform the NQAR(s) of deficiencies identified during internal audit unless otherwise agreed between the NQAR and/or the Purchaser and the Contractor.*

[SOW 536] *The Contractor shall include a risk management section within the QAP including the risks connected to the sub-Contractors of the Contractor.*

[SOW 537] *The Contractor shall make its quality records, and those of its Sub-Contractors, available for evaluation by the NQAR(s) throughout the duration of the Contract.*

[SOW 538] *The Contractor shall update the document, as required, from the delivery date of the initial QAP through Final Operating Capability (FOC), under Configuration control. The Contractor shall provide a copy of each new version of the QAP to the Purchaser for review and approval.*

7.7. Quality for Project Documents

[SOW 539] *A formal change management process shall be applied to all project documents, including documents naming conventions as defined by the Purchaser and coordinated with the Contractor.*

[SOW 540] *Project documents shall be configuration controlled. Each version of a project document is subject to Purchaser approval (unless otherwise specified).*

[SOW 541] *The Contractor shall ensure that any change related to the project documents are controlled, with the identity, approval status, version and date of issue are clearly identified.*

[SOW 542] *Project documents file names shall not contain any variable part, like version number, reviewer initials or maturity status. Version numbers and maturity status shall be marked in the document content and/or attributes.*

7.8. Risks

[SOW 543] *The Contractor and Sub-Contractor shall provide objective evidence, that risks are considered during planning, including but not limited to Risk Identification, Risk analysis, Risk Control and Risk Mitigation.*

[SOW 544] *The Contractor shall start planning with risk identification during Contract review and updated thereafter in a timely manner. The Purchaser reserve the right to reject QPs, Risk Plans and their revisions*

7.9. Deficiencies

[SOW 545] *The Contractor shall establish and implement a quality/product assurance Issue Tracking System (ITS) to ensure prompt tracking, documentation and correction of problems and deficiencies, during the lifecycle of the Contract.*

[SOW 546] *The ITS shall implement a lifecycle (status, responsibilities, relationship to affected Contract requirements, if applicable, and due dates) for each recorded deficiency.*

[SOW 547] *If the Contractor becomes aware at any time before acceptance by the Purchaser that a deficiency exists in any supplies, the Contractor shall log it in the ITS, coordinate with the Purchaser and promptly correct it.*

[SOW 548] *The Contractor shall demonstrate that all deficiencies are solved / closed before product acceptance.*

[SOW 549] *When the Contractor establishes that a Sub-Contractor or a Purchaser Furnished Equipment (PFE) product is unsuitable for its intended use, it shall immediately report to and coordinate with the Purchaser the remedial actions to be taken.*

[SOW 550] *The Contractor shall ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.*

7.10. Support Tools

[SOW 551] *The Contractor shall make all support tools available for demonstration to the NQAR, upon request.*

[SOW 552] *The Contractor shall also make available to the Purchaser for review upon request, associated records and documentation, including but not limited to, control, authorization for use, calibration, validation, qualification, as applicable, per respective Contract requirement.*

7.11. Certificates of Conformity

A Certificate of Conformity (CoC) is a document, signed by the Supplier / Vendor of a product, stating that the product conforms to contractual requirements and regulations. A Certificate of Conformity template is available in QAREF.4 in Table 2.

The CoC, provides evidence that the items produced or shipped comply with test procedures and quality specifications prescribed by the customer.

The Contractor is accountable for the conformance to requirements, of products provided to the Purchaser.

[SOW 553] *The Contractor shall deliver all the CoC's for Commercial-off-the-Shelf (COTS) products (software, including firmware and hardware) released by the COTS Vendors.*

[SOW 554] *The CoCs delivered by the Contractor shall be part of the acceptance data package of the product.*

[SOW 555] *The Contractor shall provide a CoC at release of product to the Purchaser unless otherwise instructed.*

8. CONFIGURATION MANAGEMENT

8.1. Configuration Standards

[SOW 556] *Although the Contractor is asked to install/ integrate/ test PFEs (COTS HW, SW and FW), the Contractor shall be responsible for establishing and maintaining an effective Configuration Management (CM) organisation to implement the CM programme and manage the CM functions (Configuration Identification and Documentation, Configuration Control, Configuration Status Accounting, Configuration Audits).*

[SOW 557] *The Contractor shall establish and maintain the CM policies, processes and practices in conformance with STANAG 4427 Ed. 3 and underpinning ACMPs (ACMP-2000, ACMP- 2009, ACMP-2100) and ISO 10007:2017.*

[SOW 558] *The Contractor shall include a Configuration Management Plan (CMP) as part of the PMP describing all aspects of Configuration Management following the requirements set in the ACMP-2009-SRD-40.1 ref. # 4.3.C.*

[SOW 559] *The Contractor shall implement the CM activities for any hardware, software and firmware delivered, integrated, tested and/or customized and document provided, used or defined in the frame of the project and shall fully integrate the COTS elements-data in order to implement a unique CM framework.*

[SOW 560] *The Contractor shall define the CI trees (Baselines), hierarchically structured, clearly defining and identifying each node/leaf as Configuration Item (CI), Hardware Configuration Item (HWCI), Computer Software Configuration item (CSCI), Hardware Parts (HWP) or (Computer Software Component (CSC) in accordance with the guidelines provided in the above defined ACMPs and ISO.*

[SOW 561] *The Contractor shall define and deliver, as a minimum the following Baselines:*

- ***a.*** *Allocated Baseline (ABL): it starts to be developed at the beginning of the design phase (MS0 – three (3) working weeks); it is established and "frozen" at the end of the design phase (at MS0 - it is also known as "as-designed" baseline);*
- ***b.*** *Product Baseline (PBL): It starts to be developed at the beginning of the production phase. It is established and "frozen" at the end of the production phase (at factory integration/test).*

[SOW 562] *The Contractor shall deliver the first ABL at MS0 – three (3) working weeks and the final ABL at MS1*

[SOW 563] *The Contractor shall deliver the first PBL at MS1 + four (4) working weeks and then at test start and whenever changes occur during the production, testing and warranty phases.*

[SOW 564] *Both the ABLs and the PBLs shall be maintained under Configuration Control and subject to change management processes and procedures (ECPs, RFCs) in accordance with STANAG 4427 Ed. 3 and underpinning ACMPs.*

[SOW 565] *The ABL and the PBL shall be delivered by the Contractor, with incremental contents, using the NCI Agency templates listed below:*

- ***a.*** *AI 16.32.04 - ABL Template*
- ***b.*** *AI 16.32.05 - PBL Template*

[SOW 566] *The Contractor shall use the Instructions and templates provided by the purchaser to issue any ECPs and RFCs in accordance with the following applicable AIs:*

- **a.** AI 16.32.02 – Preparation of ECP forms

b. AI 16.32.02 Annex A – ECP Form
c. AI 16.32.03 – Preparation of RFC forms
d. AI 16.32.03 Annex A – RFC Form

[SOW 567] All the baselines shall be developed, maintained and fully documented in the Contractor's PLM (Product Lifecycle Management) tool.

[SOW 568] For each Baseline and relevant modifications (in accordance with the Change Request/Engineering Change Proposal/Engineering Change Order - CM CR/ECP/ECO - processes) the Contractor shall export the baselines in the form of CMDBs, covering as a minimum the following relationships:

a. Contract functional/non-functional requirements to Functional elements of the FBL (the FBL shall not be delivered but shall be defined and maintained by the Contractor)
b. Functional Elements of the FBL to Major CIs of the ABL
c. Major CIs of the ABL to Full CIs (CIs, HWCIs, CSCIs, HWPs, CSCs) tree (PBL)
d. Major CIs of the PBL to Services/Sub-Services delivered by the System (mapping of CIs vs Services and vice versa)

[SOW 569] The Contractor shall incorporate in the baselines, under a unique hierarchical tree, all the information relevant to the OEMs/COTS hardware, software and firmware used and integrated in the System.

[SOW 570] Each element of the PBL shall include as minimum the following pieces of information (in accordance with the type of item):

a. Position in the structure (hierarchical level or indenture code)
b. Physical location (REFDEF or similar positional code) coherent with the As-Built Drawings and manuals
c. Type of Configuration Item (CI, HWCI, CSCI, HWP, CSC)
d. Type of MRI/MSI, coherent with the LBS/PBS
e. Item identifiers (i.e. PNR, NCAGE, nomenclature, issue/release/revision/version)
f. Item Data (SMR Code, Price, Price UOM, MOQ, start of warranty/licence validity etc.)
g. Inventory Data (SRN or License number if applicable etc.)
h. CI documentation:
i. For HWCIs/HWPs: specifications, datasheet, Certificates of Conformity (CoC), Declaration of Conformity (DoC), Items Setting Documents (ISD – how to configure HW/SW/FW) etc.
j. For HWCIs/CIs: interconnection diagrams, interface specifications/control documents, Test procedures, Test records, integration data, customization/setting procedures etc.
k. For CSCIs/CSCs: SW Release Notes (SRN), SW test data records, SW metrics (type of language, Line of Code, number of function points etc.), SW Source Code (if specifically generated or modified/adapted/customized in the frame of the project), SW Installation files, SW Version Description Documents (VDDs), SW installation/customization procedures, SW settings, SW operating manual etc.
l. Alternative (PNR, NCAGE, nomenclature, issue/release/revision/version)
m. NATO Stock Number (NSN)

[SOW 571] *The Contractor shall prepare and make available the PBLs and shall prepare and attend as a minimum the following Physical Configuration Audits (PCA) events:*

- ***a.*** *Pre-Test PCA – Before test start to determine the to-be-tested Products baseline*
- ***b.*** *Post-Test PCA – Immediately after test completion to determine the applicable PBL immediately before site acceptance.*
- ***c.*** *(New) Spares and consumables Audit (if any) at completion of each environment (MS 2 to 5) – three (3) working weeks.*

[SOW 572] *All the hardware, software and firmware elements and media and IPS and System documentation provided in the scope of this project shall be properly identified, coherent and consistent with the CM baselines in use at the time of issuance/installation.*

8.2. Confidentiality

[SOW 573] *The NPKI-M HPS shall ensure that a confidentiality label (policy, classification, releasability) is automatically included into each information element or product, showing the highest classification of information it contains.*

[SOW 574] *In line with [C-M(2002)49, 2002] COR5, the Security Classification in NPKI-M HPS shall include:*

a. *Policy Identifier / Information Ownership: e.g., NATO, NATO/EAPC (Euro-Atlantic Partnership Council), ISAF (International Security Assistance Force);*

b. *Classification Marking: e.g., Unclassified, Restricted, Confidential, Secret;*

c. *Category/Caveats: e.g., Releasable to AUS/FIN, Releasable to ISAF, Releasable to Coalition*

[SOW 575] *The machine readable structure of the Security Label in the solution shall be in accordance with NSECREF.20 in Table 4.*

[SOW 576] *The NPKI-M HPS shall provide visual confirmation to Users (on-screen) of the security classification including any releaseability caveats (e.g., Releasable to ISAF) of the displayed data*

[SOW 577] *The NPKI-M HPS shall include a configurable colour-based visual cue in addition to text to indicate the security classification in screens/ reports / prints / messages.*

[SOW 578] *The NPKI-M HPS shall insert a Security Classification construct into headers / footers and metadata of generated, created or exported reports, MS Office files and PDF files. The user shall be prompted to be able to change the security classification.*

[SOW 579] *The NPKI-M HPS shall propose the highest classification level of the selected objects. If no classification is specified for the selected objects, then the repository classification level shall be proposed.*

[SOW 580] *The NPKI-M HPS shall allow the authorised user to override the proposed classification level by choosing another. Classification is mandatory and shall be composed of three fields: authority, classification, releasability.*

[SOW 581] *If a file is being generated or exported in a format that does not use headers / footers, the solution shall include a Security Classification into an appropriate part of the file so that it is clearly visible to the User.*

9. HEALTH AND SAFETY

9.1. General Safety Requirements

[SOW 582] *The Contractor shall undertake all measures to comply and ensure compliance with respective Regulations for Industrial Safety applicable throughout this Contract.*

[SOW 583] *The Contractor shall comply with the national legislation of respective territorial Host Nations concerning job accidents, incident prevention and hygiene at work.*

[SOW 584] *The Contractor shall also make legal arrangements for protection of the life and security of all its personnel and to guarantee medical assistance whenever necessary due to job accidents. The same legal arrangements shall be applied to sub-Contractor personnel under Contractor's responsibility.*

[SOW 585] *When working at the Purchaser's facilities, the Contractor shall comply with all safety and security directives and procedures applicable to the site, contracted scope of work and premises in which the Contractor will perform their duties.*

[SOW 586] *The detailed procedures, instructions and guidance shall be obtained from the site commander/ the principal, the security manager and Health & Safety manager respectively at given site.*

[SOW 587] *The Contractor shall learn respective procedures.*

[SOW 588] *The Contractor shall confirm in writing that their understood the procedures.*

[SOW 589] *The Contractor shall confirm in writing commitment to comply with the procedures and apply them in practice.*

[SOW 590] *The Contractor shall provide personnel mentally and physically capable of undertaking their duties as stipulated in the subject contract.*

[SOW 591] *The Contractor is responsible for provision of Personal Protective Equipment (PPE) for its employees accordingly to the activities and scope of works stipulated in the subject contract.*

[SOW 592] *The PPE shall be compliant with Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment or its equivalent of respective territorial Host Nation in North America.*

9.2. Hardware Requirements

The hardware shall be designed to operate using an external mains power supply conforming to International Electrotechnical Commission standard IEC 60038:2009, 400/230 V, 50 Hz.' or its national equivalent of respective territorial Host Nation in North America.

[SOW 593] *The hardware shall function without degradation under the existing environmental conditions.*

All conductors and hardware shall be rated for current carrying capacity in accordance with the applicable industry standards.

All cables shall have non-toxic, non-flammable coating.

All cables shall be halogen-free, low smoke, thermoplastic insulated and sheathed cables in compliance with IEC 62821 or its national equivalent.

[SOW 594] *Free movement of cables shall be assured when equipment is pulled out for maintenance/repair.*

[SOW 595] *Wires and cables shall be placed and protected as to prevent contact with rough irregular surfaces and sharp edges and to prevent wear due to vibration.*

[SOW 596] *Cables connecting to components mounted onto doors or panels shall be protected so that no possibility of damage arises during opening and closing of doors or panels.*

[SOW 597] *Cable harnesses shall be routed away from heat generating equipment and no wire or cable connection shall be in tension.*

[SOW 598] *For the dimensioning of the bending radius of cables the regulations of VDE 0298, part 3 or equivalent shall be followed.*

[SOW 599] *All soldered connections shall be clean and smooth in appearance and shall provide excellent electrical conductivity.*

[SOW 600] *The insulation of soldered wires shall not show damage from the heat of the soldering operation.*

[SOW 601] *Dissimilar metals shall not be used in intimate contact unless suitably protected against electrolytic corrosion.*

Any equipment supplied under this Contract shall include interfaces to enable connection to the grounding system in accordance with respective national safety regulations and INFOSEC requirements.

[SOW 602] *Safety grounding interfaces shall be in accordance with safety regulations, including IEC 60364-5-54:2011 or its national equivalent of respective territorial Host Nation in North America.*

[SOW 603] *The hardware shall be designed and constructed in such a way that it does not run in a hazardous condition or put human safety at risk.*

[SOW 604] *The Contractor shall design and/or select the hardware on the basis of inherent safety features that protect not only the human operators and maintainers but also the equipment itself.*

[SOW 605] *The hardware shall be designed in such a way that no special or difficult techniques that require unusual dexterity or skill in removing or installing items is required.*

Materials used in the hardware, under the specified environmental and service conditions or as a result of heating due to conflagration, shall not liberate:

- *Gases that combine with the atmosphere to form an acid or corrosive alkali.*
- *Toxic or corrosive fumes that would be detrimental to the performance of the equipment or health of personnel.*
- *Gases that will produce an explosive atmosphere.*

No hazardous materials (of any kind) shall be used in the construction of the hardware.

Glass fibre materials shall not be used as the outer surface or covering on cables, wire or other items where they may cause skin irritation to operating personnel.

The hardware shall be provided with safety markings and labels that meet following requirements:

- *Safety markings and labels shall be provided identifying any potential hazards to personnel.*
- *Warning labels shall be attached wherever there is any potential of heavy lifting, specific handling guidance, electrical, chemical, excessive noise,*

electromagnetic radiation or heat hazard or a potential hazard caused by human contact with materials, particularly when removal of covers will expose the hazard.

- *Safety markings shall be readily visible during operation and maintenance conditions.*
- *Warning markings shall be as permanent as the normal life expectancy of the equipment on which they are affixed and shall be placed as close as possible to the point of danger.*
- *All matters of safety including but not limited to hot surfaces, mechanical hazards, electrical shocks and radiation hazards shall be fully and clearly addressed in the user operations and technical manuals.*
- *Training and other provided documentation (for example deployment manual, user manuals, maintenance manuals etc.) shall prominently identify hazardous situations and the preparation, precautions and actions to avoid and contain them.*
- *All warning instructions shall be provided in English and in the official language of the territorial Host Nation.*

Noise generated by the hardware in operation shall not exceed the levels specified in the local regulations or Environmental Noise Directive (2002/49/EC) whichever it is more restrictive for operational, maintenance areas.

Any rotating or other moving part such as ventilators, blowers, drive belts etc., shall be shielded or protected adequately to prevent accidental contact by and injury to any personnel during operation and maintenance.

[SOW 606] Projecting and overhanging edges shall be kept to a minimum.

[SOW 607] Edges and corners shall be rounded.

[SOW 608] When rounding of edges and corners is not possible, protective covers shall be applied.

[SOW 609] When protective covers are not possible or not reasonably practical for installation, sharp edges shall be marked with appropriate safety labels and marking.

[SOW 610] When packed, the system shall not include any protruding point which could either be damaged or damage persons or property during transportation.

9.3. Environmental Protection

[SOW 611] The Contractor shall take all reasonable and practical measures to protect the public and his own employees against accidents, and to safeguard the environment and apply the best practices available in the field.

[SOW 612] Environmental requirements shall be implemented and verified by the Contractor, as a minimum, in accordance with European Union environmental protection regulations and the national implementation references (i.e. law, regulation) pursuant to the EU Directives or national equivalents for North America deliveries.

[SOW 613] The Contractor shall consider the environmental impact of the delivered hardware during its life cycle and disposal, and the hardware documentation shall provide the appropriate recommendations to the user.

ANNEX A System Requirements Specification

A.1. Non-Functional Requirements

[SRS 1] *Dedicated core infrastructure shall be provided to support the NPKI system operation. The infrastructure shall be provided in Mons Datacenter and NATO HQ datacentre.*

[SRS 2] *In each location, a Production infrastructure shall be provided for each security domain (4 installations)*

[SRS 3] *In Mons, 2 separate Reference environments shall be provided, replicating the full production environment (4 installations)*

[SRS 4] *SRS requirements shall apply to each of the eight (8) installations of the hosting platform environment.*

[SRS 5] *The NPKI-M Hosting Platform Services(HPS) shall comprise active and passive components which will make up a new and separate 'NPKI' domain in in Mons Datacenter and NATO HQ datacentre, to accommodate the NPKI systems to be installed by the Work Package 1 Contractors.*

[SRS 6] *The NPKI-M HPS cabling, active and passive components used in forming the NPKI domain shall be physically separate from any other network and be used exclusively to support the NPKI systems*

[SRS 7] *The NPKI-M HPS shall comply with the PRREF.1 (HLD).In particular, the NPKI-M HPS shall comprise all equipment (Hardware and Software) as necessary and in line with the purchaser furnished equipment (PFE) included in the NPKI-M High Level design document.*

[SRS 8] *The NPKI-M HPS shall include all components required to configure and operate the hosting environment as well as the networking environment.*

[SRS 9] *The NPKI-M HPS shall comprise sufficient processing and storage to be able to support the NPKI applications. The interface between the storage system and the NPKI-M HPS is included in this project.*

[SRS 10] *The NPKI-M HPS shall comprise a management security zone, protected by approved firewall, and extended to NPKI operations locations in NATO HQ and Mons for dedicated administration terminals be used for the isolated management zone. Management workstations shall be configured and connected to the management zone.*

[SRS 11] *The NPKI-M HPS shall comprise two (2) PFE core switches with the detailed specification according to the PRREF.1 (HLD), high-level design document, as well as patches to interconnect the core switches. The core switches shall be configured according to the Purchaser's guidance.*

[SRS 12] *The NPKI-M HPS shall comprise one (1) Out Of Band Switch with the detailed specification according to the PRREF.1 (HLD). The switches shall be installed in the Server Room with 1Gig Fiber connections.*

[SRS 13] *The NPKI-M HPS shall include a Firewall Cluster, as well as patches to interconnect the Firewalls, with the detailed specification according to the high-level design document.*

[SRS 14] *The NPKI-M HPS shall comprise two IPSec VPN firewalls, as well as all necessary patches to interconnect, with the detailed specification according to the high-level*

design document. The VPN firewals shall be connected between Evere and Mons (Production to Production) and between the two reference environments in Mons.

[SRS 15] *The Contractor shall install and configure the 2 instances of the Vsphere software per hosting platform, and shall apply security hardening settings according to the Purchaser's guidance.*

[SRS 16] *The Contractor shall deploy VM templates for Red Hat Enterprise Linux and Windows server and support the Purchaser and partners in deploying Virtual Servers for NPKI applications.*

[SRS 17] *The NPKI-M HPS shall comprise Servers and all necessary patches to interconnect.*

[SRS 18] *The NPKI-M HPS shall comprise a VEEAM backup appliance and licenses to allow Vsphere backup and bare metal server backup and restore capabilities. VEEAM backup licenses will be provided by the Purchaser. The Contractor shall provide all necessary patches to interconnect (10Gig Fibre connection).*

[SRS 19] *The NPKI-M HPS shall comprise Hosting Servers running Vmware Vsphere Software with the detailed specification according to thePRREF.1 (HLD).*

[SRS 20] *The servers and Vmware Vsphere Software shall be installed in the server room and configured in accordance with the the Purchaser's guidance.*

[SRS 21] *The NPKI-M HPS shall comprise an SMC capability to allow Operating System patching and Anti-Virus updates based on NCSC tools including but not limited to SCCM, SCOM and Trellix EPO. The licenses for SMC tools will be provided by the Purchaser.*

[SRS 22] *The SMC servers shall be installed on the provided hosting environment. The Contractor shall support the Purchaser to install and configure the software according to the Purchaser's guidance.*

[SRS 23] *The NPKI-M HPS shall comprise two (2) NPKI management workstations (each with 1 screen, 1 keyboard, 1 mouse and 1 smartcard reader) for each site and security domain.*

[SRS 24] *The Contractor shall install and configure the above workstations according to the Purchaser's guidance in various locations in Mons and NHQ. The Contractor shall patch and cable the devices as required in Mons and NHQ.*

[SRS 25] *The NPKI-M HPS shall comprise multiple PostgreSQL database (DB)clusters deployed in a high availability configuration in compliance with PRREF.1(HLD).*

[SRS 26] *The Contractor shall provide a third party application that is required to implement multiple HA Database clusters for PostGreSQL.*

[SRS 27] *The Contractor shall provide a database expert(s) who will advise on the industry best practices regarding high availability (HA) deployment of PostgreSQL database services, as per SOIW section 3.1.4.*

[SRS 28] *The Contractor shall install and configure the PostgreSQL DB clusters, complying with the following:*

a. *PostgreSQL DB clusters shall be deployed on Red Hat operating system from the RHEL repositories, unless stated otherwise by the Purchaser.*

b. *PostgreSQL DB clusters shall be able to contain multiple databases with a synchronous replication.*

c. *PostgreSQL DB clusters shall have enough resources such as CPU, memory and storage to support the NPKI-M HPS HA deployment based on the Purchaser's resource requirements which will be shared by the Purchaser before the PostgreSQL DB cluster deployment.The Contractor may also make recommendations based on their experience.*

d. *PostgreSQL DB cluster configuration parameters shall be decided with the Purchaser such as listening ports, TLS/SSL settings, log file locations, backup locations etc.*

e. *DB cluster deployment shall apply the NATO Cyber Security Centre (NCSC) security settings for PostgreSQL on Linux. These include OS level network configurations, file permissions, user permissions, TLS settings and SELinux configurations but not limited to these settings.*

f. *DB cluster Red Hat servers shall apply the NATO Cyber Security Centre (NCSC) security settings for Red Hat Enterprise Linux 8.*

g. *PostgreSQL DB clusters shall be configured for synchronous data replication between master and standby servers.*

h. *PostgreSQL DB clusters shall be configured with automated failover to ensure service continuity without interruption to the database clients.*

i. *PostgreSQL DB clusters shall be thoroughly tested for HA availability functionalities and failover cases.*

[SRS 29] *The Contractor shall provide step by step deployment and failover recovery documents for the deployed PostgreSQL Database services.*

[SRS 30] *The NPKI-M HPS shall comprise multiple Red Hat Directory Servers deployed in a high availability configuration in compliance with PRREF.1 (HLD).*

[SRS 31] *The Contractor shall install and configure Red Hat Directory Servers, complying with the following:*

a. *Red Hat Directory servers shall be deployed on Red Hat operating system from the RHEL repositories, unless stated otherwise by the Purchaser.*

b. *Red Hat Directory servers in the controlled zone shall be configured as read-write servers as known as supplier servers. These shall be configured as multi-supplier replication nodes.*

c. *Directory servers in the front-end zone shall be configured as read only servers as known as consumer directory servers. These shall be configured to replicate data from all supplier servers.*

d. *Directory servers shall have enough resources such as CPU, memory and storage to support the NPKI-M HPS HA deployment based on the Purchaser's resource requirements which will be shared by the Purchaser before the Red Hat Directory servers deployment.*

e. *Directory servers configuration parameters shall be decided with the Purchaser such as listening ports, TLS/SSL settings, log file locations, backup locations, file permission settings etc.*

f. *Directory servers' hosts shall apply the NATO Cyber Security Centre (NCSC) security settings for Red Hat Enterprise Linux 8.*

[SRS 32] *The NPKI-M HPS shall comprise Red Hat Satellite management system deployed in a high availability configuration in compliance with PRREF.1 (HLD).*

[SRS 33] *The NPKI-M HPS shall comprise identity management functionality in compliance withPRREF.1 (HLD).*

[SRS 34] *The NPKI-M HPS shall have all Red Hat Enterprise Linux (RHEL) Licences with premium support.*

[SRS 35] *All RHEL licenses shall be associated to NCSC account by the Contractor.*

[SRS 36] *All Red Hat Enterprise Linux (RHEL) Licences shall be valid in accordance with [SOW 128].*

[SRS 37] *The ContractorContractor shall install and configure Enterprise Linux (RHEL) Licences with smartmanager add-on, directory server licenses and any additional components and add-ons required for NPKI-M HPS based on the list of VMs, specified in PRREF.1 (HLD) .*

[SRS 38] *The ContractorContractor shall do the sanitization of the Linux packages in compliance with the Purchaser's template.*

[SRS 39] *Smart Card Authentication shall be used as a Multi Factor Authentication (MFA) mechanism to the Red Hat Operating System,*

[SRS 40] *The Contractor shall provide the direct integration of Linux machines with the NCSC Tier 2 Active Directory (AD) domain including (MFA) based on two PFE smartcard types for authentication to all Red Hat operating systems.*

[SRS 41] *In case of direct integration is not feasible, the Contractor shall provide a Red Hat Identity Management Solution in compliance with PRREF.1 (HLD) .*

A.2. Functional Requirements

A.2.1. Hardening

[SRS 42] *The Contractor shall be responsible for ensuring that all components delivered under this contract are configured in accordance with NATO Approved Security Settings, as per Section 2. Any required deviations to those settings shall be informed to the Purchaser immediately*

[SRS 43] *As well as data stored in or by a product or system, security also applies to data in transmission.*

[SRS 44] *The NPKI-M HPS shall comply with security settings, installation guides and configuration guidelines from NCSC.*

[SRS 45] *The NPKI-M HPS components shall be configured with the latest security patches and updated with the latest security guidelines from the NCSC.*

[SRS 46] *In the event that security settings or guidance for a particular system/component are not available, or the guidance available is for an earlier version of the system/component, the Contractor shall provide hardening guidance based upon vendor best practices tailored to the NCSC environment.*

[SRS 47] *The Contractor shall support development of hardening guides by providing draft guidelines where required to support the NATO Agency Authorized Software List (A2SL) or other approval processes.*

[SRS 48] *The Contractor shall support any new registrations of all software provided that is opensource or otherwise and is not already listed on NATO A2SL register.*

[SRS 49] *This shall include the Contractor providing all requested and relevant documentation, installation media, appropriate licenses and use cases, to ensure that all software provided by the Contractor is correctly captured, tested, approved, and listed in NATOs A2SL register.*

[SRS 50] *All software that will be used will be the latest version supported on the A2SL.*

[SRS 51] *The NPKI-M HPS shall be capable of operating within the NS and NR WAN environments (including servers, network, services and workstations) in the presence of the currently approved NATO Security Settings (target version to be provided by the Purchaser during the Design Stage). Any deviations from the approved security settings shall be identified by the Contractor prior to testing and shall be subject to approval of the Purchaser.*

[SRS 52] *The Contractor shall harden credential stores and mechanisms.*

[SRS 53] *The solution shall automatically log account creation, modification, enabling; and privilege elevation, disabling and removal.*

A.2.2. Integrity

[SRS 54] *The NPKI-M HPS shall maintain referential integrity between entities across all services data sets.*

[SRS 55] *The NPKI-M HPS shall provide an ability to perform cascade deletion of the lower level entities that are dependent on higher level entities.*

[SRS 56] *The NPKI-M HPS shall contain residual information protection mechanisms to ensure that purged information is no longer accessible.*

[SRS 57] *The NPKI-M HPS shall ensure that newly created objects do not contain information that should not be accessible (i.e. information that has been logically deleted).*

A.2.3. Authentication

[SRS 58] *The NPKI-M HPS shall include functionality to deliver Role Based Access Control (RBAC) to define multiple roles for administrative, privileged, audit, and non-privileged users*

[SRS 59] *The NPKI-M HPS shall be configured with RBAC to implement the user roles defined in the design and agreed by the Purchaser.*

[SRS 60] *Role-based access control shall be applied according to the following guidelines:*

a. *Users are associated with User Roles and also with Organizations.*
b. *User Roles determine the functions and types of objects available to the User.*
c. *Organizations determine the data available for use by the available functions.*
d. *A user has permission on a particular data item only if the user has an authorised role and is a member of that organization*

[SRS 61] *The NPKI-M HPS shall allow two or more users to have the same role simultaneously.*

[SRS 62] *The NPKI-M HPS shall be integrated with the Purchaser's infrastructure via the Purchaser's existing authentication and authorization mechanisms as agreed in the design by the Purchaser.*

[SRS 63] *The NPKI-M HPS shall manage login and password details for Users that cannot be authenticated through Active Directory*

[SRS 64] *The NPKI-M HPS shall provide privileged system accounts (e.g., system and security administrator accounts)*

[SRS 65] *Administrator responsibilities shall be divided into three Tiers as per NSECREF.21 in Table 4.*

[SRS 66] *Tier 0 and 1 administration and controlled maintenance shall only be done from computers dedicated to administration tasks of their respective tier, controlled by the Purchaser and without Internet or external CIS access.*

[SRS 67] *Tier 0 and 1 administration dedicated computers shall be hardened, only required software shall be installed and they are on a dedicated management network segregated from the rest of the CIS.*

[SRS 68] *Tier 0 and 1 administration computers system updates shall not be pushed from a lower Tier.*

[SRS 69] *Administration shall not be allowed from standard user accounts.*

[SRS 70] *Administrator access to hypervisors shall be controlled.*

[SRS 71] *Administrator privileges shall be managed to ensure least privilege.*

[SRS 72] *The NPKI-M HPS shall implement functionality to authenticate user access using multiple-factors.*

[SRS 73] *Multiple Factor Authentication (MFA) implementations shall not rely on external network connectivity (such as telephone or mobile phone networks).*

[SRS 74] *The Contractor shall support the Purchaser to configure NPKI-M HPS to integrate with the Purchaser's existing MFA infrastructure, to be determined in the design and agreed by the Purchaser.*

[SRS 75] *The NPKI-M HPS shall uniquely Identify and Authenticate Users.*

[SRS 76] *The NPKI-M HPS shall allow an authorised user (i.e. System Admin) to manage (create, update, delete) System User Accounts, password details, and assign User Roles to User Account and manage general access privileges of individual User Accounts*

[SRS 77] *The NPKI-M HPS shall apply the Purchaser's password policy.*

The password policy will enforce individuals to select a password that is at least 9 characters long, comprising uppercase, lowercase and symbols. The password must be changed every 6 months or if the user suspects it has been compromised (for example, if the user thinks anyone has observed entering the password).

[SRS 78] *The NPKI-M HPS shall deny the re-use of 10 previous passwords.*

[SRS 79] *The NPKI-M HPS user accounts shall be locked after 5 unsuccessful authentication attempts.*

[SRS 80] *The NPKI-M HPS passwords shall be stored in encrypted form.*

[SRS 81] *The NPKI-M HPS accounts that are no longer required shall be locked/ deleted.*

[SRS 82] *The NPKI-M HPS shall protect User credentials in transit.*

[SRS 83] *The NPKI-M HPS shall protect session IDs.*

[SRS 84] *The NPKI-M HPS session IDs shall never be included in any URL or sent in the referrer header to prevent caching by the browser. Session IDs shall be long, complicated random numbers which cannot be easily guessed.*

[SRS 85] *The NPKI-M HPS shall employ encryption of the entire login transaction using SSL or similar technologies.*

[SRS 86] *The NPKI-M HPS shall allow the system administrator to set a "timeout" period which shall automatically log-out any sessions which have been inactive for that period of time. The system administrator shall be able to disable this feature.*

[SRS 87] *The NPKI-M HPS shall allow the system administrator to prevent multiple concurrent authentications from the same user from different locations (IP addresses). The system administrator shall be able to disable this feature*

[SRS 88] *The NPKI-M HPS shall protect the User's entire session via SSL to ensure that the session ID (e.g., session cookie) cannot be read off the network*

[SRS 89] *The NPKI-M HPS shall allow the User (with the same User-id) to access the same information and functionality from any workstation within the solution's domain (i.e., 'roving User' functionality). This capability shall not depend on the availability of Active Directory.*

[SRS 90] *The NPKI-M HPS containing passwords of privileged system accounts (e.g. Domain Admin) shall be stored as NATO SECRET information in an approved container with controlled and recorded access.*

[SRS 91] *The interval for password change in NPKI-M HPS shall be selectable.*

[SRS 92] *The NPKI-M HPS shall allow authenticated Users to manage their password and their User profile (e.g., e-mail address, unit) information.*

[SRS 93] *The NPKI-M HPS shall provide help texts to support the login process together with links to recover lost password and login details.*

[SRS 94] *The NPKI-M HPS shall limit the feedback of information during authentication to prevent Users gaining knowledge of the authentication process.*

[SRS 95] *The NPKI-M HPS shall include functionality to integrate with Purchaser's infrastructure via the following authentication and authorization mechanisms:*

a. *Microsoft Active Directory (AD),*
b. *Lightweight Directory Access Protocol (LDAP) (plus LDAP over SSL/TLS aka LDAPS),*
c. *X.509 Certificate-based authentication,*
d. *Secure Shell (SSH) versions that are considered secure at time of deployment using password / public-key authentication,*
e. *Kerberos Single Sign-On (SSO),*
f. *Terminal Access Controller Access Control System Plus (TACACS+),*
g. *Remote Access Dial-In User Service (RADIUS).*

[SRS 96] *Lateral movement of an attacker shall be restricted/prevented by using appropriate security measures including but not limited to segmentation and LAPS.*

A.2.4. Audit and Accountability

[SRS 97] *The NPKI-M HPS shall generate audit records for auditable events, addressing, among others, the following events:*

a. *System start-up (including re-starts) and shutdown*
b. *Log-on (including log-on attempts) and log-off of individual users*
c. *Changes to permissions and privileges of users and groups*
d. *Changes to security relevant system management information(including audit functions)*
e. *Start-up and shutdown of the audit function*
f. *Any access to security data*
g. *Deletion, creation or alteration of the security audit records*
h. *Changes to system date and time*
i. *Unsuccessful attempts to access system resources*

[SRS 98] *Audit tracing in NPKI-M HPS shall be permanently effective.*

[SRS 99] *The NPKI-M HPS shall protect the information from unauthorised modification or deletion.*

[SRS 100] *The NPKI-M HPS shall establish access permissions to audit information.*

[SRS 101] *The NPKI-M HPS shall associate individual user identities to auditable events.*

[SRS 102] *The NPKI-M HPS shall action on failed attempts at log-on.*

[SRS 103] *The NPKI-M HPS shall create and maintain an archive of audit information.*

[SRS 104] *The NPKI-M HPS shall generate and forward logs compatible with the Purchaser's existing Splunk-based logging solution.*

[SRS 105] *All required additional Splunk licenses will be provided by the Purchaser.The Contractor shall support the Purchaser to integrate NPKI-M HPS's log sources, providing a mapping to the Splunk CIM (common information model) to ensure logs are parsed correctly by Splunk.*

[SRS 106] *The NPKI-M HPS in each NATO security domain shall send its logs to the Purchaser's Splunk-based logging solution in the same domain.*

[SRS 107] *In addition to forwarding logs to Splunk, NPKI-M HPS shall additionally store logs locally to its own storage for independent inspection by administrators for a minimum of thirty (30) days.*

A.2.4.1. User Audit Logs

[SRS 108] *The NPKI-M HPS shall record in traceable logs all selected transactions, database activities, technical events (e.g., dataset synchronisation, directory replication) and accessing of data.*

[SRS 109] *The NPKI-M HPS shall ensure operations at the business object level are recorded in traceable logs.*

[SRS 110] *If so configured, The NPKI-M HPS shall ensure User operations at system function level are recorded in traceable logs.*

[SRS 111] *If so configured, The NPKI-M HPS shall support audit trailing to all User and System actions and messages on sending, deleting and viewing to log all User activities*

[SRS 112] *If so configured, The NPKI-M HPS shall log all configurations changes with the trace to persons or systems.*

A.2.4.2. System Audit Logs

[SRS 113] *The NPKI-M HPS shall generate and maintain an Audit Log for each of the following auditable events, shall associate individual User identities to those events, and shall include date and time of the event, type of event, User identity, and the outcome (success or failure) of the event:*

a. *System start-up and shutdown*
b. *The start/end time of usage of system applications (system components) by individual Users*
c. *Changes to permissions and privileges of Users and groups*
d. *Changes to security relevant system management function*
e. *Configuration changes*
f. *Any access to audit log*
g. *Deletion, creation or alteration of the security audit records*
h. *All privileged operations*
i. *All updates of system access rights*
j. *All attempts to delete, write or append the Audit files*

[SRS 114] *The NPKI-M HPS shall use integrity checking countermeasures to ensure that the Audit Log has been archived successfully*

[SRS 115] *The NPKI-M HPS shall support the following warning system events:*

a. *Low network bandwidth: Organisational Node-specific*
b. *Almost out of disk space: solution server specific*
c. *Almost out of table space: solution server specific*

[SRS 116] *The NPKI-M HPS shall support the following error system events:*

a. *Crashing of software components*
b. *Unplanned and recovering of a connection with a terminator*
c. *Incorrect received data*
d. *Replication failure*

A.2.5. TLS

[SRS 117] *The NPKI-M HPS shall include functionality to secure all network communication between its components with Transport Layer Security (TLS) using a protocol version of at least v1.2, unless otherwise stated in the requirements or agreed in the design by the Purchaser.*

[SRS 118] *The NPKI-M HPS shall be configured to prefer secure network communication using TLS v1.3 wherever available within the constituent components that must interoperate, unless otherwise stated in the requirements or agreed in the design by the Purchaser*

[SRS 119] *The NPKI-M HPS shall be configured to use secure network communication using TLS v1.2 wherever TLS v1.3 is not available within the constituent components that must interoperate, unless otherwise stated in the requirements or agreed in the design by the Purchaser*

[SRS 120] *Where components in the NPKI-M HPS support deprecated TLS protocol versions support for those protocol version(s) shall be disabled in those components. For the avoidance of doubt, no component shall be able to initiate or receive communications using TLS versions prior to v1.2.*

[SRS 121] *The NPKI-M HPS shall be configured to use TLS communication using key material from the NATO PKI, unless otherwise stated in the requirements or agreed in the design by the Purchaser.*

[SRS 122] *The NPKI-M HPS products and components containing TLS functionality shall support the ability to validate certificates using Certificate Revocation Lists (CRLs) as per NNREF.15 in Table 6.*

[SRS 123] *The NPKI-M HPS products and components containing TLS functionality shall be configured to validate certificates using the Purchaser's CRL locations defined within the certificates, within each domain, site, and enclave as agreed in the design and by the Purchaser.*

[SRS 124] *All digital certificates installed / configured / used within the course of the NPKI-M project or required to support project implementation shall be compatible with the specifications laid out in the NATO PKI (NPKI) policy document, NSECREF.16 in Table 4.*

[SRS 125] *The NPKI-M HPS products and components containing TLS functionality shall be compliant with the specifications laid out in the NATO PKI (NPKI) policy documents.*

[SRS 126] *The NPKI-M HPS products and components using TLS shall support the following algorithms and key sizes, or a subset of these if using a preferred later protocol version (i.e. TLS v1.3):*

a. *Hash: SHA-2 (FIPS 180-2) with parameter sizes of both 256 and 384 bits*
b. *Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) (ANSI X9.62) with parameter size of 384 bits*
c. *Signature: RSA (PKCS #1) with parameter size of at least 2048 bits*
d. *Key Wrap: AES (see FIPS 197) with parameter sizes of both 128 and 256 bits*
e. *Key Establishment: Elliptic Curve Diffie-Hellman (ECDH) (ANSI X9.63) with parameter size of 384 bits*
f. *Key Establishment: RSA (PKCS #1 latest version) with parameter size of at least 2048 bits*
g. *The NPKI-M HPS products and components using TLS shall support Galois Counter Mode (GCM) for authenticated encryption.*

[SRS 127] *The NPKI-M HPS products and components using TLS shall prevent the use / negotiation of cipher suites with the following options:*

a. *NULL ciphers.*
b. *Anonymous (Anon) authentication.*

c. *All NPKI-M HPS network components using TLS shall allow the Purchaser to whitelist or approve only a specific subset of approved cipher suites for TLS-based communication.*

[SRS 128] *A path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and each server certificate shall match the Fully Qualified Domain Name of the server and be valid.*

[SRS 129] *TLS shall be used for all connections, internal (e.g. backend) or external, that involve sensitive data or functions.*

[SRS 130] *Backend TLS connection failures shall be logged.*

[SRS 131] *Connections to external systems that involve sensitive information or functions shall be authenticated.*

[SRS 132] *Connections to / from external systems shall use accounts configured to have the minimum privileges necessary for the application to function properly.*

[SRS 133] *Failed TLS connections shall not fall back to an insecure connection.*

[SRS 134] *Certificate paths shall be built for all client certificates using configured trust anchors and revocation information.*

[SRS 135] *Each application shall use a single standard TLS implementation that is configured to operate in an approved mode of operation.*

[SRS 136] *Specific character encodings shall be defined for all connections (e.g., UTF-8).*

A.2.6. VPN

[SRS 137] *The NPKI-M HPS shall include Virtual Private Networks (VPN) functionality to terminate and transit connections of VPNs for at least the following types:*

a. *Internet Protocol Security (IPsec) (up to and including IPsec Version 2, as per IETF RFCs),*

b. *Transport Layer Security (TLS, up to and including TLS v1.3).*

A.2.7. DNS

[SRS 138] *The NPKI-M HPS shall receive Internal name/Address resolution services from the Purchaser's DNS capability.*

[SRS 139] *The Contractor shall support the Purchaser to integrate all compatible components of the NPKI-M HPS with the Purchaser's DNS Capability in accordance with PRREF.1 (HLD) .*

[SRS 140] *The Contractor shall support the Purchaser to do the initial configurations and tuning in the solution components to ensure that the integration with Purchaser's existing DNS capability work properly.*

A.2.8. Transmission Security

[SRS 141] *When cryptography is used as a security measure to protect transmitted information, the requirements of NSECREF.19 in Table 4 are met.*

A.2.9. Protection of Hardware and Media

[SRS 142] *Hardware and Media components' BIOS/UEFI of the NPKI-M HPS shall be accessible only by authorized privileged users.*

[SRS 143] Security patching of BIOS/UEFI firmware shall be performed.

[SRS 144] Unnecessary BIOS/UEFI features shall be disabled.

[SRS 145] UEFI secure boot shall be enabled when available.

[SRS 146] In order to protect the integrity of the data and media and the confidentiality of the data, CIS storage media shall be physically transported in accordance with NSECREF.4 and and where appropriate, NSECREF.5 in Table 4.

A.2.10. Protection of Services

[SRS 147] FC and IP SANs shall use mutual authentication.

[SRS 148] All PKI certificates shall be obtained from the appropriate NPKI Certification Authority (CA).

[SRS 149] The validity of PKI certificates shall be verified through all subordinate CAs to the Root CA.

A.2.11. Accreditation

[SRS 150] The Contractor shall support the Purchaser in performing a security vulnerability analysis of all Contractor-delivered components in the NPKI-M HPS in in each NATO security domain prior to acceptance. (A "Type 3 Security Audit" as per NSECREF.18 in Table 4.

[SRS 151] The Contractor shall take corrective action to address any vulnerabilities identified from the security vulnerability analysis.

[SRS 152] The Contractor shall replace any item where a TEMPEST seal has been broken at no additional cost to the purchaser.

A.2.12. Web Security

The following requirements are applicable to any and all components of the NPKI-M HPS exposing a web-based user or management interface.

A.2.12.1. Authentication

[SRS 153] Password fields shall not echo the user's password when it is entered, and password fields (or the forms that contain them) have autocomplete disabled.

[SRS 154] Authentication controls shall fail securely.

[SRS 155] Identity Information related to authentication (such as credentials) managed by the website shall not traverse networks unencrypted.

[SRS 156] Forgot password functionality and other recovery paths shall not send the existing or new passwords in clear text to the user.

[SRS 157] Username enumeration shall not be possible via login, password reset, or forgot account functionality.

[SRS 158] No default passwords shall be used, for the website or any components.

[SRS 159] Passwords shall never be hard-coded in any source code. Not even in an encrypted/hashed form.

[SRS 160] *All authentication credentials for accessing services internal (e.g. local authentication) and external to the application (e.g. a DB) are encrypted or hashed, and stored in a protected location (not in source code).*

[SRS 161] *When applicable, decryption keys shall not be accessible or exposed through the web service.*

[SRS 162] *All authentication controls shall be enforced on the server side.*

[SRS 163] *Account passwords shall be stored encrypted or hashed in such a way it should not be possible to identify identical passwords.*

[SRS 164] *A mechanism shall be in place to protect against vertical (a single account tested against all possible passwords) and horizontal brute forcing (all accounts tested with the same password e.g. "Password1"). A correct credential entry should incur no delay.*

[SRS 165] *Password entry fields shall allow or encourage the use of passphrases, and do not prevent long passphrases or highly complex passwords from being entered, and shall provide a sufficient minimum strength to protect against the use of commonly chosen passwords.*

[SRS 166] *Account management functions (such as registration, update profile, forgot username, forgot password or disabled / lost token) that might regain access to the account shall be at least as resistant to attack as the primary authentication mechanism.*

[SRS 167] *Users shall be able to safely change their credentials using a mechanism that is at least as resistant to attack as the primary authentication mechanism.*

[SRS 168] *Authentication credentials shall be configured to expire after an administratively configurable period.*

[SRS 169] *All authentication decisions shall be logged, including increased delays between successive unsuccessful logging attempts (linear back-offs) and temporal account locks (soft-locks).*

[SRS 170] *Forgot password and other recovery paths shall send a time-limited activation token or use two factor proofs.*

[SRS 171] *Shared knowledge questions/answers (so called "secret" questions and answers) shall not be used.*

[SRS 172] *The system shall be configured to disallow the use of a configurable number of previous passwords.*

[SRS 173] *All authentication controls (including libraries that call external authentication services) shall have a centralized implementation, used for all websites.*

A.2.12.2. Session Management

[SRS 174] *A session management mechanism shall be used after a successful authentication.*

[SRS 175] *The related security context shall be maintained until the session expires.*

[SRS 176] *Any change in the security context shall require re-authentication.*

[SRS 177] *Sessions shall be invalidated when the user logs out.*

[SRS 178] *Sessions shall timeout after a specified period of inactivity.*

[SRS 179] *Only non-persistent cookies shall be used for session management purposes, so that the session ID does not remain on the web client cache for long periods of time.*

[SRS 180] All pages that require authentication to access them shall have logout links.

[SRS 181] A Session ID shall never be disclosed other than in areas specifically designed to hold session tokens (e.g. cookie headers or custom HTTP headers); particularly in URLs, error messages, or logs.

[SRS 182] The application shall not support URL rewriting of session cookies.

[SRS 183] Session ID shall be changed or cleared on logout or when the session expires.

[SRS 184] At least one mechanism shall be used to prevent cookie theft and session hijacking. (e.g. HttpOnly and Secure attributes or usage of TLS during the entire session)

[SRS 185] The Session ID shall be changed on re-authentication.

[SRS 186] The name used by the session ID shall not be extremely descriptive nor offer unnecessary details about the purpose and meaning of the ID.

[SRS 187] Session IDs shall never be cached, applications must use restrictive cache directives for all the web traffic exchanged through HTTP and HTTPS, such as the "Cache-Control: no-cache, no-store" and "Pragma: no-cache" HTTP headers, and/or equivalent META tags on all or (at least) sensitive web pages.

[SRS 188] It shall not be possible to determine a session ID knowing the previously generated ID(s). For that reason, session IDs shall be generated using a cryptographically secure (pseudo)random number generator and they shall be at least 128 bits long.

[SRS 189] Only Session IDs generated by the application framework shall be recognized as valid by the application, unless for a business requirement such as single sign on.

[SRS 190] Session IDs using cookies shall have their path set to an appropriately restrictive value for that site. The domain cookie attribute restriction should not be set unless for a business requirement, such as single sign on.

[SRS 191] The application shall not permit duplicate concurrent user sessions, originating from different machines.

[SRS 192] Sessions shall timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).

A.2.12.3. Access Control

[SRS 193] The NPKI-M HPS shall use AD integrated authentication, with role based users access to the content (at web application and DB level).

[SRS 194] The NPKI-M HPS shall be deployed such that:

a. *Users shall only access functions or services for which they possess specific authorization.*
b. *Users shall only access URLs for which they possess specific authorization.*
c. *Users shall only access data files for which they possess specific authorization.*
d. *Directory browsing shall be disabled unless deliberately desired.*
e. *Access controls shall fail securely.*
f. *Access controls shall be enforced on the server side.*
g. *User and data attributes and policy information used by access controls shall not be manipulated by end users unless specifically authorized.*

h. *If access controls are enforced by the presentation layer on the client side (e.g. input validation, access to functions, etc.) the same controls shall be enforced on the server side.*

i. *Access control decisions involving non-granted accesses shall always be logged. In addition, it shall be possible to configure the site to log all access control decisions.*

j. *The application shall use a mechanism to identify users as part of all high value transactions or accessing sensitive data, and the application shall verify this identity when processing these requests.*

k. *There shall be a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource.*

A.2.12.4. Input Validation

[SRS 195] *The runtime environment shall not be susceptible to buffer overflows, or there shall be security controls preventing buffer overflows.*

[SRS 196] *The runtime environment shall not be susceptible to SQL Injection, or there shall be security controls preventing SQL Injection.*

[SRS 197] *The runtime environment shall not be susceptible to Cross Site Scripting (XSS), or there shall be security controls preventing XSS Injection.*

[SRS 198] *The runtime environment shall not be susceptible to LDAP Injection, or there shall be security controls preventing LDAP Injection.*

[SRS 199] *The runtime environment shall not be susceptible to OS Command Injection, or there shall be security controls preventing OS Command Injection.*

[SRS 200] *The runtime environment or parser shall not be susceptible to XML and XPath injection or there shall be security controls preventing XML and XPath injection.*

[SRS 201] *All input validation failures shall result in input rejection or input sanitization in accordance with the NSECREF.15 in Table 4.*

[SRS 202] *Input validation or encoding routines shall be performed and enforced on the server side in accordance with the NSECREF.15 in Table 4.*

[SRS 203] *If input validation controls are enforced by the presentation layer on the client side (e.g. size or format constraints, input type, etc.) the same controls shall be enforced on the server side.*

[SRS 204] *Untrusted data that are output to HTML pages (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) shall be properly escaped for the applicable context.*

[SRS 205] *URL redirects and forwards shall not include unvalidated data.*

[SRS 206] *Parameters shall be canonicalized, input validated, and output encoded to prevent both local and remote file inclusion attacks, particularly where input could be executed, such as header, source, or template inclusion. Parameters shall never be used to manipulate filenames, pathnames or any file system object without first being canonicalized and input validated to prevent local file inclusion attacks.*

[SRS 207] *Input data shall be canonicalized for all downstream decoders or interpreters prior to validation.*

[SRS 208] *When an application framework is used on client side, security sensitive fields (such as role, password, etc.) shall be protected against clear text disclosure when sending requests to the server (encryption, protection from automatic binding, etc.).*

[SRS 209] *The application shall have defences against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.).*

[SRS 210] *A single input validation control shall be used by each application for each type of data that is accepted.*

[SRS 211] *All input validation failures shall be logged.*

[SRS 212] *For each type of output encoding/escaping performed by each application, there shall be a single security control for that type of output for the intended destination.*

A.2.12.5. Cryptography at Rest

[SRS 213] *All cryptographic functions shall be implemented on the server side unless purposely designed in another manner.*

[SRS 214] *All cryptographic modules shall fail securely.*

[SRS 215] *Data-at-rest decryption keys shall be protected from unauthorized access.*

[SRS 216] *Cryptographic keys shall be managed (e.g., generated, distributed, revoked, expired) using approved NATO policies in NSECREF.19 in Table 4.*

[SRS 217] *Cryptographic algorithms used by the application shall be selected from the NATO Type B algorithm[4] suite.*

[SRS 218] *Cryptographic modules shall operate in their approved mode according to their published security policies.*

A.2.12.6. Error Handling and Logging

[SOW 614] *Each application shall not output error messages or stack traces containing sensitive data that could assist an attacker, including Session ID and personal information.*

[SOW 615] *Logs events shall include at a minimum:*

a. *Time stamp from a reliable source*
b. *Severity level of the event*
c. *An indication that this is a security relevant event (if mixed with other logs)*
d. *The identity of the user that caused the event (if there is a user associated with the event)*
e. *The source IP address of the request associated with the event*

---

[4] *Type B cryptographic algorithms are evaluated and approved by a NATO member nation's NCSA, but are not developed under their control.*

f. *Status of the event (e.g. succeeded or failed)*

g. *A description of the event*

[SRS 219] Error handling logic in security controls shall deny access by default.

[SRS 220] Logging controls shall be implemented on the server.

[SRS 221] Security logging controls shall have the ability to log both success and failure events that are identified as security-relevant.

[SRS 222] Security logs shall be protected from unauthorized access and modification.

[SRS 223] The application shall not log application-specific sensitive data that could assist an attacker, including user's Session IDs and personal or sensitive information.

[SRS 224] A log analysis tool shall be available to allow the analyst to search for log events based on combinations of search criteria across all fields in the log record format supported by this system.

[SRS 225] There shall be a single logging implementation that is used by each application.

A.2.12.7. Data Protection

[SRS 226] Forms containing sensitive information shall have disabled client side caching, including autocomplete features.

[SRS 227] Sensitive data shall be sent to the server in the HTTP message body (i.e., URL parameters are never used to send sensitive data).

[SRS 228] Cached or temporary copies of sensitive data sent to the client or stored in the server shall be protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).

[SRS 229] The list of sensitive data processed by each site shall be identified, and that there shall be an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit).

[SRS 230] There shall be a method to remove each type of sensitive data from the application at the end of its required retention period.

[SRS 231] The integrity of interpreted code, libraries, executables, and configuration files shall be verified using checksums or hashes.

[SRS 232] Sensitive data shall be rapidly sanitized from memory as soon as it is no longer needed.

[SRS 233] Each application should have the ability to detect and alert on abnormal numbers of requests to prevent screen scraping, automated use of web service extraction or data loss prevention.

A.2.12.8. HTTP Security

[SRS 234] All applications shall accept only a defined set of HTTP request methods, such as GET and POST, unused methods shall be explicitly blocked.

[SRS 235] Every HTTP response shall contain a single content type header specifying a safe character set (e.g., UTF-8).

[SRS 236] HTTP headers, in both requests and responses, and URIs shall contain only printable ASCII characters.

[SRS 237] *Web sites shall never switch a given session from HTTP to HTTPS, or vice versa, as this can disclose the session ID in the clear through the network.*

[SRS 238] *Web applications shall avoid the extremely common HTTP to HTTPS redirection on the home page, as this single unprotected HTTP request/response exchange can be used by an attacker to gather (or fix) a valid session ID.*

[SRS 239] *If HTTPS is required, the web application shall make use of "HTTP Strict Transport Security (HSTS)" (previously called STS) to enforce HTTPS connections.*

[SRS 240] *HTTP headers and / or other mechanisms for older browsers shall be used to protect against click jacking attacks.*

[SRS 241] *When feasible, web applications should not mix encrypted and unencrypted contents (HTML pages, images, CSS, Javascript files, etc.) on the same host (or even domain - see the "domain" cookie attribute), as the request of any web object over an unencrypted channel might disclose the session ID.*

[SRS 242] *When feasible, web applications, should not offer public unencrypted contents and private encrypted contents from the same host. It is recommended to instead use two different hosts, such as www.example.com over HTTP (unencrypted) for the public contents, and secure.example.com over HTTPS (encrypted) for the private and sensitive contents. The former host only has port TCP/80 open, while the later only has port TCP/443 open.*

A.2.12.9. Business Logic

[SRS 243] *The application logic shall have protection mechanisms against application crashing, memory access violations (buffer overflow) and unexpected exceptions such as data destruction and resource depletion (Memory, CPU, Bandwidth, Disk Space, etc.)*

[SRS 244] *Each application shall limit the use of CPU intensive operations and set timeouts for operations requiring unreasonable times.*

[SRS 245] *High value business logic flows shall be processed and/or verified in a trusted environment, such as on a protected and monitored server.*

[SRS 246] *Each application shall not allow spoofed transactions, such as tampering with or replaying session, transaction state, transaction or user IDs.*

[SRS 247] *Each application shall not allow tampering of business logic parameters.*

[SRS 248] *Each application shall have defensive measures to protect against repudiation attacks, such as verifiable and protected transaction logs, audit trails or system logs, real time monitoring of user activities and transactions for anomalies.*

[SRS 249] *Each application shall protect against information disclosure attacks, such as direct object reference, tampering, session brute force or other attacks.*

[SRS 250] *Each application shall have sufficient detection and governor controls to protect against brute force (such as continuously using a particular function) and denial of service attacks.*

[SRS 251] *Each application shall have sufficient access controls to prevent elevation of privilege attacks.*

[SRS 252] *Each application shall only process business logic flows in sequential step order, with all steps being processed in realistic human time, and not process out of order, skipped steps, process steps from another user, or too quickly submitted transactions.*

[SRS 253] *Each application shall have business limits and enforces them in a trusted location (as on a protected server) on a per user, per day or daily basis, with configurable alerting and automated reactions to automated or unusual attack. The business limits and totals shall be reasonable for the business concerned.*

[SRS 254] *Each application shall have protection against Cross-Site Request Forgery attacks (CSRF), such as the inclusion of random tokens, which shall be validated for each action in the context of the web application (in the protected area, i.e. post-authentication).*

[SRS 255] *Each application shall have additional authorization (such as step up or adaptive authentication), and / or segregation of duties to enforce anti-fraud controls as defined by a risk assessment.*

A.2.12.10. Files and Resources

[SRS 256] *Files, other than static pages and dynamic content (CGI scripts), shall be stored outside the webroot.*

[SRS 257] *Each web or application server shall be configured by default to deny access to remote resources or systems outside the web or application server.*

[SRS 258] *All application code shall not execute uploaded data.*

[SRS 259] *Files shall be scanned by anti-virus scanners to prevent upload of known malicious content.*

[SRS 260] *Remote IFRAMEs and HTML 5 cross-domain resource sharing shall not allow inclusion of arbitrary remote content.*

[SRS 261] *File upload to all applications shall be restricted based on a whitelist. Binary file inspection, file extensions checks and content mime-type checks shall be conducted on file upload.*

A.2.12.11. Miscellaneous (HTML5/Java)

[SRS 262] *Sensitive data shall not be stored in storage area of a thick client, including to system or application logs.*

[SRS 263] *3rd-party JavaScript libraries or thick-clients shall be hosted within the web application / web server and not hot-linked from external untrusted sources.*

[SRS 264] *Secret keys or passwords shall not be hard-coded in the executable.*

[SRS 265] *Unique identifiers shall never be used as security controls (e.g. Unique device ID (UDID) or MAC addresses).*

[SRS 266] *Session timeouts shall be configurable.*

[SRS 267] *All thick clients shall not request more permissions or access to resources than those strictly required for its correct operation.*

[SRS 268] *Files with unrestricted permissions shall never be generated.*

[SRS 269] *3rd-party JavaScript libraries in use shall be up to date and contain no known vulnerabilities.*

[SRS 270] *All code shall be signed.*

[SRS 271] *All thick clients shall be configured to run a in a restricted sandbox, with no access to OS resources, such as file system or native libraries.*

[SRS 272] *Any thick client binary shall be obfuscated.*

[SRS 273] *Any thick client shall implement certificate pinning to prevent the proxying of app traffic.*

[SRS 274] *Web data, such as HTTPS traffic, shall not be cached.*

[SRS 275] *The query string shall not be used for sensitive data. Instead, a POST request via SSL should be used with a CSRF token.*

[SRS 276] *Remote sign-in for content management operation shall not be available from outside the domain.*

A.2.13. Management and Maintenance

[SRS 277] *The NPKI-M HPS (including but not limited to servers, workstations, operating systems, hypervisors, applications, network switches, and firmware) shall be remotely (via internal networks) configured, managed, monitored, patched and updated.*

[SRS 278] *The NPKI-M HPS shall include a secure remote access capability to each instance in each solution with the latest version of SSH or via an HTTPS web GUI.*

[SRS 279] *Remote access to the NPKI-M HPS shall be routed through managed access control points.*

[SRS 280] *If remote access by privilege users is required, it shall be explicitly authorized by the SAA during the security accreditation process and strictly controlled during the system operation.*

[SRS 281] *Information exchange through the internet shall be allowed and configured via remote access through the Purchaser's Boundary Protection Systems (BPS)*

[SRS 282] *The Contractor shall support the Purchaser to integrate all components of the NPKI-M HPS with the existing configuration, management, monitoring, patching, and update solutions in NCSC in accordance with PRREF.1 (HLD) .*

[SRS 283] *The Contractor shall support the Purchaser to integrate of all compatible components of the NPKI-M HPS with the Purchaser's Monitoring Capability, based on the Solarwinds platform. All components not capable of integration shall be indentified to the Purchaser for evaluation of a alternate mechanisms for service monitoring.*

[SRS 284] *The Contractor shall support the Purchaser to integrate of all compatible components of the NPKI-M HPS into the Purchaser's Logging and Auditing capability, based on the Splunk platform.*

[SRS 285] *The Contractor shall support the Purchaser to integrate the initial configuration and tuning of the logs sources to ensure relevant data is ingested into the Purchaser's Splunk SIEM solution.*

[SRS 286] *The Contractor shall support the Purchaser to do the initial configurations and tuning in the NPKI-M HPS components to ensure that the integration with existing NCSC solutions work properly.*

[SRS 287] *The Contractor shall ensure that the NPKI-M HPS being deployed for every subsystem contains common product components, firmware and software versions, and configurations, wherever possible, to minimize the spares and maintenance overhead for the Purchaser.*

[SRS 288] *The NPKI-M HPS shall be delivered in the latest, vendor supported stable version at the time of delivery unless otherwise agreed by the Purchaser during the design phase.*

[SRS 289] The NPKI-M HPS's web GUIs shall support modern browsers and shall be compatible HTML 5 or newer.

[SRS 290] Any type of maintenance shall be authorized and documented in accordance with configuration management procedures.

[SRS 291] Maintenance shall only be conducted by appropriately authorized or supervised personnel.

[SRS 292] The Contractor shall conduct the maintenance under the classified contract procedure as set out in reference K. on equipment containing classified information.

[SRS 293] The confidentiality of data shall be ensured during maintenance.

A.2.14. Supportability

[SRS 294] The Contractor shall support the Purchaser to integrate the NPKI-M HPS with Microsoft System Center Configuration Manager (SCCM) where supported by the product.

[SRS 295] The NPKI-M HPS shall support collection and reporting of asset inventory metrics for all components using Microsoft System Centre Configuration Manager, including:

a. Memory
b. Operating System
c. Peripherals
d. Services
e. Login tracking
f. Software existence and usage
g. Licensing

A.2.15. Out of Band Management

[SRS 296] All Out-of-Band Management Ports shall be cabled and connected to dedicated VLANs as agreed in the design and by the Purchaser.

A.2.16. Monitoring

[SRS 297] The Purchaser's existing Solarwinds installation in each domain shall be configured to monitor each component of the NPKI-M HPS.

[SRS 298] All required additional Solarwinds licenses will be provided by the Purchaser. The Contractor shall support the Purchaser to install and configure Solarwinds license and software to accommodate each component of the NPKI-M HPS in each NATO security domain.

[SRS 299] The NPKI-M HPS shall include functionality to manage and monitor its components via the Simple Network Management Protocol (SNMP) version 3 using AES encryption

[SRS 300] Each component the NPKI-M HPS of shall be able to report its 'capacity' related aspects for the resources used (disk, memory, cpu, network) to the Purchaser's existing Solarwinds installation.

[SRS 301] Each component of the NPKI-M HPS shall be able to report its application aspects addressed (loads, transactions,users) to the Purchaser's existing Solarwinds installation.

A.2.17. Virtualization

[SRS 302] All virtualized workloads deployed by the Contractor shall support native operation on a VMWare ESXi hypervisor.

[SRS 303] All virtualized workloads shall be integrated with the Purchaser's VMware management platforms in each domain.

[SRS 304] A physical server or server cluster shall only host VMs processing information of the same security domain.

A.2.18. Technical Configurations

[SRS 305] New or modified versions of equipment shall be validated prior to their introduction in the system.

[SRS 306] Only authorized privileged users shall implement changes to the NPKI-M HPS baseline.

[SRS 307] Configuration settings shall be established, documented by the Contractor and approved by the Purchaser.

[SRS 308] The NPKI-M HPS components shall be configured to provide only required capabilities (least functionality).

[SRS 309] The NPKI-M HPS components which are not required are either shall be uninstalled, not installed or disabled.

A.2.19. Network

[SRS 310] The NPKI-M HPS operating systems and applications shall not be configured as network appliances without SAA approval.

[SRS 311] The NPKI-M HPS shall include Network Address Translation (NAT) functionality to remap Internet Procotol (IP) address spaces between one another by modifying the header information on packets transiting the firewall.

[SRS 312] The NPKI-M HPS shall include Port Address Translation (PAT) functionality to remap port numbers in the headers of packets transiting the firewall.

A.2.20. NTP

[SRS 313] The Contractor shall support the Purchaser to integrate the NPKI-M HPS with the NCIA NCSC's existing NTP solution.

A.2.21. Security Domains

[SRS 314] The hardware and software delivered by the Contractor shall operate in four (4) independent domains; NR, NS, and NR-REF and NS-REF domains.

A.2.22. Independent Operation

[SRS 315] Each solution provided by the Contractor shall be capable of operating fully and independently within an air-gapped enclave with no access to or from external networks, excepting specific solution components where such access is intrinsically required by the functions agreed by the Purchaser (for example, where a requirement states that such access is required). In no case shall access be allowed from networks

operating at a system high level (such as those classified NATO SECRET) to a system of lower operation except via method agreed during design and with accredidation.

[SRS 316] *Each solution shall not require access to the Internet for any purpose, including but not limited to product activation or functional operations, excepting specific solution components where such access is intrinsically required by the functionality and agreed by the Purchaser (for example, where a requirement states that Internet-based cloud access is required).*

[SRS 317] *Systems deployed in separate classification domains (e.g. NR and NS) shall be able to operate fully and independently of one another, unless otherwise agreed by the Purchaser*

A.2.23. Business Continuity

[SRS 318] *The Contractor shall design, install, and configure the backup including data, logs, software, baseline configuration and VM templates for the solution as agreed in the design and by the Purchaser*

[SRS 319] *The solution shall include functionality to perform a manual backup and restore of all configuration elements on each solution component.*

[SRS 320] *Data back-ups shall be stored so that an incident cannot impact both the solution and its back-ups.*

A.2.24. Compliance with standards and guidelines

[SRS 321] *All icons included in the designed solution shall be compliant with the NNREF.18 in Table 6.*

[SRS 322] *All solutions shall be compliant with the NNREF.17 in Table 6. In particular:*

a. *All solutions shall be compliant to ISO 9241-12 for the presentation of information*
b. *All solutions shall be compliant to ISO 9241-13 for user guidance.*
c. *All solutions shall be compliant to ISO 9241-14 for menu dialogues*
d. *All solutions shall be compliant to ISO 9241-16 for direct manipulation dialogues*
e. *All solutions shall be compliant to ISO 9241-143 for form filling dialogues*
f. *All solutions shall be compliant to ISO 9241-171 for accesibility*
g. *All solutions shall follow the dialogue principles stated in ISO 9241-110.*

A.2.25. Logon Procedures

[SRS 323] *In applications where users must log-on to the system, log-on shall be a separate procedure that must be completed before a user is required to select among any operational options.*

[SRS 324] *Appropriate prompts for log-on shall be automatically displayed on the user's terminal when accessing the application.*

[SRS 325] *User identification procedures shall be as simple as possible, consistent with adequate data protection.*

[SRS 326] *When required, the password shall not be echoed on the display. An asterisk (*) or similar symbol will be displayed for each character when inputting secure passwords during log-on.*

[SRS 327] *When passwords are required, users shall be allowed to choose their own passwords since a password chosen by a user will generally be easier for that individual to remember. Guidelines for password selection shall be given so that users will not choose easily guessable ones.*

[SRS 328] *Users shall be allowed to change passwords whenever they choose; all passwords should be changed at periodic intervals (not to exceed six months).*

[SRS 329] *Users shall be provided feedback relevant to the log-on procedure that indicates the status of the inputs.*

[SRS 330] *If a user cannot log-on to a system, a prompt shall be provided to explain the reason for this inability. Log-on processes should require minimum input from the user consistent with the requirements prohibiting illegal entry.*

A.2.25.1. Logon Banners

[SRS 331] *For each entry point to each solution where an interactive user logon is possible, the solution shall be capable of displaying a customisable logon warning banner.*

[SRS 332] *The customised logon warning banners on each solution shall be configured as agreed in the design and by the Purchaser.*

A.2.25.2. Log-off Procedures

[SRS 333] *When a user signals for system log-off, or application exit or shut-down, the system shall check pending transactions to determine if data loss seems probable. If so, the computer should prompt for confirmation before the log-off command is executed.*

A.2.26. Error Management and Data Protection

[SRS 334] *Where users are required to make entries into a system, an easy means shall be provided for correcting erroneous entries. The system shall permit correction of individual errors without requiring re-entry of correctly entered commands or data elements.*

[SRS 335] *Data shall be protected from unauthorized use, potential loss from equipment failure, and user errors.*

[SRS 336] *A capability shall be provided to facilitate detection and correction of errors after keying in, but before entering into the system. While errors should be detected early,error checking should occur at logical data entry breaks, e.g., at the end of data fields rather than character-by-character, in order to avoid disrupting the user.*

[SRS 337] *User errors shall be minimized by use of software checks of user entries for validity of item, sequence of entry, completeness of entry, and range of value.*

[SRS 338] *Error messages shall be constructive and neutral in tone, avoiding phrases that suggest a judgment of the user's behaviour. The error messages shall reflect the user's view, not that of the programmer. Error messages should be appropriate to the user's level of training, be as specific as possible to the user's particular application, and describe a way to remedy, recover, or escape from the error situation.*

[SRS 339] *The user shall be able to (a) stop the control process at any point in a sequence as a result of indicated error or as an option and (b) return easily to previous levels in multi-step processes in order to nullify an error or to effect a desired change.*

[SRS 340] *When the user enters correction of an error, such corrections shall be implemented by an explicit action by the user (e.g., actuation of an ENTER key). All error corrections by the user shall be acknowledged by the system, either by indicating that a correct entry has been made or by another error message.*

[SRS 341] *Spelling and other common errors shall not produce valid system commands or initiate transactions different from those intended. When possible, the system shall recognize common misspellings of commands and execute the commands as if spelling had been correct. Computer-corrected commands, values, and spellings shall be displayed and highlighted for user confirmation.*

[SRS 342] *Where control input errors are detected by the system, error messages shall be available, and error recovery procedures shall be provided.*

[SRS 343] *A computer-detected error, as well as the error message, shall be continuously displayed until the error is corrected.*

[SRS 344] *Provision shall be made to prevent accidental actuation of potentially destructive control actions, such as accidental erasure or memory dump.*

[SRS 345] *Automated measures shall be provided to minimize data loss from intruders in a system or from errors by legitimate users.*

ANNEX B Purchaser Furnished Equipment (PFE) and services

Purchaser Furnished Equipment (PFE) list will be provided to the Contractor with the Puchaser's NPKI-M High Level Design in PRREF.1.

ANNEX C Cyber Incident Reporting

1. **NATO Information Protection**

1.1 The Contractor shall identify all NATO Information associated with the execution and performance of this contract. At the post-award conference, the Contractor and Purchaser Project Manager shall identify and affirm marking requirements for all NATO Information to be provided to the Contractor, and/or to be developed by the Contractor, associated with the execution and performance of this contract.

1.2 The Contractor shall track all NATO Information associated with the execution and performance of this contract. The Contractor shall document, maintain, and upon request, provide to the Purchaser, a record of subcontractors, vendors, and/or suppliers who will receive or develop NATO Information and associated with the execution and performance of this contract.

1.3 The Contractor shall restrict unnecessary sharing and/or flow down of NATO Information associated with the execution and performance of this contract – in accordance with NATO marking and dissemination requirements and based on a 'need-to-know' to execute and perform the requirements of this contract.

1.4 The contractor shall develop and store all NATO technical data (e.g., source code) in a secure facility. The contractor shall prevent computer software, in the possession or control of non-NATO entities on non-NATO information systems, from having connections to the network through segregation control (e.g., firewall, isolated network, etc.).

1.5 The Contractor shall flow down the requirements of this clause to their subcontractors, vendors, and/or suppliers.

2. **Safeguarding of NATO RESTRICTED Information**

Introduction

2.1 This contract security clause is published by the Security Committee (AC/35) in support of NATO Security Policy, C-M (2002)49, and its supporting directives.

Background

2.2 This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract. This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

2.3 This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

Section I- Responsibility

2.4 Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by

the Contracting Authority. The SO shall also act as the point of contact with the Contracting Authority or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

Section II – Personnel Security

2.5 A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the facility security officer.

Section III – Physical Security

2.6 NR information classified NR shall be stored in a locked cabinet or Office Furniture (e.g. office desk drawer) within an Administrative Zone, Class I Security Area, or Class II Security Area. Information classified NR may also be stored in a locked cabinet, vault, or open storage area approved for information classified NC or higher shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet, or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone[5]).

2.7 NR information shall be handled in Administrative Zones or National equivalent to Class I or II security areas. NR information can be also held under personal custody.

Section IV- Security of Information

Control and Handling

2.8 Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

2.9 Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5, second sentence.

Reproduction

2.10 Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

[5] An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

Destruction Requirements

2.11 NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

2.12 Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

2.13 Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

2.14 NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transmission

2.15 The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

a) moved by postal or commercial services;

b) carried by Contractor's personnel; or

c) transported as freight by commercial services.

Release

2.16 NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

2.17 Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the Contracting Authority.

Section V- Sub-Contracting

2.18 Sub-contracts shall not be let without the prior approval of the Contracting Authority.

2.19 Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

2.20 Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

International Visits

2.21 Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be

provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

Section VI- Handling of NATO RESTRICTED Information on Communication and Information Systems (CIS)

Security Accreditation of Communication and Information Systems (CIS)

2.22 Security accreditation shall be performed by the National Security Accreditation Authority (SAA) (or their delegated SAA) for all contractors' CIS that are used to handle (store, process or transmit) NATO RESTRICTED (NR) information. The security accreditation process shall ensure that the NATO's minimum security standards[6] are met.

2.23 This contract security clause contains the rules and regulations that shall be applied by the contractor's SO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the contractor as a result of the contract. This clause includes specific provisions to be satisfied by the contractor under delegation from the Contracting Authority for the accreditation of the contractor's CIS handling NR information. Under this delegated authority the contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the contractor's response in acknowledgement of the receipt and requirements of the Security Aspects Letter associated with the contract.

2.24 It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

2.25 The SO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

2.26 The following describes the minimum security requirements for handling NR information on contractors' CIS that shall be met:

Identification and Authentication

2.27 An up-to-date list of authorised users shall be maintained by security management staff.

2.28 Credentials shall be established and maintained to identify authorised users.

2.29 Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.

2.30 Passwords shall be a minimum of 9 characters long and shall include numeric and "special" characters (if permitted by the system) as well as alphabetic characters;

[6] As described in the policy on Security within the NATO and its supporting Directives on CIS Security

2.31 Passwords shall be changed at least every 180 days. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.

2.32 The re-use of a number of previous passwords shall be denied.

2.33 The system shall provide only limited feedback information to the user during the authentication process.

2.34 Accounts that are no longer required shall be locked or deleted.

2.35 When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

Access Control

2.36 The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security-related documentation.

2.37 From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.

2.38 Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.

2.39 Access to security and system information shall be restricted to only authorised security and system administrators.

2.40 Access privileges shall be implemented to restrict the type of access that a user may be permitted (e.g., read, write, modify, and delete).

2.41 The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user's data access/display devices other than unlocking the activity of the session.

2.42 The system shall allow user-initiated locking of the user's own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user's data access/display devices other than unlocking the activity of the session.

2.43 Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

Security Audit

2.44 An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:

- all log on attempts whether successful or failed;

- log off (including time out where applicable);
- the creation, deletion or alteration of access rights and privileges;
- the creation, deletion or alteration of passwords.

2.45 The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in human readable format either directly (e.g., storing the audit trail in human-readable format) or indirectly (e.g., using audit reduction tools) or both.

2.46 Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.

2.47 The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.

2.48 A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security violation).

Protection against Malicious Software

2.49 Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependant upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).

2.50 The virus/malicious code detection software shall be regularly updated.

Mobile Code

2.51 The source of the mobile code shall be appropriately verified.

2.52 The integrity of the mobile code shall be appropriately verified.

2.53 All mobile code shall be verified as being free from malicious software.

2.54 Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

Availability

2.55 Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

Import/Export of Data

2.56 Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.

2.57 All data imported to or exported from the CIS shall be checked for malware.

Configuration Management

2.58 A detailed hardware and software configuration control system shall be available and regularly maintained.

2.59 Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.

2.60 Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.

2.61 An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.

2.62 The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.

2.63 The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects

2.64 i.e. any potential adverse effects of the modification on existing security measures, shall be considered and appropriate action taken.

2.65 The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.

2.66 The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.

2.67 Changes to the system or network configuration shall be assessed for their security implications/impacts.

2.68 The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

Security Management

2.69 Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.

2.70 The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

Approved products

2.71 An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

2.72 The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

Security Testing

2.73 The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

Transmission Security

2.74 NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using approved cryptographic products.

2.75 Wireless LAN

2.76 The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

2.77 NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

Virtualisation

2.78 When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

2.79 A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

2.80 Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

2.81 Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure. For example, a firewall shall not be virtualised.

2.82 The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

2.83 Access to the hypervisor functions shall be appropriately controlled.

2.84 The ability to “cut-and-paste” between virtual machines shall be appropriately configured and controlled.

2.85 The ability to create virtual machines shall be appropriately configured and controlled.

2.86 Virtual Machines shall be suitably de-commissioned after use.

2.87 Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

2.88 Virtual Servers and Virtual Workstations shall not be located on the same physical host.

2.89 Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be located on the same physical host as those operating in the LAN.

2.90 The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti malware and Active Directory communication mode shall be allowed.

2.91 Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative account.

2.92 The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.

2.93 The SAN used to host Virtualisation operating at different security classifications shall be isolated onto separate Logical Unit Numbers.

2.94 Modifications to the 'Master Copy/Version' of a Virtual Machine shall be appropriately controlled.

2.95 Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

Interconnections to a CIS not accredited to handle NR information

2.96 Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" (current reference AC/322-D/0030-REV5) and "Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet" (current reference AC/322- D(2010)0058). These Directives may be obtained from the Contracting Authority.

2.97 Interconnection to another CIS, especially the internet, will significantly increase the threat to a contractor's CIS and therefore the risk to the security of the NR information handled by the contractor's CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process. Security requirements can also be found in the latest version of the NATO document entitled "Technical and Implementation Directive on CIS Security (current reference AC/322-D/0048- REV3). This Directive may be obtained from the Contracting Authority.

2.98 When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

Disposal of IT Storage Media

2.99 For IT storage media that has at any time held NR information the following sanitisation shall be performed to the entire storage media prior to disposal:

- EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives):
- overwrite with random data at least three times, then verify storage content matches the random data;
- Magnetic Media (e.g. hard disks): overwrite or degauss;
- Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of 10mm2 or less;
- Other storage media: seek security requirements from the Security Accreditation Authority.

Portable Computing Devices (laptops, tablets, etc)

2.100 Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR information that do not use approved encryption shall not be taken outside the contractor's premises unless held under personal custody. The term "drives" includes all removable media. Any authentication token and/or password(s)

associated with the encryption product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

Physical Security of CIS Handling NR information

2.101 Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

2.102 CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

Security of NR Removable Computer Storage Media

2.103 Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle.

Use of CIS Equipment Privately Owned by Contractor's Personnel

2.104 The use of privately-owned equipment of contractor's personnel (hardware and software) for processing NR information shall not be permitted.

CIS Users' responsibilities

2.105 CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

Advice

2.106 Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

Audit/inspection

2.107 At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor shall provide evidence of compliance with this SoW Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.

3. Contractor Cyber Incident Management Plan

3.1 The Contractor shall be required to deliver a Cyber Incident Management Plan (CIMP) that is aligned to cyber security controls in line with NATO Security Policy and its supporting directives.

3.2 The Contractor shall create, maintain and operate a formal incident response and forensic capability for protection of NATO Information residing on non-NATO Information Systems. The Contractor shall include the subcontractors and suppliers that perform support work that involves NATO Information.

3.3 The Contractor shall establish an incident-handling capability plan that consists of:

1) incident response policy and plan,

2) procedures for performing incident handling and reporting

3) guidelines for communicating with outside parties regarding incidents

4) incident team structure and staffing model

5) relationships and lines of communication between the incident response team and other groups, both internal and external

6) services the incident response team should provide, and

7) staffing and training the incident response team

3.4 The final Program CIMP shall be in Adobe Acrobat format with a digital signature from the contractor cognizant authority.

3.5 If no approved Program CIMP currently exists between the contractor and NATO, then one must be created and submitted. If an approved Program CIMP already exists and sufficiently satisfies the CIMP requirements for the contract, then no new CIMP delivery is required. In such cases, the Contractor in consultation with the Purchaser shall only submit a Contract Letter to the Contracting Officer stating that all CIMP requirements are satisfied by the existing Program CIMP.

3.6 The Contactor shall report cyber incidents that result in an actual or potentially adverse effect on the Contractor CIS and/or NATO Information residing therein, or on a contractor's ability to deliver on the requirement.

3.7 The Contractor shall report status of the incident-handling capability including plan-of actions for capabilities not at full operational status, and periodic operational status.

3.8 The Contractor shall provide status of a cyber-incident from first identification to closure as described in the CIMP.

3.9 The contractor shall report cyber incidents for all section of the SoW to the Purchaser as described in the NCI Agency Special Provisions Clause, Cyber Incident Reporting.

3.10 The Contractor shall establish and document a digital forensics readiness plan, and upon an incident execute the plan on the Contractor CIS to include the collection, examination, analysis, and reporting.

3.11 The contractor shall use a community-developed, standardized specification language for representing and exchanging information in the broadest possible range for cyber-investigation domains, including forensic science, incident response, and counter terrorism.

3.12 The Contractor forensic team assessment as required shall initiate corrective actions to include securing identified vulnerabilities, improve existing security controls, and provide recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

3.13 Subject to the Purchaser’s consultation with the Contractor’s national cyber defense authority and/or as prescribed in the contractor’s nation’s Memorandum of Understanding (MoU) on Cyber Defence with NATO, the Purchaser reserves the right to examine and audit all records and other evidence sufficient to reflect proper program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of NATO Information. If the Purchaser identifies any

security deficiencies during the audit, the contractor shall implement corrective actions to address the shortfalls identified during these assessments at its own expense within a timeframe agreed with the Purchaser. The Purchaser reserves the right to re-examine and audit evidence of the implemented corrective actions.

ANNEX D Maintenance and support definitions

D.1. Scope

This annex specifies the maintenance levels, the support levels and the relevant activities to be carried on by the relevant stakeholders.

The SOW specifies who is responsible for what, at the various maintenance and support levels.

D.2. Maintenance concept

A maintenance concept is a statement of maintenance considerations, constraints, and strategy for the operational support that governs the maintenance levels and type of maintenance activities to be carried out for the Product[7] under analysis (ref. ASD/AIA SX000i).

A maintenance concept is applicable to both hardware and software, and produces maintenance tasks that will be performed on site, at civil or military maintenance facilities, or at industry (OEM, Contractor) maintenance facilities.

A maintenance concept identifies who-does-what-at-what-level in accordance with the applicable maintenance levels.

The main SOW is required to clearly identify what is the maintenance concept for the relevant project.

D.3. Maintenance Levels (ML)

A ML is the position in an organization where specified levels of maintenance are to be carried out. The ML is characterized by the skill level of the personnel, the facilities and tools provided, the location, etc.

There are four ML to ensure the highest possible availability of the product, from ML1 to ML4.

A. **ML1**: fast and easy replacement of Maintenance Relevant/Significant Items (MRI/MSI) performed on the Product by organizational personnel when a malfunction occurs;
B. **ML2**: exchange of MRI/MSI and/or the replacement of modules, performed on the Product by organizational personnel when a malfunction occurs;
C. **ML3**: repair of subassemblies, modules and MRI/MSI after their replacement at ML1 and ML2. Testing on test-benches or integration tests can be included. This ML can be performed either on Product (e.g. on-site) or at specific repair shops/facilities;
D. **ML4**: All repairs and overhaul activities beyond ML1 to ML3 – e.g.: repair of subassemblies, modules and Line Replaceable Units (LRU) after their replacement at ML1 to ML3; major modifications to improve the design and/or operational activities will be prepared and, if necessary, embodied at this level.

D.4. Hardware maintenance and hardware change

The hardware maintenance is Corrective or Preventive:

D.4.1. Corrective hardware maintenance

[7] I.e. Any capability (or part of), system or equipment (air, sea, land, vehicle, equipment or facilities, civil or military), or service.

Corrective Hardware Maintenance can be:

A. **Deferred**: maintenance carried out to perform a remove and install task of a faulty item not affecting Product operation. It is done in a time slot that does not further impact the operational availability (e.g. during a schedules maintenance downtime period) or on "live" equipment if this is possible (e.g. when active redundancy or hot stand-by are implemented).
B. **Run-to-failure**: maintenance carried out to perform a remove and install task of a faulty item affecting Product operation (critical failure). The task is done as soon as all the resources (skills, tools and spares) are available to minimise the product downtime.

D.4.2. Preventative hardware maintenance

Preventive Hardware Maintenance can be:

A. **On-condition**: maintenance carried out to mitigate degradation and reduce the probability of failure after analysis of Product conditions through defined indicators assessed on a periodic basis.
B. **Scheduled (planned)**: maintenance carried out on a periodic basis (time-related or number-of-occurrences-related).

D.4.3. Hardware maintenance concept

The hardware maintenance concept is based on the modularity of the equipment.

The items to be removed from the product for replacement, to be repaired or to be replaced/refilled for preventative maintenance is defined Maintenance Relevant/Significant Item (MRI/MSI), with the following characteristics:

A. Include those items in the Logistic Support Analysis (LSA) Breakdown Structure (LBS) which are significant for maintenance at the Organisational Level;
B. Include all the candidate items of the spare parts and consumables lists;
C. Are subdivided into the following categories:
    a. LRU;
    b. Insurance Item (II);
    c. Consumable Items;
    d. Attaching Parts.

D.4.3.1. Line Replaceable Unit (LRU)

LRU characteristics are the following:

A. Its failure can be detected and indicated by a Built In Test System (BIT) or by abnormal condition/failure display/alarm, in conjunction with Technical Manuals (TM) and general-purpose test equipment and troubleshooting procedures;
B. It is easily accessed for replacement purposes;
C. It is easy to replace, through the use of a plug-in connector, screwed terminal, nut/bolt fixing or similar connector;
D. It has minimal adjustment/alignment requirements, such as voltage level settings, software/firmware installations/adaptations etc.;
E. Adjustments may be carried out with the BIT or with general-purpose hardware/software tools and test equipment;
F. When only one LRU has failed, its replacement returns the product to full operational status.

LRU are subdivided into the following two categories:

A. **Statistical (LS)**: includes the items subject to faults that occur with a statistical probability (most of them are electronic items) – e.g. Intermediate/Radio Frequency (IF/RF) strips/boards, computers/servers/workstations and theirs components and peripherals, networking equipment (routers, switches), power supplies, electric/electronic components in general;
B. **Limited Life (LL)**: includes the items whose faults are due to ageing (most of them are electromechanical items) – e.g. fans and fan assemblies, Transmit/Receive (T/R) switches, Travelling-Wave Tubes (TWT), rotary joints, slip rings, engines.

D.4.3.2. **Insurance Items (II)**
This category includes those items that have a very low failure rate and whose replacement may be necessary as a consequence of deterioration or fault by accident – e.g. passive elements (attenuators, couplers, circulators, terminations), circuit breakers, patch panels, cables, metallic frames/cabinets/chassis.

D.4.3.3. **Consumables**
Consumable are subdivided into the following three categories:

A. **Technical Consumables (C[T])**: fuses, bulbs, lamps, gaskets, o-rings, Electromagnetic (EMI)/tempest seals, surge protectors, gas dischargers, batteries and, in general, any other item replaced in case of preventive or corrective maintenance on the product;
B. **Not-Technical Consumables (C[NT])**: all Petrol-Oils-Lubricants (POL), adhesive, sealing paste, gas and, in general, any other item replaced in case of preventative or corrective maintenance on the product;
C. **Generic Consumables (C[G])**: ink cartridges, toners, printing paper, print ribbons, generic cleaning material and in general all the materials whose consumption cannot be predicted (e.g. is not associated to any preventative or corrective maintenance on the Product).

D.4.3.4. **Attaching Parts (AP)**
The AP are the items reported in the corrective and preventative maintenance procedures and in the illustrated parts breakdown such as screws, gaskets, nuts, bolts, washers, etc.

D.4.4. **Hardware ML**
The hardware ML are referred to as HL1, HL2, HL3 and HL4.

D.4.4.1. **HL1 – Organizational maintenance**
HL1 is hardware maintenance capable of being carried out:

A. On-site;
B. By relatively low technical skill level personnel performing preventive maintenance and changing LRU and Insurance Items (II) on the basis of diagnostic outputs;
C. Using Built-In-Test (BIT) facilities for start-up and on-line diagnostics;
D. Using commercial Tools and Test Equipment (TTE) – e.g. screwdrivers, multimeters, oscilloscope, adapters;
E. By following the relevant maintenance procedures as per the applicable organizational technical publications.

HL1 typical tasks are: visual inspection, preventative maintenance tasks, manual reconfiguration if necessary, external adjustments, removal and replacement of LRU/II;

HL1 includes:

A. Product failure recovery by the application of simple on-line diagnostics or technician initiated restart of the Product and the use of off-line diagnostics which do not require external test module support;
B. Generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

D.4.4.2. **HL2 – Organizational maintenance**

HL2 is hardware maintenance capable of being carried out:

A. On-site;
B. By higher technical skill level personnel performing preventive maintenance and changing LRU and II on the basis of diagnostic outputs;
C. Using BIT facilities for start-up and on-line diagnostics;
D. Using standard TTE, and Special-To-Type Equipment (STTE) in addition to BIT as a means for on-line and off-line diagnostics;
E. Following the relevant maintenance procedures as per the applicable organizational technical publications.

Where the fault is beyond the capabilities of on-site technical support, HL2 activities are performed by support site personnel, through on-site intervention.

Where remote fault management is not feasible, technicians from the host site will travel to the remote site hand carrying relevant spares to perform maintenance tasks.

HL2 includes generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

D.4.4.3. **HL3 – Intermediate maintenance**

HL3 is hardware maintenance capable of being carried out:

A. At maintenance facilities and through technical support and assistance or on-site intervention by maintenance personnel with skills enabling tasks to be accomplished within the relevant technologies;
B. By higher technical skill level personnel performing:
    a. Repairing, testing and calibrating LRU, Shop Replaceable Units (SRU) and secondary spare parts (SSPs);
    b. On-site investigations and major scheduled servicing/overhaul, detailed inspection, major equipment repair, major equipment modification, complicated adjustments, Product testing;
    c. Failure trend analysis including reporting to relevant Purchaser authorities and Post Design Services (PDS);
C. Using Automatic Test Equipment (ATE), general purpose TTE and STTE, calibration equipment, any applicable support software;
D. Following the relevant maintenance procedures as per the applicable intermediate technical publications.

Where the fault is beyond the capabilities of HL1/2 technical support, HL3 activities are performed by Support Site personnel (through on-site intervention) or by the Contractor, depending on the applicable maintenance concept;

HL3 includes generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

D.4.4.4. **HL4 – Depot maintenance**

HL4 is hardware maintenance capable of being carried out:

A. At maintenance facilities (industry or military, OEMs) and through technical support and assistance or on-site intervention by maintenance personnel with skills enabling tasks to be accomplished within the relevant technologies;
B. Where the fault is beyond the capabilities of HL1/3 technical support, by Contractor's personnel;
C. By using the relevant Technical Data Package (TDP).

It includes generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

D.5. Software maintenance and software change

The software maintenance is a modification for the purposes of software fault removal, adaptation to a new environment, or improvement of performance.

The software maintenance for the purposes of software faults avoidance, identification and/or removal can be:

A. **Corrective/Unscheduled**: it refers to tasks necessitated by actual errors in a software product. If the software product does not meet its requirements, corrective maintenance is performed. It is a reactive modification of a software product performed after a new version is made available (patch/update) to correct the discovered problem(s). This activity is linked to configuration management, change management (Contractor initiated Engineering Change Proposal, ECP), new software release(s) and Product Baseline (PBL) change.
B. **Preventative/Scheduled**: it refers to tasks necessitated for detecting potential errors in a software product or anticipate and avoid potential failures (daily checks, DBs clean up/integrity checks, cache cleaning, rebooting/restarting etc.). The task can lead, if latent failures are discovered, to a modification of a software product after delivery to detect and correct latent faults in the software product before they become effective faults (leading to a deferred corrective action).

The software maintenance for the purposes of adaptation to a new environment, or improvement of performance is a software change that enhances the software product. These changes are those that were not in the original design specifications or in the originally released software and are subject to Purchaser initiated ECP:

A. **Adaptive maintenance**: software maintenance for the purposes of adaptation to a new environment (e.g.: a new environment could be a new type of hardware or a new operating system on which the software is to be run). Adaptive refers to a change necessary to accommodate a changing environment. Adaptive changes include changes to implement new Product interface requirements, new Product requirements, or new hardware requirements. This is a modification of a software product performed after delivery to keep a software product usable in a changed or changing environment.
B. **Perfective maintenance**: software maintenance performed to improve the performance, maintainability, or other attributes of a computer program (e.g.: maintenance that adds new required functions is often referred to as enhancement). Perfective refers to a change that improves the software product's performance. A perfective change might entail providing new functionality improvements for users or reverse engineering to create maintenance documentation that did not exist previously

or to change existing documentation. This is a modification of a software product after delivery to improve performance or maintainability.

D.5.1. Software maintenance levels

The software maintenance levels are referred to as SL1, SL2 SL3 and SL4.

D.5.1.1. SL1 – Organizational maintenance

SL1 is software maintenance capable of being carried out with the same characteristics highlighted for HL1.

SL1 are those functions/tasks in support of the on-site software that are within the capabilities of site maintenance personnel. This includes software failure recovery by the application of simple diagnostics, or site maintenance personnel initiated restart.

D.5.1.2. SL2 – Organizational maintenance

SL2 is software maintenance capable of being carried out with the same characteristics highlighted for HL2 – e.g. software settings, simple software customizations (per site/instance), software reloading/installation with automated or detailed procedures reported in the technical manuals, execution of scripts, management of users/profiles. SL2 are those functions/tasks in support of the on-site software that are within the capabilities of a system administrator.

D.5.1.3. SL3 – Intermediate maintenance

SL3 is software maintenance capable of being carried out with the same characteristics highlighted for HL3 – e.g. software/firmware fine tuning (per site/instance), e.g. software/firmware bugs recording and reporting, software/firmware troubleshooting including operating systems. SL3 (on-site intervention) comprises those functions/tasks in support of the on-site software that require specialist intervention (software system architects, software programmers, experienced system administrators, network specialists). The tasks can be performed either by software personnel visiting the site or by remote diagnostics if enabled by the Product.

D.5.1.4. SL4 – Depot maintenance

SL4 is software maintenance capable of being carried out with the same characteristics highlighted for HL4 – e.g. software/firmware debugging, re-coding and testing (both in simulated and emulated environments), software/firmware patches creation and deployment. The tasks can be performed by software engineers in properly configured environments (software development and testing facilities) under strict configuration control.

D.6. Support concept

A support concept is a definition of the support objectives (scenarios) in relation with maintenance levels, maintenance support and their interrelationships.

This is peculiar for IT/software-intensive and IT/software-driven Products and is implemented in conjunction and coordination with the maintenance concept.

D.6.1. Support levels

There are four support levels:

A. **SUPL1**: first level support – on-site, non-specialised;
B. **SUPL2**: second level support – centralised;
C. **SUPL3**: third level support – centralised;
D. **SUPL4**: fourth level support – OEM/Vendor)

D.6.1.1. SUPL1 – On-site, non-specialised

It consists of simple routine administration and activities. This level is user facing and is the first line of technical support. A single point of contact inside the central Service Desk is

provided to Customers for the implemented services. The Service Desk will log, categorise prioritise, diagnose and resolve incidents within the boundaries of their training and permissions. The pertinent Support Units (CSUs) carry out this level of support, in coordination with the centralised Service Desk.

The SUPL1 process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket, TT), performs an initial assessment and distributes it to the predefined stakeholders to solve it.

D.6.1.2. **SUPL2 – Centralized**

It provides escalated technical support to incident investigation and diagnosis. This level delivers advanced expertise to process services related to centralized system operations, fault isolation, system administration, management of maintenance services, system configuration, including reconfiguration of data sources and data connectivity to restore operations, assistance to first level and on-site support. This level performs end-to-end service monitoring and takes actions to resolve the incident and recover the services impacted.

The SUPL2 process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

The Problem Management process receives the TT from the Service Desk and performs the following tasks:

A. (Re-)evaluation of TT category, criticality and priority;
B. Identification of the root cause of the issue – e.g. by issue replication testing;
C. Identification of workarounds;
D. Identification and initial planning of possible short, medium and long-term solutions (e.g. Workarounds, Patches, or new Baseline or CI Releases);
E. Create Problem Analysis Report and Change Request (CR), including schedule of implementation, and synchronisation with the baseline maintenance process;
F. Presentation of the Problem Analysis Report and CR to the Change Advisory Board (CAB) for approval;
G. Monitor and control the approved CR during implementation;
H. Trigger SUPL3 and/or ML3 process to implement the CR;
I. Perform the post- CR implementation review.

D.6.1.3. **SUPL3 – Centralized**

It consists of central service management, central problem isolation and resolution, system-level maintenance, local repairs or spares provision, and management of deficiencies and warranty cases, beyond the capability of the second level support.

The SUPL3 process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

The Deployment and Release Management process receives the approved Change Request from the SUPL2 and performs the following tasks:

A. Release of the solution (release unit/record);
B. Development of the solution (e.g. new configuration item fix, repair, replacement, patch, or release);
C. Testing of the solution (e.g. regression testing, issue/deficiency replication testing);
D. Update of baseline content and status;

E. Delivery and deployment of the solution.

D.6.1.4. **SUPL4 – OEM/Vendor**

It consists of off-site factory/Vendor problem resolution and maintenance, beyond the capability of SUPL3.

ACRONYMS

Abbreviation/Acronym	Meaning
A2SL	Agency Authorized Software List
ABD	As Built Drawings
ABL	Allocated Baseline
ACMP	Allied ConfigurationManagement Publications
ACO	Allied Command Operations
AD	Active Directory
AES	Advanced Encryption Standard
AI	Agency Instruction
AIL	Action Items List
ANSI	American National Standards Institute
AP	Attaching Part
AQAP	Allied Quality Assurance Publication
ASCII	American Standard Code for Information Interchange
ATE	Automatic Test Equipment
BIOS	Basic Input/Output System
BIT	Built In Test System
BPS	Boundary Protection Services
CA	Certificate Authority
CAW	Contract Award
CCB	Change Control Board
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CGI	Computer-generated imagery
CI	Configuration Item
CIM	Common information model
CIS	Communication and Information Systems
CM	Configuration Management
CM	Corrective Maintenance
CMDB	Configuration Management Database
CMP	ConfigurationManagement Plan
CoC	Cenrtificate of Conformity
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CQAR	Contractor Quality Assurance Representative
CR	Change Request
CRL	Certicate Revocation List
CSA	Configuration Status Accounting
CSC	Computer Software Component
CSCI	Computer Software Configuration Item
CSRF	Cross-Site Request Forgery attacks

Abbreviation/Acronym	Meaning
CSS	Cross-Site Scripting (input validation context)
CSS	(AccessData) Child Site Server
DB	Database
DDP	Delivery Duty Paid
DI	Developmental Item
DNS	Domain Name Server
DoC	Declaration of Conformity
EAPC	Euro-Atlantic Partnership Council
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECO	Engineering Change Order
ECP	Engineering Change Proposal
EDC	Effective Data of Contract
EMI	Electromagnetic Interference
EOL	End Of Life
EOS	End Of Support
ePO	Trellix ePolicy Orchestrator
ERM	Event Review Meeting
ESD	Electro-Sensitive Device
ETP	Event Test Plan
FBL	Functional Baseline
FC	Fiber Channel
FIN	Finland
FIPS	Federal Information Processing Standard
FOC	Final Operating Capability
FSA	Final System Acceptance
FW	Firewall
FW	Firmware
GCM	Galois Counter Mode
GQA	Government Quality Assurance
GUI	Graphical User Interface
HA	High Availability
HL	Hardware Level
HLD	High Level Design
HPS	Hosting Platform Services
HQ	HeadQuarters
HSTS	HTTP Strict Transport Security
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
HWCI	Hardware Configuration Item
HWP	Hardware Part

Abbreviation/Acronym	Meaning
IEC	International Electrotecnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force (Open Standards Organization)
IETPs	Interactive Electronica Technical Publications
IEV	International Electrotechnical Vocabulary
II	Insurance Item
IMP	Integrated Management Plan
IMS	Integrted Maangement Schedule
INCOTERMS	International Chamber of Commerce Terms
INFOSEC	Information Security
IP	Internet Protocol
IPS	Integrated Product Support
IPSP	Integrated Product Support Plan
ISA	Instruction Set Architecture
ISAF	International Security Assistance Force
ISD	Items Setting Document
ISO	Intenration Standardization Organization
IT	Information Technology
ITS	Issue Tracking System
IVVQ	Independent Verification, Validation and Quality
KEDB	Known Error DataBase
LAPS	Local Administrator Password Solution
LBS	Logistic Breakdown Structure
LDAP	Lightweight Directory Access Protocol Server
LDAPS	Lightweight Directory Access Protocol Server Secure
LLD	Low Level Design
LRU	Line Replaceable Unit
LS	Line Replaceable Unit-statistical
LSA	Logistic Support Analysis
MAC	Media Access Control (address)
MFA	Multi-Factor Authentication
MOQ	Minimum Order Quantity
MRI	Maintenance Relevant Item
MS	Milestone
MSI	Maintenance Significant Item
MSR	Monhtly Status Report
MTBCF	Mean Time Between Critical Failures
MTBF	Mean Time Between Failures
MTP	Master Test Plan
MTTR	Mean Time to Repair
MTTRS	Mean Time to Restore System
NAC	Network Access Control

Abbreviation/Acronym	Meaning
NAF	NATO Architecture Framework
NAT	Network Address Translation
NATO	North Atlantic Treaty Organisation
NCAGE	NATO Commercial and Government Entity code
NCIA	NATO Communications and Information Agency
NCSC	NATO Cyber Security Centre
NHA	Next Higher Assembly
NHQ	NATO Headquarters
NPKI	NATO Public Key Infrastructure
NQAR	NATO Quality Assurance Representative
NR	NATO Restricted
NS	NATO Secret
NSAB	NATO Security Accreditation Board
NSN	NATO Stock Number
NTP	Network Time Protocol
O&M	Operation And Maintenance
OATM	Operational Acceptance Traceability Matrix
OEM	Original Equipment Manufacturer
OJT	On the Job Training
OS	Operating System
PAT	Port Address Translation
PBL	Product Baseline
PBS	Product Breakdown Structure
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PDS	Post Design Services
PFD	Product Flow Diagram
PFE	Purchaser Furnished Equipment
PHST	Packaging, Handling, Storage and Transportation
PILAR	Risk Assessment Methodology
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PLM	Product Lifecycle Management
PLT	Procurement Lead Time
PM	Project Manager
PM	Preventative Maintenance
PMO	Project Management Office
PMP	Project Management Plan
POC	Point of Contact
PRM	Project Review Meeting
PSA	Preliminary System Acceptance
PSC	Personal Security Clearance
QA	Quality Assuarance

Abbreviation/Acronym	Meaning
QAP	Quality Assurance Plan
QC	Quality Control
QEI	Quantity per End Item
QMS	Quality Management System
RADIUS	Remote Access Dial-In User Service
RBAC	Role Based Access Control
RBD	Reliability Block Diagrams
RCT	Repair Cycle Time
REF	Reference
RFID	Radio Frequency Identification
RFC	Request For Concession
RFC	Request for Change
RHEL	Red Hat Enterprise Linux
RMA	Reliability, Maintainability, Avaialbility
RSA	Rivest-Shamir-Adleman
RTM	Requirements Traceability Matrix
SA	Security Accreditation
SAA	Security Accreditation Authority
SAP	Security Accreditation Plan
SAT	System Acceptance Test
SCCM	System Center Configuration Manager
SCOM	System Center Operations Manager Server
SDS	System Design Specification
SHA	Secure Hash Algorithm
SHAPE	Supreme Headquarters Allied Powers Europe
SIEM	Security Incident and Event Manager
SIP	Site Implementation Plan
SIS	Site Installation Specification
SIT	System Integration Test
SIVP	Security Implementation Verification Procedure
SMC	System monitoring and configuration
SME	Subject Matter Expert
SMR	Source, Maintenance, Recoverability
SNMP	Simple Network Management Protocol
SOW	Statement of Work
SPOC	Singe Point of Contact
SQL	Structured Query Language
SRA	Security Risk Assessment
SRD	Security Related Documentation
SRM	Security Risk Management
SRN	Software Release Note
SRR	System Requirements Review
SRS	System Requirements Specification

Abbreviation/Acronym	Meaning
SRU	Shop Replaceable Units
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On
SSRS	System Security Requirements Statement
SSS	Scope of Supply and Services
STANAG	Standardization Agreement
STS	HTTP Strict Transport Security (HSTS)" (previously called STS)
STVP	Security Test & Verification Plan
STVR	Security Test & Verification Report
SW	Software
SWDL	Software Delivery List
TACACS	Terminal Access Controller Access Control System
TAT	Turn Around Time
TC	Technical Centre
TCP	Transmission Control Protocol
TD	Test Director
TDP	Technical Data Package
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
TLS	Transport Layer Security
TM	Technical Manuals
TNA	Training Needs Analysis
TP	Training Plan
TP-POAP	Training Plan Plan An A Page
TRNP	Training Plan
TRR	Test Readiness Review
TT	Trouble Ticket
TTE	Tools and Test Equipment
TtT	Train the Trainer
TVV	Test , Verification, Validation and Acceptance
UAT	User Acceptance Test
UDID	Unique device ID
UEFI	Unified Extensible Firmware Interface
UOM	Unit of Measure
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	United States (of America)
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VCRM	Verification Cross Reference Matrix

Abbreviation/Acronym	Meaning
VEEAM	Veeam Software (US-based information technology company)
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Networks
VRF	Virtual routing and forwarding
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross Site Scripting

NPKI MITIGATION (NPKI-M) High Level Design for Reference and Production Infrastructure in Mons and NATO HQ

Ver. 1.2

Dated : 20 July 2023

TABLE OF CONTENTS

List of Figures

List of Tables

1 INTRODUCTION

This document contains the high-level design (HLD) for the Reference and Production environments for the NATO PKI (NPKI) Mitigation system (hereinafter identified as NPKI-M).

Additional details will be added to this document once information becomes available and as the implementation commences. Accordingly, this document will mature over time and will become the low-level design document for the NPKI-M.

An important aspect of NPKI-M is High Availability (HA). How the HA should be achieved, is not spelled out yet in this document. It is expected from the Contractor to fully design and implement HA in further iterations of this HLD and the implementation documents.

1.1 Scope

As stated in 5 Reference: RFQ-CO-115518-NPKI-M NPKI MITIGATION (NPKI-M) HOSTING PLATFORM SERVICES BOOK II - PART IV STATEMENT OF WORK (SOW):

A dedicated core infrastructure shall be provided to support the NPKI-M. The infrastructure shall be provided in Mons datacentre and NATO HQ datacentre. The HLD consists of 8 installations; 4 Production and 4 Reference. Production installations are split between the two datacentres. Reference installations are to be installed in the Mons Datacentre.

Each security domain is responsible for different levels of classified information:

- Processing up to and including NR data in the NR/NU domain.
- Processing up to and including NS data in the NS domain.

Unless specifically stated otherwise, design information applies to both security domains for reference and production infrastructure.

In total, the Hosting Platform Environment is as follows:

- Both Mons Datacenter and NATO HQ Datacenter: 1 production infrastructure
- Mons: 2 separate Reference infrastructure
- All infrastructures have a separated physical implementation.

The NPKI-M infrastructure is fully isolated from other networks except for explicit external connections described in section 3.2, Figure 4, and Figure 5.

The Purchaser delivers hardware (excluding cabling not already included within the rack infrastructure). Therefore, the activities of the Contractor are specific to establishing the Hosting Platform Services, required for NPKI-M. Hardware is listed within section 4.1 Purchaser Furnished Equipment (PFE).

This HLD document does not duplicate the requirements stated in the NPKI-M HPS SRS, but provides the technical implementations.

2 HIGH LEVEL DESIGN

This chapter explains the high level design of the solution. Attention is paid to the description of the solution, the physical implementation and the logical implementation of NPKI-M.

2.1 Description of Solution

The NPKI-M project will deliver a public key infrastructure system covering:

- Two datacenters (DC) in Belgium; NATO Headquarter (HQ) Brussels and SHAPE Mons for production environments;
- Two separate production infrastructures to cover NATO Secret (NS) and NATO Unclassified (NU) /NATO Restricted (NR) security domains in each datacenter (4 production installations);
- Each installation consists of a layered Infrastructure with firewalls separating the Front End PKI services from multiple back end PKI service zones and a second layer of firewalls separating front end PKI services from external systems;
- Two reference environments fully replicating the functionality and installations of the two production infrastructures and two security domains; to be located in Mons. (4 Reference installations).

This work package provides for the following elements to be installed within each installation:

- Racking and cabling of all equipment required to implement the NPKI-M system;
- Provision of cabling where not already available in the rack;
- Establishment of Virtual LANs (VLAN) ;
- Build and configure of Hosting Platform services consisting of two physically separate VMWare infrastructures per installation;
- Establishing High availability (HA) for all components between datacenters;
- Installation and configuration of two HA PostgreSQL services and configuration of automated failure detection and HA failover and recovery (2 sets of 2 PostgreSQL servers per installation);
- Installation and configuration of RedHat Enterprise Linux (RHEL) 389 Directory Servers and configuration of automated failure detection and HA failover and recovery for each of the two VMware infrastructures per installation;
- Installation and configuration of infrastructure services, proxies and other applications covering the entire installation;
- Establishment of all virtual machines described in this HLD;
- Installation of specific set of network interconnections which will provide services across the NATO enterprise;
- Validating the firewall rulesets for required communications between all VLANs, Operating systems, and applications identified in the NPKI-M HPS SOW and HLD.

2.1.1 Description of Zones

Each installation consists of two physically separated virtualization infrastructures providing the following services.

1. Core PKI VMware infrastructure consisting of the following virtualized zones:
    - Management, Control, and Production zones (Core Zones);
    - Physical Hardware Security Module (HSM) zone;
    - Physical Out of Band (OOB) management switch for the Management Zone.
2. Front End services consisting of the following virtual domains:
    - Externally accessible Front End service zone;
    - Second Externally accessible Front End (limited) NU services zone. This zone is not applicable to the NS security domain;
    - Connection to Core Management zone, via the OOB switch.

2.2 Logical HLD

Figure 1 provides the high level design concept. Two VMware infrastructures are depicted for each of the Mons and Brussels datacentres each containing the Front end and Core NPKI-M zones and firewalls. The NATO Cyber Security Center (NCSC) Tier-2 infrastructure providing external infrastructure services are shown at the bottom.

Figure 2 illustrates more details for the logical design of two NPKI-M installations (Mons and NATO HQ, Brussels) within a single security domain. The description given in this figure illustrates the NR/NU implementation. Figure 2 shows the firewall separation of zones and the basic VLANs separating them. Each zone provides services. The Front end zones provide services to external entities.

The NPKI-M infrastructure is duplicated in two datacenters to provide a high availability infrastructure. The environment is divided into a Front End and Core zones each with their own dedicated VMware infrastructures. Separation between zones, networks, and systems is enforced via VLANs and Firewalls. The VLAN Separation including physical firewall segmentation provides a North - South layered approach to protect NPKI-M services.

The North-South physical interconnection includes dedicated firewalls and a VMWare cluster for the DMZ/Front End service (and a separate NU Front End service for the NR/NU Domain in addition to the NR Front End.) A second set of firewalls and VMWare cluster supports the Management, Production, and Core zones.

Interconnectivity between the two datacentres is provided for by the existing high speed Data Centre Interconnect (DCI).[1] Front end firewalls for both NPKI-M sites are configured as a GEO Cluster to maximize overall system availability across the two sites. These firewalls are dedicated for NPKI-M.

The two physically separated VMWare infrastructures within an installation are managed by the same vCenter Service. Within vCenter, there is a logical separation between the VMware infrastructures.

All exposed interfaces (Front End services) are housed within a dedicated VMware infrastructure implementing DMZs for inbound traffic. The DMZs are visualized in Figure 6. There are separate virtual Front End services and VLANs for NU and NR traffic.

RHEL HA Proxy and keep alive provides layer-2 high availability leveraging Operating System (OS) based Virtual Router Redundancy Protocol (VRRP). The network switching infrastructure provides additional layer-2 high availability leveraging Virtual Router Redundancy Protocol (VRRP) and a contiguous layer-2 stretched subnet across DCs.

For additional East – West security between sites, VPN tunnels will be implemented for sensitive PKI data in each Zone. This is visualised with red lines in Figure 2. The figure and configuration for the NS-domain is largely similar to the NR/NU, but only includes a single Front End.

[1] This is delivered via NCI Coloured Cloud.

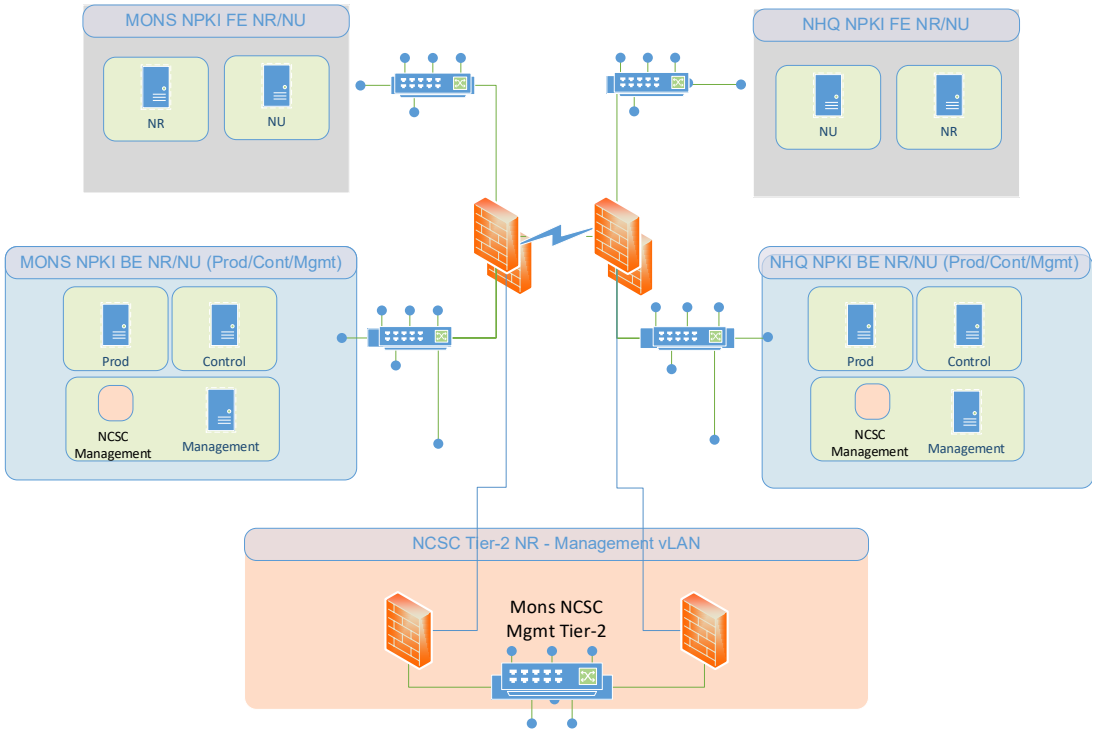

Figure 1- High level design concept for NPKI-M NUNR

2.2.1 Management Zone

The management zone, protected by Purchaser's Furnished Equipment (PFE) firewalls, shall be created, connected to the OOB switch, and extended to NCSC INFRA and NHQ Communications and Information Systems (CIS) Support Unit (CSU) locations for dedicated administration terminals be used for the isolated management of the NPKI-M system. NPKI installations in both datacenters shall be connected to form a cross site management capability. PFE Management stations shall be provided, configured, and connected to the management zone. The virtual machines identified in 4.2 shall be deployed to support the infrastructure services as described in section 3.5 and applications as described in 3.8.3. These services shall be deployed and configured by the contractor and connected to the appropriate PFE Back end service.

2.2.2 Control and Production Zones

The Control and Production zones, protected by PFE firewalls, shall be created. The virtual machines identified in 4.2 shall be deployed to support the infrastructure services as described in section 3.5 which shall be deployed and configured by the contractor. NPKI installations in both datacenters shall be connected to form a cross site management capability. Applications described in 3.8 shall be deployed and configured to provide a high availability service across datacenters.

2.2.3 Front End Zones

The Front end zones, protected by PFE Front end firewalls, shall be created. Within the NS security domain, an NS Front End zone shall be created. Within the NUNR security domain, separate NU and NR front end zones shall be created. The virtual machines identified in 4.2 shall be deployed to support the infrastructure services as described in section 3.5 which shall be deployed and configured. NPKI installations in both datacenters shall be connected to form a cross site. Applications described in section 3.8 shall be deployed and configured to provide a high availability service across datacenters.

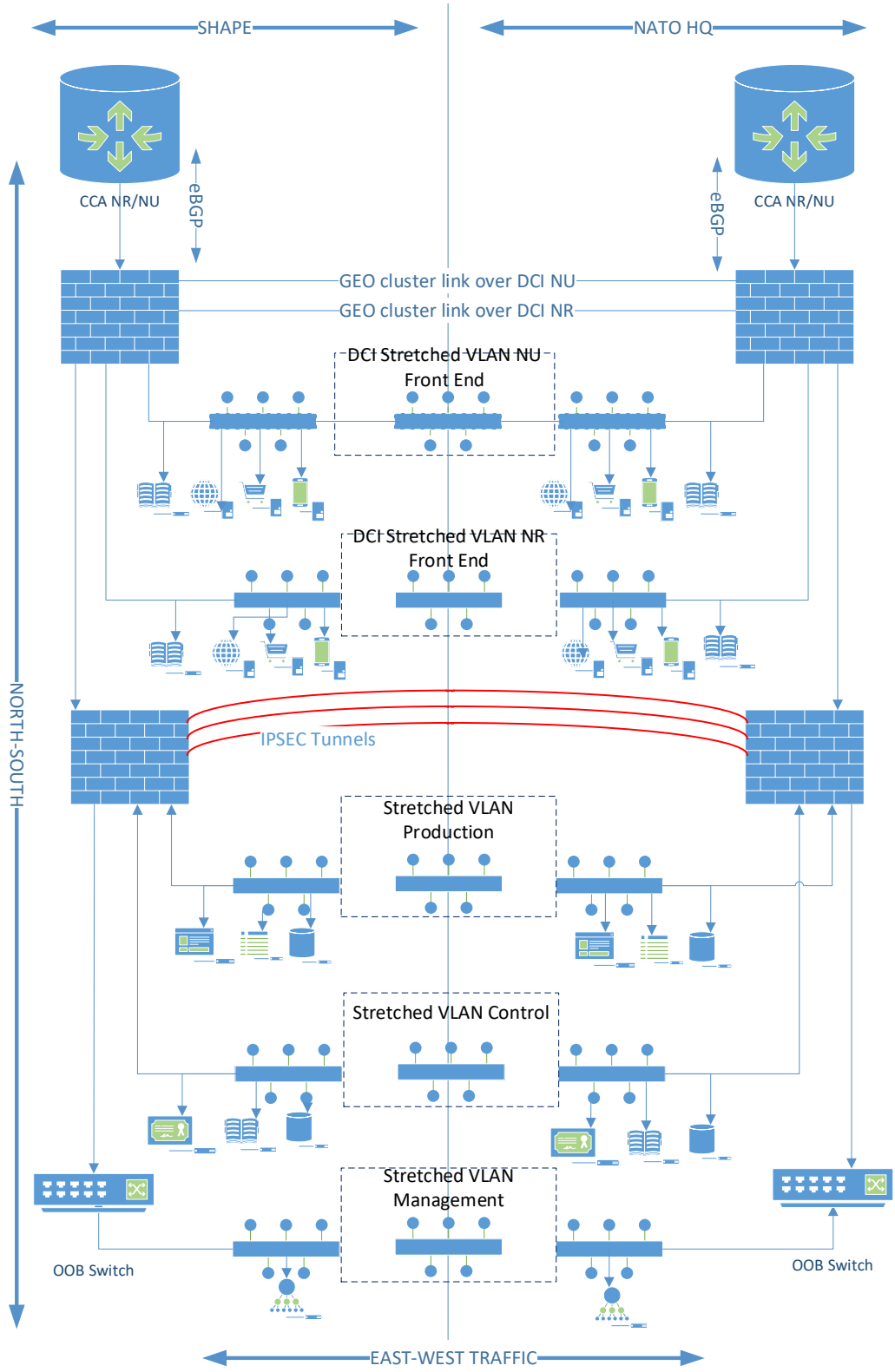

Figure 2 - High Level Diagram showing North-South and East-West traffic across the NPKI-M zones

2.3 Physical Design

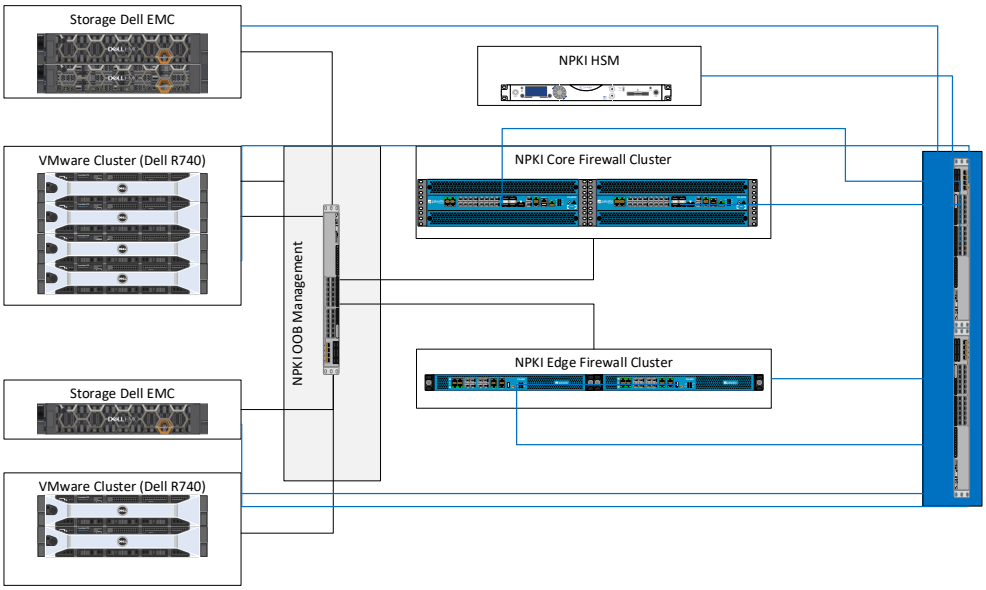

Figure 3 High Level Physical Design per installation

Figure 3 provides the physical design of a single installation, single security-domain, in a single datacentre, and illustrates the implementation of the logical diagram in Figure 2. There are a total of 4 production installations and 4 Reference installations. Reference nodes will have reduced Storage Area Network (SAN) and compute resources due to their smaller infrastructure needs. Redundancy shall be in place and there shall be no single point of failure of any HW, SW and networking.

- The NPKI OOB Management switch is connected to the management port of all physical infrastructure components, including firewalls, switches, the Storage and VMware Clusters, in both Front End and core zones.
- Both domains have a VMware Cluster and Storage respectively.
- A combination of switches, vlans, and firewalls provide segregation for the following physical core components:
    - HSMs
    - Core switch
    - Core Storage SAN
    - Core VMware Cluster (Compute)
    - Core Firewall Cluster
- A separate combination of switches, VLANs, and firewalls provide segregation for the following physical Front End components:
    - Core switch Front End firewall
    - Front End Storage SAN
    - Front End VMware Cluster (Compute)

3 IMPLEMENTATION/CONFIGURATION

3.1 Naming convention

The naming of all infrastructure and application components, follow the NCIA SOP 06.03.01 naming convention and utilizes the following unique descriptors: <domain><owner><host type><index>

3.2 External Connections

NPKI-M will be a self-contained infrastructure. However, there will be interconnections to other networks, via the Front end and Management networks:

- NPKI will provide PKI services for the NATO Enterprise and other NPKI consumers through the NPKI-M Front end interfaces.
- NPKI will feed Communication and Information Systems (CIS) security information to NCSC Tier 2 services,
- Some management components are not hosted within the NPKI-M infrastructure and will be managed from NCSC Tier-2 Management components hosted within the NCSC Tier 2 Management Network are detailed in section 1.1 and visualised in Figure 6.
- Time Synchronization for NTP is detailed in section 3.5.4.
- Active Directory (AD) and DNS Services are subordinate to their parent infrastructure hosted in NCSC Tier 2,
- Administrator accounts will be managed via the NCSC Tier 2 Active Directory Servers.

The external interconnections shown in Figure 4 are specific to the NS installation, however they are indicative of both infrastructures. External interconnections for the low side network will also include mobile device management, and Front End services will be segregated between NU and NR security classifications, with dedicated front ends for each of NU and NR. Firewall (Palo Alto) configuration information will be provided by the Purchaser after the contract award.

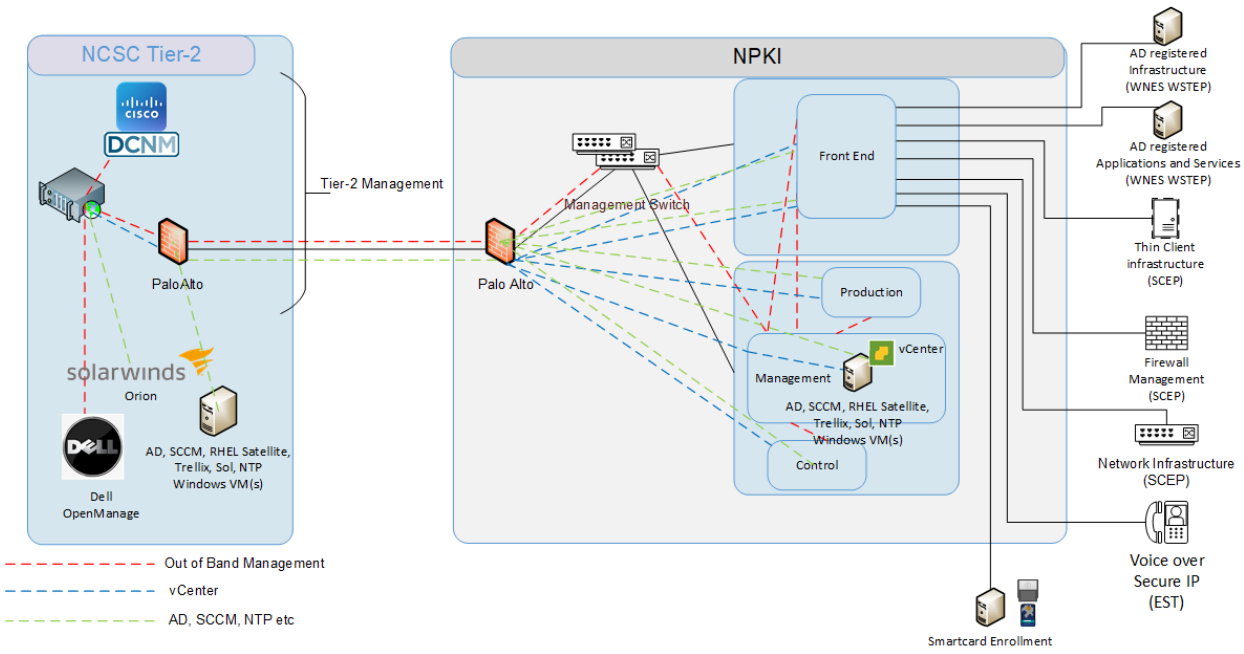

Figure 4 External Registration Interfaces from NPKI-M

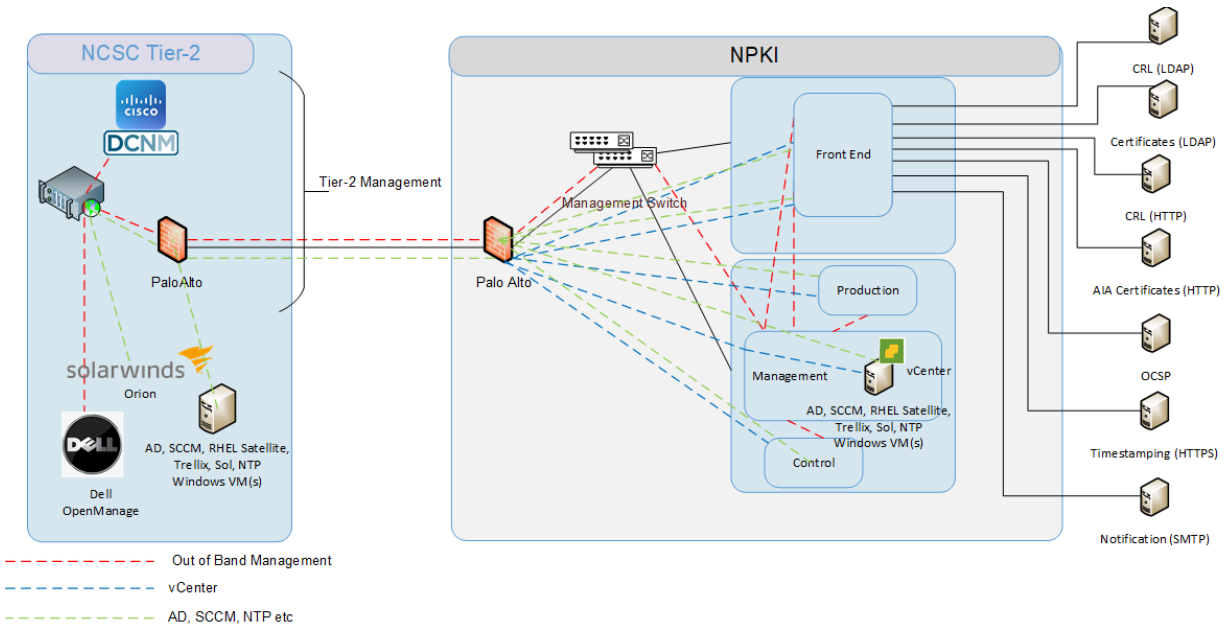

Figure 5 External Validation, Notification, and Timestamp Interfaces from NPKI-M

3.3 Network Services

Network services are provided through a combination of core switches and OOB switches. Core switches are centrally managed by Cisco DCNM (Datacentre Network Manager), which is as a virtual component installed on the VMware environment as a virtual appliance.

3.3.1 Core Switches

The NPKI-M services will be connected via the redundant core switches with redundant IP connections for all devices. The core switches will implement all VLANS provided in this design. Any VLAN omissions in the HLD will be implemented and documented in the low level design from the contractor. All VLANS shall be terminated on either the Core or Front end firewalls.

3.3.2 Out of Band Switches

Out of band switches provide network management interface connectivity with the Management Zone and management machines.

3.3.3 Virtual Local Area Networks (VLANs)

All VLANs shall be terminated on either the Core or Front end firewalls.

Table 1 defines the network Services VLANs used within NUNR NPKI-M. Table 2 defines the Hosting Services VLANs used within NUNR NPKI-M. Table 3 defines the Infrastructure Services VLANs used within NUNR NPKI-M, which defines the PKI internal Services VLANs used within NUNR NPKI-M. For each of these NR and RR VLANS there shall be defined the equivalent VLANs for the NS and RS environments. The NS and Reference Secret (RS) environments do not have NU VLANS. VLAN specific names will provided after the contract award.

Service	Network Description
Network Services	OOB Core Management NETWORK SHAPE production
	OOB Core Management NETWORK HQ production
	Front End NETWORK SHAPE production
	Front End NETWORK HQ production
	Front End NETWORK SHAPE NU production
	Front End NETWORK HQ NU production
	HSM NETWORK SHAPE production
	HSM NETWORK HQ production
	PKI Prod Zone HQ SHAPE Production
	PKI Prod Zone HQ Production
	PKI Control Zone HQ SHAPE Production
	PKI Control Zone HQ Production
	OOB Core NETWORK SHAPE reference
	OOB Core NETWORK HQ reference
	Front End NETWORK SHAPE reference
	Front End NETWORK HQ reference
	Front End NETWORK SHAPE NU reference
	Front End NETWORK HQ NU reference
	HSM NETWORK SHAPE reference
	HSM NETWORK HQ reference
	PKI Prod Zone HQ SHAPE reference
	PKI Prod Zone HQ reference
	PKI Control Zone HQ SHAPE reference
	PKI Control Zone HQ reference

Table 1 – Network Services VLANs within NPKI-M (NUNR)

Service	Network Description
Hosting Services	VMware Management
	VMware Vmotion
	Core Storage iSCSI SHAPE
	Core Storage iSCSI HQ
	Core ESXI Cluster SHAPE
	Core ESXI Cluster HQ
	Core VMware Fault Tolerance
	Front End Storage iSCSI
	Front End Storage iSCSI
	Front End ESXI Cluster
	Front End ESXI Cluster
	Front End VMware Fault Tolerance
	Core Storage VEEAM Replication
	Front End Storage VEEAM Replication

	VMware Management REFERENCE
	VMware Vmotion REFERENCE
	Core Storage iSCSI SHAPE REFERENCE
	Core Storage iSCSI HQ REFERENCE
	Core ESXI Cluster SHAPE REFERENCE
	Core ESXI Cluster HQ REFERENCE
	Core VMware Fault Tolerance REFERENCE
	Front End Storage iSCSI SHAPE REFERENCE
	Front End Storage iSCSI HQ REFERENCE
	Front End ESXI Cluster SHAPE REFERENCE
	Front End ESXI Cluster HQ REFERENCE
	Front End VMware Fault Tolerance REFERENCE
	Core Storage VEEAM Replication REFERENCE
	Front End Storage VEEAM Replication REFERENCE

Table 2 – Hosting Services VLANs within NPKI-M (NUNR)

Service	*Network Description*
Infrastructure Services	Identity Servers -Production
	Admin Jump Boxes - Production
	Identity Servers - REFERENCE
	Admin Jump Boxes - REFERENCE
	DELL IDRAC Management Production
	DeLL IDRAC Management Reference
	Solarwinds Production
	Solarwinds Reference
	EPO Production
	EPO Reference

Table 3 – Infrastructure Services VLANs within NPKI-M (NUNR)

3.3.3.1 IP addresses Allocation

NPKI-M will be allocated dedicated IP address spaces. This information will be provided by the Purchaser during the project implementation.

3.4 Firewalls

Firewall rules will be managed by the Purchaser. The Contractor needs to ensure that the rules are sufficient to meet their interconnection requirements.

3.4.1 Front End firewall

A Palo Alto firewall cluster will be configured as a perimeter firewall for NPKI-M.

Hostname	Management IP	Comment
TBD1	TBD	Firewall node 1
TBD2	TBD	Firewall node 2

Table 4 – Firewall Host Information

3.4.2 Core Firewall

A Palo Alto firewall cluster will be configured that serves as a core firewall for NPKI-M.

Hostname	Management IP	Comment
TBD3	TBD	Firewall node 3
TBD4	TBD	Firewall node 4

Table 5 – Firewall Host Information

3.4.3 Firewall Zones

Rulesets are to be further reviewed and updated based on the LLD development and information still required from the NPKI-M application owners.

3.4.4 Firewall Ruleset (VLAN Connectivity)

Tables regarding firewall rulesets will be provided by the Purchaser after contract award.

3.4.5 Firewall and IPSec VPN Management

All the NPKI firewalls will utilize a dedicated OOB interface for all management activities. This interface allows both SSH and HTTPS access to the device for configuration and management, separate from the data plane. Authentication will be performed via an external RADIUS server. IPSec VPN capability is integrated within the firewalls installed in each NPKI-M Rack at NHQ and SHAPE to provide NATO approved IPSec Tunnel access for the stretched VLAN traffic flows between datacenters for Front End, Production, Control, and Management zones within NPKI-M.

The following AD Security groups shall be created for administrators and operators roles and individual user accounts will be added to these groups:

- TBD-Admin
- TBD-Operator
- TBD-Admin
- TBD-Operator

3.5 Infrastructure Services

This section deals with the infrastructure services, which are relevant for NPKI-M. Some of the services will be managed by other parties. NCSC Tier-2 will provide several central management services, for infrastructure components of the NPKI-M.

The dedicated core infrastructure services shall be managed by an identified limited subset of NCSC Infrastructure administration staff with support from NISC and CSU staff where domain specific skills are required. These components will therefore be managed from NCSC tier-2. Where possible, satellite, gateway or relay servers will be used as an intermediary between NCSC Tier-2 and the NPKI-M infrastructure. This needs to be worked out in further iterations of this document. Figure 6 and Figure 7 provide an overview of the infrastructure services to be provided for NPKI-M.

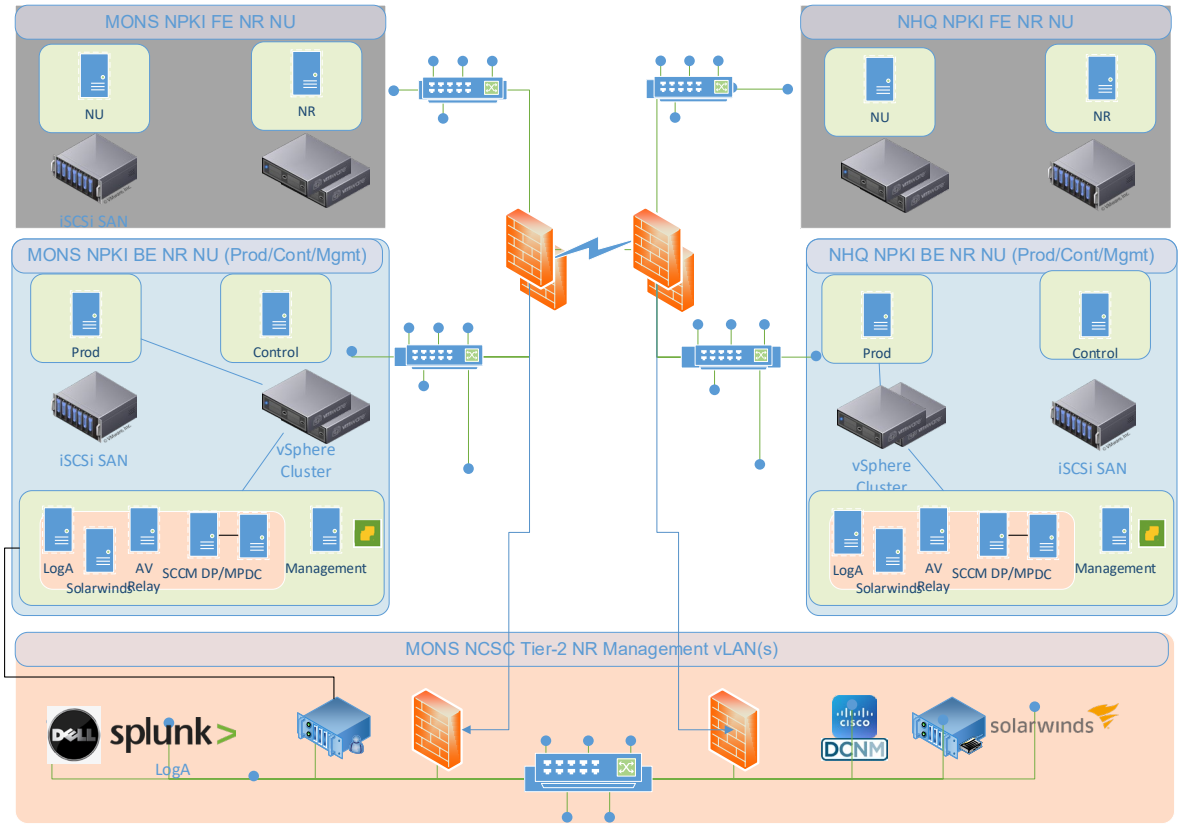

Figure 6 Logical Infrastructure Design NUNR

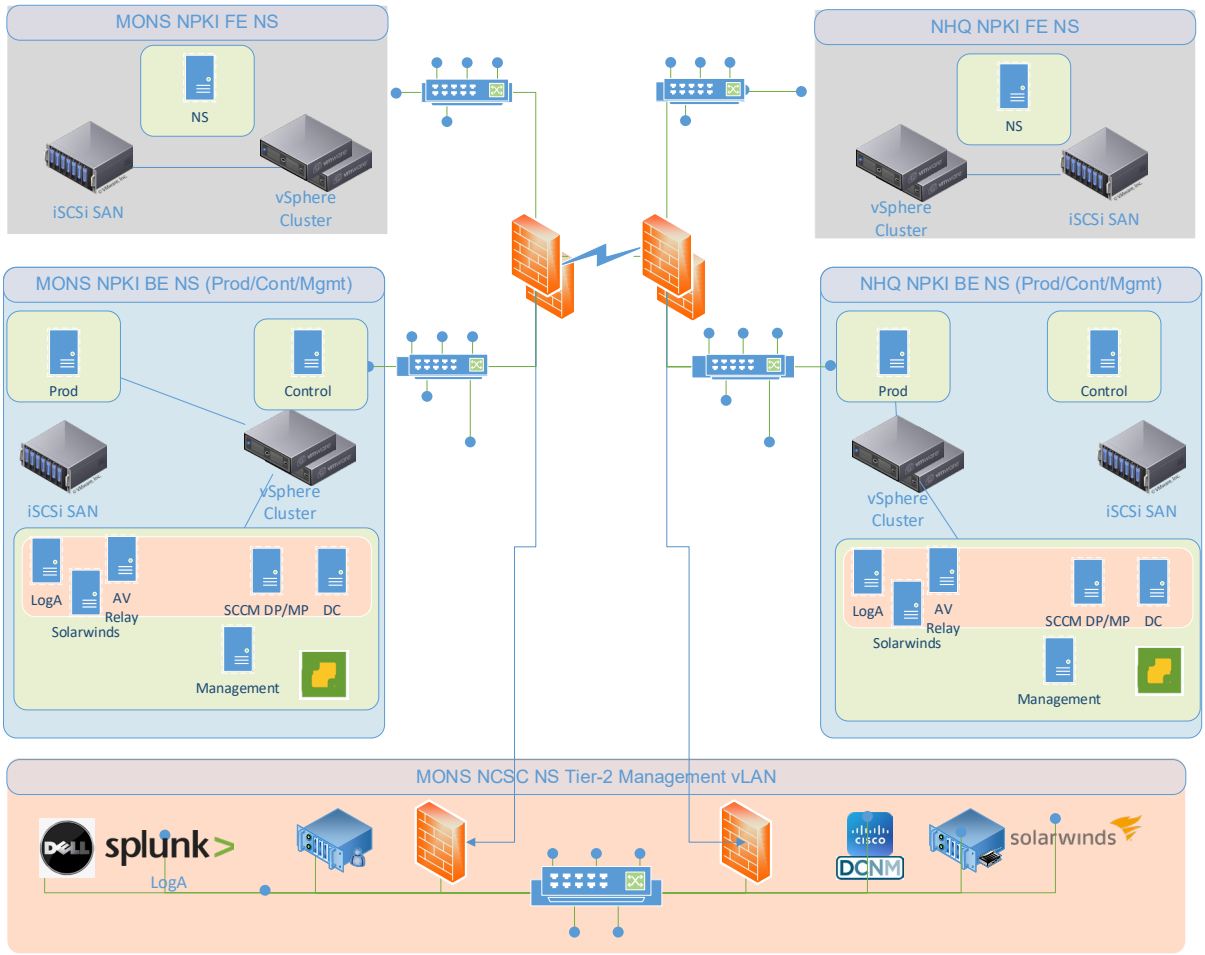

Figure 7- Logical Infrastructure Design NS

3.5.1 Active Directory

NPKI-M will utilize Microsoft's Active Directory Service to collectively manage Microsoft components. It provides authentication and authorization mechanisms as well as a framework within which other related services will operate as needed.

3.5.1.1 Domain Controllers

Two Read Only Domain Controllers for NPKI-M will be installed as virtual machine (VM)s and connected to NCSC Tier-2, allowing centralized authentication services for the domain and all subsystems via Active Directory Domain Services or Lightweight Domain Access Protocol Secure (LDAPS) services.

Attribute	*Value*
Hostname(s)	TBD1, TBD2
Virtual Cores	2
RAM (4Gb)	8
OS Drive	60
Data Drive	n/a
VLAN	TBD

IP Address	TBD

Table 6 – Domain Controllers specifications

3.5.1.2 Domain Name

The NPKI Mitigation Active Directory domain name will be provided after contract award.

3.5.1.3 Red Hat Integration

The direct integration of Linux machines with the NCSC Tier 2 Active Directory (AD) domain including Multi Factor Authentication based on two PFE smartcard types for authentication to all Red Hat operating systems. If necessary to meet this requirement, Red Hat Identity Management for the NPKI Mitigation Hosting Infrastructure to complete the Active Directory integration, may be required

Red Hat built-in Certificate Authority shall not be used. All required X.509 certificates shall be obtained from the NPKI CA.

3.5.1.4 Password Management

Password complexity will be enforced in line with NCSC policies and hardening guides.

3.5.1.5 Security OUs, Groups and Objects

Active Directory OUs, security groups and objects will be provided by the Purchaser after contract award.

Group Policy Object (GPO) s will be applied (NCSC GPO's) as required and shall implement the latest version.

3.5.2 DNS

NPKI-M DNS services will be hosted on the NPKI-M Active Directory servers. No DNS queries/traffic will be permitted to leave the NPKI-M network. Forwarders and Root Zones will be deleted from the DNS server ensuring that recursive DNS is not possible. The blocking of DNS traffic will be enforced by the NPKI-M both core and Front End firewall clusters, providing a second level of protection against recursive DNS queries as well as preventing clients from querying non-NPKI-M DNS servers directly.

3.5.3 DHCP

All clients will have a permanently reserved DHCP lease.

NPKI-M DHCP services will be hosted on a virtual machine and utilize VMWare High Availability for resiliency.

Attribute	*Value*
Hostname	TBD
Virtual Cores	2
RAM	8GB
OS Drive	60GB
Data Drive	N/A
VLAN	TBD
IP Address	TBD

Table 7 – DHCP servers

3.5.4 NTP

Network Time Protocol will be provided in NPKI-M from the NCSC Tier 2 system. 2 RHEL NTP Servers in each site will receive the NTP from NCSC Tier-2 and present said time source to all systems within the security domain.

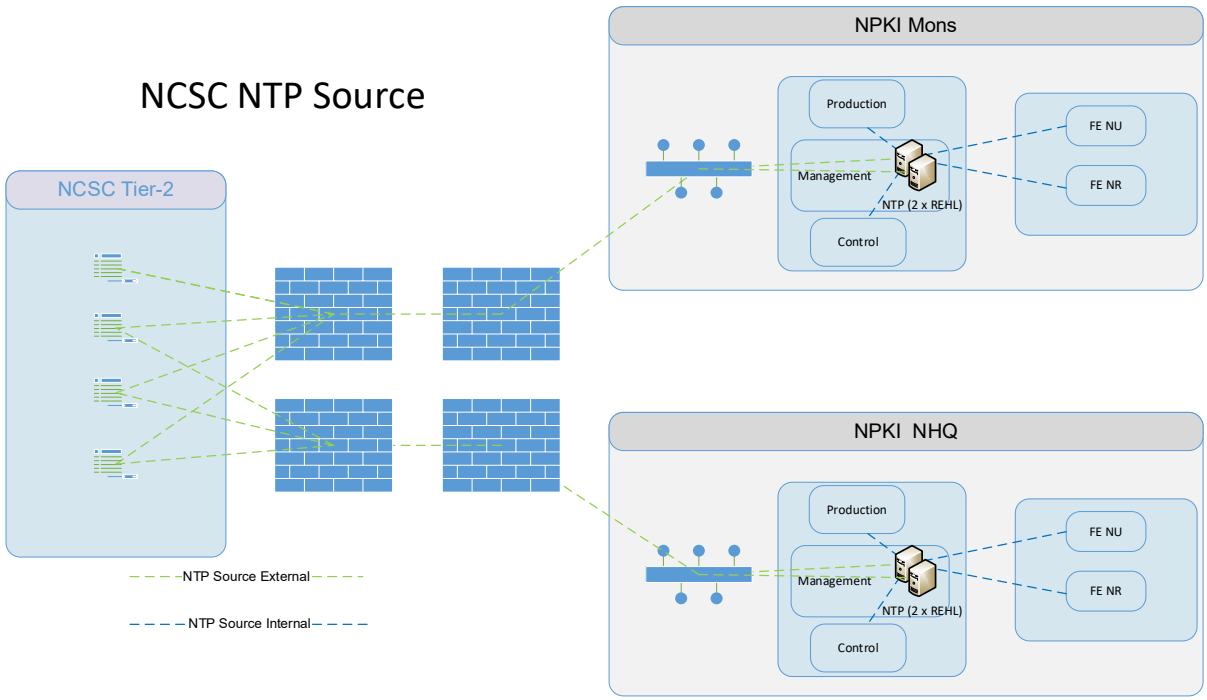

Figure 8: NTP Flow Diagram

3.5.5 Solarwinds

For the purpose of monitoring equipment installed and configured during the NPKI Project, an existing NCIA Solarwinds Monitoring system (Orion platform) will be implemented. Every domain will have a dedicated Solarwinds System installed (Orion Satellite Server).

There will be three components:

- The Orion server hosted in NCSC Tier-2 (already exists)
- The Orion proxy server: hosted within the NPKI-M management zone.
- The Orion agents: installed and configured on systems throughout the NPKI-M security domains.

SolarWinds agents will be used for monitoring, wherever possible. All agents will be configured as active agents, which means that any communication between the Orion proxy server or additional polling engines and the agent service is initiated by the agent service itself. In active mode, there are no listening ports on the agent.

The Orion proxy server shall be the only server that communicates with the NCSC Tier-2 Orion server.

The firewall rules need to be adjusted to allow communication between the Orion agent → Orion proxy server → Orion Server. Firewall rules are:

- Orion Server and Orion Proxy server:

Service/ Process	Direction	Description	Communication method	OS
n/a	Outbound	Used to install the agent on Linux/Unix computers through SSH and SFTP or SCP.	Either	Linux/Unix
Orion Module Engine SolarWinds Agent	Inbound	Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.	Agent-initiated	All

Table 8: **Firewall rules for Solarwinds Orion Server and Orion Proxy server**

- Orion Agent:

Service/ Process	Direction	Description	Communication method	OS
n/a	Outbound	Used to install the agent on Linux/Unix computers through SSH and SFTP or SCP.	Either	Linux/Unix
Orion Module Engine SolarWinds Agent	Inbound	Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.	Agent-initiated	All

Table 9: Firewall rules for Solarwinds Orion Agent.

3.5.5.1 SNMP

On all devices SNMP communication will be enabled for monitoring purpose and it will use:

- SNMP version 3 with Security Level "AuthPriv".
- Minimal privileges.
- Views defined in MIB limiting information to only those which are required.

Network devices will be configured to send SNMP traps in a case of issues. SNMP traps are received by the SolarWinds Trap Service, which listens for incoming trap messages on UDP port 162, and then decodes, displays, and stores the messages in the SolarWinds Orion database.

Firewall rules need to be adjusted in a following way:

- Orion Server and Orion Proxy server:

Service/Process	Direction	Description	Communication method
SolarWinds Job Engine v2 Solarwinds Cortex	Bi-Directional	Send and receive SNMP information	SNMP v3 with AES encryption
SolarWinds Trap Service SNMP Informs	Inbound	Receive trap messages	n/a

Table 10: Firewall rules for Solarwinds Orion Server and Orion Proxy server SNMP.

- SNMP Device:

Service/Process	Direction	Description	Communication method
SNMP Informs	Bi-Directional	Send and receive SNMP information	SNMP v3 with AES encryption
SNMP Informs	Outbound	Send trap messages	n/a

Table 11: Firewall rules for the SNMP device.

3.5.6 ITSM

BMC Remedy Footprints Server in the NCSC is used for service management and support ticketing. Tickets are created by calling or emailing the service desk, where their lifecycle is managed. There is no technical integration required with NPKI-M.

3.5.7 SCCM

System Center Configuration Manager (SCCM) Current Branch 1902 is used in the NPKI-M domain as the single tool to manage all servers and client workstations environments.

The primary site SCCM will be provided from NCSC Tier-2, deploying a branch distribution point and management point into the NPKI management VLAN. This will be a Windows VM hosted in the NPKI Hosting Services, domain joined to the NCSC domain. All Windows clients will connect to this server as a proxy. These roles are to be configure as HTTPS only with CA issued certs for secure communication.

A Site server deployed from NCSC Tier-2 this will remotely provide a gateway/ proxy server for the following roles:

- The SMS Provider service installed assigns roles to SCCM servers
- Management Point (MP) providing policy and location information to clients.
- The Distribution Point (DP) that contains files for clients to download
- Software Update Point (SUP, also known as WSUS) for patching clients.

This server will be a domain member of the tier-2 NCSC network but hosted in the NPKI-M management zone.

SCCM CB1902 will be used mainly for the following tasks:

- Consolidate inventory management
- Application delivery.
- Patch management.
- Reporting.
- Software Compliance.
- Increase IT productivity by reducing manual tasks.

The following table details the NPKI Tier-2 Servers per node:

ITEM #	*Site System Roles*	*Hostname*	*QTY*
1	Management Point SMS Provider	TBD	1

	Distribution Point Software Update Point		

Table 12 - SCCM Role Distribution

3.5.8 ePO

The Trellix ePO server is the central software repository for all Trellix product installations, updates, and other content. Packages are components that are checked in to the master repository, and then deployed to client systems.

One ePO relay server for each security classification domain will be deployed in both NATO HQ and Mons Management zones to manage the NPKI-M subsystems.

The NPKI-M ePO shall be manually uploaded from the ePO server within NCSC Tier-2. The updates will be automatically deployed to all managed endpoints within NPKI-M.

Attribute	*Value*
Hostname	TBD
Cores	4
RAM	16
OS Drive	80GB
Data Drive	50GB
Evidence Drive	100GB
VLAN	TBD
IP Address	TBD

Table 13 –Trellix ePO

3.5.8.1 Host Based Firewall and Intrusion Detection System (IDS)

Trellix Endpoint Security Threat Prevention (TP) and Firewall (FW) shall be deployed as part of the NPKI-M hardening of endpoints. Threat Prevention has three modules as follows, Access Protection, Exploit Prevention and Antivirus.

Exploit Prevention and Access Protection shall be deployed with the NCSC baseline configuration, when required the baseline configuration may be customized based on service/system requirements.

Trellix Firewall shall be deployed using a baseline server and workstation configuration based on NCSC Tier 2 instructions. Deviations to policies shall be implemented when a service/system requires an additional communication.

3.5.8.2 Anti-Virus

On Access scanning shall be enabled on all compatible systems using best practice and recommended exclusions. On Demand scanning shall be enabled and scheduled as per NCSC guidelines.

3.5.8.3 Data Loss Prevention

DLP will be deployed using Trellix EPO management server and using the DLP policies as implemented in NCSC Tier-2.

Trellix Data Loss Prevention shall be deployed into the Trellix ePolicy Orchestrator for central management and incident reporting. DLP policies shall follow NCSC DLP ruleset.

3.5.8.4 Application Control

Trellix Application Control shall be deployed into the Trellix ePolicy Orchestrator server where it can be centrally managed. Trellix Application Control shall be deployed to all supported endpoints where the system shall be inventoried and marked as trusted.

A Server and Client image shall be deployed to a server and workstation where the inventory will be discovered and be marked as trusted. This will allow for Gold Image deviation reports to be executed.

Microsoft Applocker shall not be deployed.

3.5.9 Logging Auditing and Retention

The Logging/Auditing/Retention capability will be performed via syslog messaging from network and firewall devices and Splunk universal forwarders on servers to a centralized syslog receiver in the NPKI-M. Transmission of NPKI-M logs to the NCSC Splunk implementation will be performed.

The contractor shall install and configure Splunk universal forwarders one per each server.

A virtual machine in the NPKI-M domain will be provisioned to host the Splunk Heavy Forwarder software. The Heavy Forwarder software parses these DB sourced logs and forwards them to the Splunk Indexer.

The specifications for the Heavy Forwarder VM are as follows:

Attribute	*Value*
Hostname	TBD
Virtual Cores	12
RAM	12 GB
OS Drive	60 GB
Data Drive	100 GB (capable of a minimum of 800 average IOPS)
VLAN	TBD
IP Address	TBD

Table 14 Splunk Heavy Forwarder VWs

Logs will be forwarded to the Heavy Forwarder either via Syslog or the use of the Universal Forwarder software agent, depending on the particular server type. The Heavy Forwarder will store all logs locally until what time the logging is integrated into the NCSC Splunk capability.

The Universal Forwarder agents will be deployed using the SCCM server hosted in the NPKI-M domain.

3.5.10 Dell OpenManage Enterprise

The Dell Openmanage Enterprise installed at NCSC Tier-2 will be used to manage, update and monitor the Dell hardware deployed throughout the NPKI network. This is operated and maintained by the NCSC infra team, via OOB.

Role based access can be used to grant others access to specific sets of hardware to allow NPKI team the ability to monitor hardware also. This will be provided by the NCSC Tier-2 DC, installed within the NPKI-M management zone.

3.5.11 Infrastructure Services Management

Management access is provided via the use of dedicated management servers called jumpboxes. Jumpboxes provide a central location to install administrator tools, scripts, and applications that can be shared among administrators. This provides the benefit that these privileged tools do not need to be installed on individual workstations that may be accessed by non-administrators. Additionally the jumpboxes are located in VLANs and Zones dedicated for management allowing for tighter control at the network and host firewalls by limiting authorized traffic from a limited IP range.

3.5.12 Red Hat HA PROXY

Each VMware cluster will have a Red Hat server configured to provide load balancing services for windows based services described in this document. Each Red hat server installed will also have the HA proxy installed and configured to provide failover support for the server hosted services.

3.5.13 VEEAM Backup

Backup services are provided by Veeam solution, which will use the PFE online datastore space. Disk backups shall be configured for both local and remote node storage. The following table proposes the backup and retention schedules for the NPKI-M. This information shall be verified with the purchaser prior to implementation.

Name	*Backup Type*	*Schedule*	*Retention*
Virtual Machines Local	VEEAM Backup	Daily (start 1800hrs)	14 daily (Incremental) 4 weekly 6 Monthly
Virtual Machines Remote	VEEAM Backup	Daily (start 1800hrs)	14 daily (Incremental) 4 weekly 6 Monthly
PostGreSQL	SQL Agent Based Backups	Daily (start 1800hrs)	14 daily (Incremental) 4 weekly 6 Monthly
File Servers	Snapshot	Daily (start 1800hrs)	14 daily (Incremental) 4 weekly 6 Monthly
Firewalls	Backup to Fileshare	On Demand	14 daily (Incremental) 4 weekly 6 Monthly

Table 15: Backup Schedule

3.6 VMware Hosting Services

The hosting services are the virtualization layer operating on top of the processing resources. The virtualization platform is VMWare vSphere-ESXI v8 hich manages the virtual machines. For each NPKI-M installation described in this document, two VMware infrastructures shall be installed matching the Storage and compute elements described in this document. HA VMware clusters shall be created and dedicated to the NPKI-M subsystem.

3.6.1 Processing (Compute) resources

The Processing resources consists of the physical processing hardware that provide the CPU and RAM capability for the environment. Processing equipment for the Reference environment is listed within PFE. Similar PFE equipment for the Production environments will be provided at Contract award. The required size of each cluster is provided in Table 16. The resources are managed via Resource Pools (soft resource isolation) and Affinity rules (hard separation). Hosts will be added to the cluster using host profiles, the purpose being speeding up the process, avoiding manual work and therefore reducing the room for error. Compute resource host information is provided in Table 17 and Table 18. Cluster attributes are provided in Table 19. Network segregation will be enforced through firewall terminated VLANs which are described in section 3.3.3.

Installation	*Virtual Cores* *Total Estimated Demand*	*Physical Cores* *Total Designed Availability*	*RAM* *Total Estimated Demand*	*RAM* *Total Designed Availability*	*CPU Speed*	*Servers (Per Site)*
NS Reference Core	94	96	288GB	384GB	2.6GHz	4
NS Reference Front End	26	48	104GB	192GB	2.6GHz	2
NS Production Core	94	96	288GB	384GB	2.8GHz	4
NS Production Front End	26	48	104GB	192GB	2.8GHz	2
NUNR Reference Core	94	96	288GB	384GB	2.6GHz	4
NUNR Reference Front End	48	32	192GB	256GB	2.6GHz	4
NUNR Production Core	94	96	288GB	384GB	2.8GHz	4

NUNR Production Front End	48	96	192GB	256GB	2.8GHz	4

Table 16: Processing Resources (Cores and RAM)

Attribute	*Value*
Vendor	Dell
Model	R740
Hostname	
Hostname OOB (iDrac)	
CPUs/Cores	2 / 12
RAM	TBD
NICs (RDMA capable)	4x 10GbE ports
Front End	2x 10GbE
Storage dedicated	2x 10GbE
Additional drivers / configurations	Dell VMware bestpractices Advanced Options NCSC Hardening IPMI intergration

Table 17 – Core VMWare Host information

Attribute	Value
Vendor	Dell
Model	R740
Hostname	
Hostname OOB (iDrac)	
CPUs/Cores	2 / 12
RAM	TBD
NICs (RDMA capable)	4x 10GbE ports
Front End	2x 10GbE
Storage dedicated	2x 10GbE
Additional drivers / configurations	Dell VMware best practices Advanced Options NCSC Hardening IPMI integration

Table 18 – Front END VMWare Host information

Attribute	*Value*

Name/Label	
HA	Yes
DRS	Yes
Settings	VM Groups Hostgroups[2] (Anti)Affinity rules (as requested by each VM owner)
EVC	no
Resource Pools	Yes
vApps	Yes
Datastores	Will leverage the auto-tiering provided by the SAN

Table 19 - VMware Cluster Information

3.6.2 Datastores

Datastores will be presented over iSCSI block protocol in a redundant and load balanced manner provided by the protocol itself, and NOT by any sort of teamed interface (e.g. LACP, switch independent teaming).

If deployed on individual NICs, as opposed to teamed interfaces, iSCSI protocol will enable multipathing and will leverage Round Robin policy, therefore the traffic will use both physical links.

The datastores will be provisioned as vVOL which counts a number of performance and management advantages. This is fully compatible with the backup solution, Veeam and fully supported by both VMware and Dell SAN.

Configuration advanced changes will be applied as per VMware best practices, specific to the Dell Unity SAN.

Attribute	Value
Datastores	Will leverage the auto-tiering provided by the SAN (optional)
Modern (vVOL - preferred)	Over iSCSI (see footnote)
Datastore 1	
Datastore 2	

Table 20: VMware Datastores

3.6.3 Virtual networking

Redundancy has to be implemented at the networking level, switch independent teaming, but there are 2 exceptions, in which we allow the higher level protocol to handle load balancing and redundancy (vMotion and iSCSI traffic). For these types of traffic, any sort of teaming will lower the performance.

[2] Having a single cluster for both Front End NU and Front End NR separation of resources will be done based on Host groups/Affinity rules.

3.6.4 vCenter configuration

vCenter server will be provided by the contractor in collaboration with NCSC from Tier-2 administration for each network , in a vendor supported scalable layout, providing HA within each DC.

3.6.5 VMware Management

VMware vCenter/Cluster access will be segregated in order to ensure role separation between admins of this environment. NCSC Tier-2 dedicated Active Directory will become an identity source for VMware vCenter and at least four levels of access will be created for the core admins based on their strict responsibilities.

Each relevant AD Security Group will be mapped against built-in VMware role.

3.6.6 Remote Management

The NPKI Mitigation servers utilize the Dell Integrated Device Remote Access Controller (iDRAC) for OOB management. The iDRAC is embedded within every Dell PowerEdge™ server and provides functionality that helps IT administrators deploy, update, monitor, and maintain Dell servers with no need for any additional software to be installed.

Access to the centralized processing management consoles shall be through the dedicated administrative jumpboxes within the dedicated VLANs described in section 3.3.3.

Administrators will be able to remotely configure the server hardware and initiate a remote desktop connection to the server from the NPKI-M administrative jumpboxes. Jumpboxes are detailed in section 3.5.11.

3.6.6.1 Security groups

Security groups will be created for administrators and operators roles and individual user accounts will be added to these groups:

3.7 Storage Services

Storage Services are provided on the dedicated DELL ME4024 Storage Arrays with DELL EMC ME412 Storage Expansion in Reference Environments. Two Dell ME5 Storage Arrays are provided per node in Production Environments. Separate storage services are provided for Core and Front end zones. The IaaS hosting infrastructure will connect to the storage system via a separate iSCSI storage VLAN, in a multipathing layout. iSCSI has been implemented as the main storage protocol, for security reasons, authentication between ESXi iSCSI initiators and Dell EMC Unity targets will be employed. The Low Level Design shall provide a detailed design implementing HA configurations between Datacenters.

3.8 Applications

3.8.1 Red Hat 389 Directory Servers

NPKI Mitigation project requires deployment of multiple Red Hat Directory Servers in a high availability configuration. Number of deployments shall follow Table 21.

Environment	Classification	Zone	# of Nodes
Production	NS	Control	2
Production	NS	Front-end	2
Production	NR	Control	2

Production	NR	Front-end	2
Reference	NS	Control	2
Reference	NS	Front-end	2
Reference	NR	Control	2
Reference	NR	Front-end	2

Table 21- Red Hat 389 Directory Server installations

These directory services shall be installed and configured to comply with the following requirements:

- Directory servers shall be deployed on Red Hat operating system from the RHEL repositories, unless stated otherwise by the Purchaser, during the design review sessions.
- Directory servers in the controlled zone shall be configured as read-write servers as known as supplier servers. These shall be configured as multi-supplier replication nodes.
- Directory servers in the front-end zone shall be configured as read only servers as known as consumer directory servers. These shall be configured to replicate data from all supplier servers.
- Directory servers shall have enough resources such as CPU, memory and storage to support the NPKI Mitigation HA deployment. The Purchaser will provide the resource requirements before the directory servers deployment.
- Directory servers configuration parameters shall be decided with the Purchaser such as listening ports, TLS/SSL settings, log file locations, backup locations, file permission settings etc.
- Directory servers' hosts shall apply the NATO Cyber Security Centre (NCSC) security settings for Red Hat Enterprise Linux 8.

The Purchaser will provide an installation guide for multi-supplier replication nodes as a starting point. Instructions for installation of consumer directory servers shall be produced.

A step-by-step deployment and installation documents for the deployed directory servers, including with the required updates for the multi-supplier servers and consumer servers shall be produced.

3.8.2 PostgreSQL

NPKI Mitigation project requires deployment of multiple PostgreSQL database clusters in a high availability configuration based on the industry best practices regarding high availability deployment of PostgreSQL database services. Deployments shall follow Table 22.

Environment	Classification	Zone	# of DB Cluster	# of Nodes
Production	NS	Control	1	4
Production	NS	Production	1	4
Production	NR	Control	1	4
Production	NR	Production	1	4
Reference	NS	Control	1	4
Reference	NS	Production	1	4

Reference	NR	Control	1	4
Reference	NR	Production	1	4

Table 22- PostgreSQL Database installations

These database clusters shall be installed and configured to comply with the following requirements:

- DB clusters shall be deployed on Red Hat operating system from the RHEL repositories, unless stated otherwise by the Purchaser.
- DB clusters shall be able to contain multiple databases with a synchronous replication.
- DB clusters shall have enough resources such as CPU, memory and storage to support the NPKI Mitigation HA deployment. The Purchaser will provide the resource requirements before the DB cluster deployment. The Contractor may also make recommendations based on their experience.
- DB cluster configuration parameters shall be decided with the Purchaser such as listening ports, TLS/SSL settings, log file locations, backup locations etc.
- DB cluster deployment shall apply the NATO Cyber Security Centre (NCSC) security settings for PostgreSQL on Linux. These include OS level network configurations, file permissions, user permissions, TLS settings and SELinux configurations but not limited to these settings.
- DB cluster Red Hat servers shall apply the NATO Cyber Security Centre (NCSC) security settings for Red Hat Enterprise Linux 8.
- DB clusters shall be configured for synchronous data replication between master and standby servers.
- DB clusters shall be configured with automated failover to ensure service continuity without interruption to the database clients.

DB clusters shall be thoroughly tested for HA availability functionalities and failover cases.

The Contractor shall provide step by step deployment and failover recovery documents for the deployed PostgreSQL Database services.

3.8.3 Red Hat Capsule Servers

The Contractor shall deploy Red Hat Capsule servers in each installation of the NPKI-M Hosting infrastructure. The Contractor shall connect the Capsule servers to the Purchaser's Red Hat Satellite management system.

NPKI Mitigation Red Hat Capsule servers shall adhere to the following requirements:

- Management system shall not require internet connectivity and be able to work offline.
- Shall integrate with the Red Hat Satellite servers in the NCSC Tier-2 Management Zone.
- All NPKI-M hosting infrastructure Red Hat servers shall be managed by the Red Hat Capsule Servers.

4 BILL OF MATERIALS

This section details the bill of materials for NPKI-M. It contains the PFE and the expected virtual machines within the environment.

4.1 Purchaser Furnished Equipment (PFE)

All physical infrastructure components for NPKI-M are provided by the purchaser. The following table details the PFE provided by the Purchaser.

Environment	Device Function	Model	Specification	Number of devices per installation	Number of installations	Total Number of Devices
Production (NS+NU/NR) NHQ+SHAPE	Core Switch	Nexus 93180YC-FX3 (NX-OS Mode) 48 port switch (fiber)	License: NX-OS Essentials(minimum). All ports licensed. NX-OS mode / accessory kit(rack mounts) Port side Exhaust Nexus Fan Port side Exhaust Dual 650W AC Power Supply Port Side Exhaust 2 AC Cabinet Power Cables	2	4	8
	OOB Switch	Cisco Switch Catalyst C9200-48T-A (IOS Mode)	Network Advantage License All ports licensed / Accessory kit(rack mounts) Dual Power Supply PWR-C6-125WAC C9200-NM-4X Network Module 2xAC Cabinet Power Cables	1	4	4
	CISCO Transceivers	CISCO QSFP	QSFP-4x10G 2 meter cable compatible with Nexus 93180YC-FX3	2	4	8
	CISCO Transceivers	CISCO 10Gb SFP+	Multimode (Short Range) Compatible with Nexus 93180YC-FX3 and Catalyst 9200-48-A (for uplinks)	68	4	272
	CISCO Transceivers	CISCO 1Gb Copper SFP	Compatible with Nexus 93180YC-FX3 (will be used to connect the HSMs)	6	4	24
	Storage (Core SAN)	Dell EMC ME5024 Storage Array	Hardware — Quantity Dell EMC ME5024 Storage Array — 1 25 Gb iSCSI 8 Port Dual Controller — 1 2.4TB HDD 10k SAS12 2.5 — 12 1.92 TB SSD SAS ISE Read Intesive 12 Gbps — 7 Dual power supplies, Cable Management Europe AC Cabinet Power Cables	1	4	4
	Storage (Front SAN)	Dell EMC ME5024 Storage Array	Hardware — Quantity Dell EMC ME5024 Storage Array — 1 25 Gb iSCSI 8 Port Dual Controller — 1 2.4TB HDD 10k SAS12 2.5 — 12 1.92 TB SSD SAS ISE Read Intesive 12 Gbps — 4 Dual power supplies, Cable Management Europe AC Cabinet Power Cables	1	4	4
	Dell Transceivers	Dell Transceivers, 10 Gb SFP+ (fiber)	Short Range	8	4	32
	Virtualization servers (Low Side)	Dell PowerEdge R750 with TPM	2x 3rd generation Intel Xeon CPUs (Intel Xeon Platinum 8358) minimum: 256 GB RAM (8x32GB RAM modules) 2X 3.5 inch SAS 600GB hard drives Intel Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0 Intel X710 Quad Port 10GbE SFP+ Adapter, PCIe Full Height Dual power supplies/ Cable management/ Europe AC Cabinet Power Cables	8	2	16
	Virtualization servers (High Side)	Dell PowerEdge R750 with TPM	2x 3rd generation Intel Xeon CPUs (Intel Xeon Platinum 8358) minimum: 256 GB RAM (8x32GB RAM modules) 2X 3.5 inch SAS 600GB hard drives Intel Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0 Intel X710 Quad Port 10GbE SFP+ Adapter, PCIe Full Height Dual power supplies/Cable management/ Europe AC Cabinet Power Cables	6	2	12
	KVM switch	Dell DMPU2016-G01 16-port remote KVM switch	With 2 remote users, 1 local user, Dual power supply	2	4	8
	KVM monitor and keyboard	Dell LED KMM, 18.5", 1U, International English Keyboard - DKMMLED185 - 001		2	4	8
	KVM mounting bracket	DELL DRMK-77 for Dell only oneU KVM mounting braket for Dell 185FPM and DKMMLED185 LED		2	4	8
	Firewall	PA 3420	Dual power	2	4	8
	Firewall	PA 3410	Dual power	2	4	8
	Palo Alto Transceivers	Palo Alto 1 GB SFP+	Compatible with PA 3420 and PA 3410	4	4	16
	Palo Alto Transceivers	Palo Alto 10 GB SFP+	Multimode (Short Range) Compatible with PA 3420 and PA3410	24	4	96
	HSM	SafeNet Network HSM S790	Dual power	3 (2+1 including spares)	2	6
	Rack	APC Netshelter SX AR3300 42U rack with side panels	Two independent physical locks on the front door and two independent physical locks on the back door. This is to enforce Two Person Integrity (TPI) for the physical access to the NPKI-M equipment.	2	4	8
	Rack PDU	10 KW per rack	2 per rack	2	4	8

Environment	Device Function	Model	Specification	Number of devices per installation	Number of installations	Total Number of Devices
Reference (NS+NU/NR) SHAPE	Core Switch	C9300X-48TX-A to replace the CISCO Nexus 31108TC-V	License: NX-OS Essentials(minimum). All ports licensed NX-OS mode Accessory kit(rack mounts) Port side Exhaust Nexus Fan Port side Exhaust Dual AC 350w Power Supply Port Side Exhaust 2x AC Cabinet Power Cables	2	4	8
	OOB Switch	Cisco Switch Catalyst C9200-48T-A (IOS Mode)	Network Advantage License All ports licensed Dual Power Supply PWR-C6-125WAC C9200-NM-4X Network Module 2x AC Cabinet Power Cables	1	4	8
	Storage	Dell EMC ME5024 Storage Array	Hardware Quantity Dell EMC ME5024 Storage Array 1 10 Gb iSCSI Base-T 8 Port Dual Controller 1 2.4TB HDD 10k SAS12 2.5 12 1.92 TB SSD SAS ISE Read Intesive 12 Gbps 3 Dual power	2	4	8
	Network Cards	Network Cards for Dell R740 TPM servers	Intel X710-T4L Quad Port 10GbE Base-T Adaptor PCIe Full Height	7	4	28
	Rack	APC Netshelter SX AR3300 42U rack with side panels	Two independent physical locks on the front door and two independent physical locks on the back door. This is to enforce Two Person Integrity (TPI) for the physical access to the NPKI-M equipment.	2	4	8 (currently there are 4+2 racks in ref)
	Rack PDU	10 KW per rack	2 per rack	2	4	8
Additional HW (NS+NU/NR)	Smartcards	Thales TCT SC650 v4.2	High Side			100
	Smartcards	Thales IDPrime PIV 3	Low side			100
	Smartcard readers	Gemalto IDBridge CT31				20
	Management workstations	Standard NCSC management workstation				7
SW	Windows Server License					88
	Windows client (management workstations)					7
	Esxi Licenses (Virtualization)	vSphere 8 Enterprise Plus				112
	vSphere (required for dedicated vCenter)	vSphere 8 Enterprise Plus				4
	Smartcard middleware	90 meter				20
	SCCM node to Enterprise					
	Trellix EPO Relay Server					
	Solarwinds Orion Proxy Server					
	VEEAM					
	Splunk Heavy Forwarder					

Table 23 Overview of PFE

4.2 Virtual machines

For NPKI-M, different services have to be provisioned within the infrastructure. Table 24 and Table 33 give an overview of these services.

Zone	Description / Role	OS	Add On	Classification	vCPU	Disk 1 (GB)	Disk 2 (GB)	RAM (GB)
NU Front-end	Load Balancer node 1	Red Hat		NU	4	60	100	16
	Load Balancer node 2	Red Hat		NU	4	60	100	16
	CRL web server	Red Hat		NU	2	60	100	8
	EAAS Front-end	Red Hat		NU	2	60	100	8
	OCSP proxy-TSA proxy	Red Hat		NU	2	60	100	8
	EIE SSM proxy	Red Hat		NU	2	60	100	8
	CA proxy	Windows		NU	2	60	100	8
	NATO RA Module	Windows 10 (client)		NU	2	60	100	8
	SMTP Mail Relay Server	Red Hat		NU	2	60	100	8
NR Front-end	Load Balancer node 1	Red Hat		NR	4	60	100	16
	Load Balancer node 2	Red Hat		NR	4	60	100	16
	Shadow Directory Services	Red Hat	Red Hat Directory services	NR	4	60	200	16
	CRL web server	Red Hat		NR	2	60	100	8
	EAAS Front-end	Red Hat		NR	2	60	100	8
	OCSP proxy-TSA proxy	Red Hat		NR	2	60	100	8
	EIE SSM proxy	Red Hat		NR	2	60	100	8
	CA proxy	Windows		NR	2	60	100	8
	NATO RA Module	Windows 10 (client)		NR	2	60	100	8
	SMTP Mail Relay Server	Red Hat		NR	2	60	100	8
Production	EIE	Red Hat		NR	2	60	100	8
	SQL server	Red Hat	Postgres SQL server	NR	4	60	200	16
	SQL server	Red Hat	Postgres SQL server	NR	4	60	200	16
	EAAS Back-end APP Server	Red Hat		NR	2	60	100	8
	Cert Hub	Red Hat		NR	4	60	200	8
	CA Gateway	Red Hat		NR	4	60	200	8
Controlled Zone	CA	Red Hat		NR	2	60	100	8
	OCSP	Windows		NR	8	60	200	16
	TSA	Windows		NR	8	60	200	16
	Main Directory Services	Red Hat	Red Hat Directory services	NR	4	60	200	16
	SQL server	Red Hat	Postgres SQL server	NR	4	60	200	16
	SQL server	Red Hat	Postgres SQL server	NR	4	60	200	16
Core Management Zone	Read Only Domain Controller 1	Windows		NR	2	60	100	8
	SCCM node to Enterprise	Windows		NR	2	60	100	8
	Orion Proxy Server	Windows		NR	2	60	200	8
	EPO Relay Server	Windows		NR	2	60	200	8
	VEEAM	Red Hat		NR	8	60	200	16
	Jump box	Red Hat		NR	2	60	1000	16
	Jump box	Windows		NR	2	60	1000	16
	SPLUNK Heavy Forwarder	Red Hat		NR	12	60	100	12
	SMA	Windows (32 bit)		NR	2	60	100	8
	NTP node to Enterprise	Red Hat		NR	2	60	100	8
	NTP node to Enterprise	Red Hat		NR	2	60	100	8
	RH Capsule Server	Red Hat	Red Hat Capsule Server	NR	4	60	200	12
	RH Identity Server	Red Hat	RH Identity Server	NR	2	60	100	8

Table 24 Virtual Machines and services for NPKI-M NU/NR

Zone	Description	OS	Add On	Classification	vCPU	Disk 1 (GB)	Disk 2 (GB)	RAM (GB)
Front-end	Load Balancer node 1	Red Hat		NS	4	60	100	16
	Load Balancer node 2	Red Hat		NS	4	60	100	16
	Shadow Directory Services	Red Hat	Red Hat Directory services	NS	4	60	200	16
	CRL web server	Red Hat		NS	2	60	100	8
	EAAS Front-end	Red Hat		NS	2	60	100	8
	OCSP proxy-TSA proxy	Red Hat		NS	2	60	100	8
	EIE SSM proxy	Red Hat		NS	2	60	100	8
	CA proxy	Windows		NS	2	60	100	8
	NATO RA Module	Windows 10 (client)		NS	2	60	100	8
	SMTP Mail Relay Server	Red Hat		NS	2	60	100	8
Production	EIE	Red Hat		NS	2	60	100	8
	SQL server	Red Hat	Postgres SQL server	NS	4	60	200	16
	SQL server	Red Hat	Postgres SQL server	NS	4	60	200	16
	EAAS Back-end	Red Hat		NS	2	60	100	8
	Cert Hub	Red Hat		NS	2	60	200	8
	CA Gateway	Red Hat		NS	2	60	200	8
Controlled Zone	CA	Red Hat		NS	2	60	100	8
	OCSP	Windows		NS	8	60	200	16
	TSA	Windows		NS	8	60	200	16
	Main Directory Services	Red Hat	Red Hat Directory services	NS	4	60	200	16
	SQL server	Red Hat	Postgres SQL server	NS	4	60	200	16
	SQL server	Red Hat	Postgres SQL server	NS	4	60	200	16
Core Management Zone	Read Only Domain Controller	Windows		NS	2	60	100	8
	SCCM node to Enterprise	Windows		NS	2	60	100	8
	Orion Proxy Server	Windows		NS	2	60	200	8
	EPO Relay Server	Windows		NS	2	60	200	8
	VEEAM	Red Hat		NS	8	60	200	16
	Jump box	Red Hat		NS	2	60	1000	16
	Jump box	Windows		NS	2	60	1000	16
	Splunk Heavy Forwarder	Red Hat		NS	12	60	100	12
	SMA	Windows (32 bit)		NS	2	60	100	8
	NTP node to Enterprise	Red Hat		NS	2	60	100	8
	NTP node to Enterprise	Red Hat		NS	2	60	100	8
	Red Hat Capsule Server	Red Hat	Red Hat Capsule Server	NS	4	60	200	12
	RH Identity Server	Red Hat	RH Identity Server	NS	2	60	100	8

Table 25 Virtual Machines and services for NPKI-M NS

5 REFERENCE**: RFQ-CO-115518-NPKI-M WP 2 – DATA CENTRE INSTALLATION SOW**

6 ACRONYMS

Abbreviation	Definition
AD	Active Directory
ADM	Administrator
AGPM	Active Directory Group Policy Manager Servers
ASAPP	Entrust Admin Service Application Server
ASWEB	Entrust Admin Service Web Server
ATA	Advanced Threat Analytics
CA	Entrust Authority Security Manager
CAG	CA Gateway
CAPRX	Entrust Authority Security Manager Proxy
CDP	Certificate Revocation List Distribution Point
CES	Core Enterprise Services
CHUB	Certificate Hub
CIS	Communication and Information Systems
CLIN	Contract Line Item Number
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSU	Cyber Security Unit
CSW	Core Switch
DB	Database
DC	Data Center/ Domain Controller
DCI	Data Centre Interconnect
DCNM	Datacentre Network Manager
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Protection
DMZ	Demilitarized Zone
DNS	Domain Name Server
DP	Distribution Point
DRS	VMware vSphere® Distributed Resource Schedule
EIE	Entrust Identity Enterprise Server
EPO	Trellix EPO Server
ESS	Electronic Security System
ESXI	Elastic Sky X Integrated

EVC	Vmware Enhanced vMotion Compatibility
FIPS	Federal Information Processing Standard
FS	File Share Servers
FW	Firewall
FW	Firewall
GB	Gigabyte
GEO	Geographic
GPO	Group Policy Object
HA	High Availability
HLD	High Level Design
HPS	Hosting Platform Services
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
iDRAC	Dell Integrated Device Remote Access Controller
IDS	Intrusion Detection System
IOPS	Input/output operations per second
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
ISCSI	Internet Small Computer Systems Interface
IT	Information Technology
ITSM	Information Technology Service Management
KVM	Keyboard Video Mouse Switch
LACP	Link Aggregation Control Protocol
LB	Load Balancers
LDAP	Lightweight Directory Access Protocol Server
LDAPS	Lightweight Directory Access Protocol Secure
LLD	Low Level Design
LOG	Log Receiver/Forwarder Server
MIB	Management Information Base
MP	Management Point
MSW	Management Switch
NAC	Network Access Control
NATO	North Atlantic Treaty Organization
NCI	NATO Communications Infrastructure
NCIA	NATO Communication & Information Agency
NCSC	NATO Cyber Security Center

NHQ	NATO Headquarters
NPKI	NATO PKI
NPKI-M	NATO PKI Mitigation
NR	NATO Restricted
NRA	NATO Registration Authority Module
NS	NATO Secret
NISC	
NTP	Network Time Protocol
NU	NATO Unclassified
OCSP	Online Certificate Status Protocol
OOB	Out of Band
OS	Operating System
OTPRX	Online Certificate Status Protocol and Time Stamping Proxy Server
PFE	Purchaser's Furnished Equipment
PKI	Public Key Cryptography
PSC	VMWare Platform Service Controller
QTY	Quantity
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RDMA	Remote direct memory access
RHCS	Red Hat Capsule Server
RHEL	RedHat Enterprise Linux
RHIS	Red Hat Identity Server
RHSS	Red Hat Satellite Server
RR	NATO Restricted in Reference Environment
RS	NATO Secret in Reference Environment
RU	NATO Unclassified in Reference Environment
SA	Storage Arrays
SAN	Storage Area Network
SCCM	System Center Configuration Manager
SCOM	System Center Operations Manager Server
SHAPE	Supreme Headquarters Allied Powers Europe
SM	Security Mechanism
SMA	Entrust Authority Security Manager Administration

SMS	SMS provider/To manage Configuration Manager, you use a Configuration Manager console that connects to an instance of the SMS Provider. By default, an SMS Provider installs on the site server when you install a central administration site (CAS) or primary site. The SMS Provider is a Windows Management Instrumentation (WMI) provider that assigns read and write access to the Configuration Manager database at a site.
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	TBD
SOW	Statement of Work
SQL	Structured Query Language
SQLC	SQL Cluster
SSH	Secure Shell Protocol
SSL	Secure Socket Layer
SUP	Software Update Point
TBD	To Be Defined
TLS	Transport Layer Security
TP	Threat Prevention
TSA	Time Stamping Authority
TU	NATO Unclassified in Test Environment
UDP	User Datagram Protocol
VH	Virtualization Host
VHC	Virtualization Host Cluster
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VVOL	Virtual Volume
WSUS	Windows Server Update Service Server