



NATO UNCLASSIFIED

Acquisition

Peter.Kowalski@ncia.nato.int

NCIA/ACQ/2022/06845

25 May 2022

To: See Distribution List

From: The Director of Acquisition, NCI Agency

Subject: **REQUEST FOR QUOTATION RFQ-CO-115114-ETEE**
"Provision Of Ballistic Missile Defence (BMD) Information Management Portal Within Education, Training, Exercise and Evaluation (ETEE) Functional Services (FS)"

Reference(s) : A. AC/4-D(2019)0004 (INV)
B. AC/4/(PP)D/27804-ADD1 (INV)
C. AC/4-DS(2020)0022

Dear Sir/Madam,

1. Your firm is hereby invited to participate in a Request for Quotation under BOA procedure for the provision of **"Ballistic Missile Defence (BMD) Information Management Portal Within Education, Training, Exercise and Evaluation (ETEE) Functional Services (FS)"**.
2. With the aim to prevent an organizational conflict of interest in industrial roles under the BMD Increment 1 Functions in ETEE FS project, Bidders participating in this RFQ and their prospective Sub-Contractors shall be excluded from participation in the companion NCI Agency ETEE FS project under IFB-CO-115115-ETEE entitled **"BMD Functions In ETEE FS - WP4 Operational Assurance & Test"**.
3. The award will be based on the proposal evaluated as the lowest price, technically compliant in accordance with the selection criteria set forth in the Bidding Instructions.
4. **THE CLOSING TIME FOR ELECTRONIC SUBMISSION OF BIDS IN RESPONSE TO THIS REQUEST FOR QUOTATION IS 12:00 HOURS (BRUSSELS TIME) ON 11 JULY 2022.**
5. This Request for Quotation consists of the Bidding Instructions (Book I) and the Prospective Contract (Book II). The Prospective Contract contains the Schedule of Supplies and Services (Part I), Contract Special Provisions (Part II), Contract General Provisions (Part III), and the Statement of Work (Part IV). The Statement of Work and the Annexes thereto set forth detailed specifications governing the performance requirements of the contract.



NATO Communications
and Information Agency
Agence OTAN d'information
et de communication

Boulevard Leopold III
1110 Brussels, Belgium

www.ncia.nato.int

NATO UNCLASSIFIED

6. The overall security classification of this Request for Quotation is "NATO UNCLASSIFIED". This Request for Quotation remains the property of the NCI Agency and shall be protected in accordance with the applicable national security regulations.
7. The Bidders have the right to request RFQ clarifications as outlined in section 2.6 of the Bidding Instructions (Book I).
8. You are requested to complete and return the enclosed acknowledgement of receipt within 5 days of receipt of this RFQ, informing NCI Agency of your intention to bid/not to bid. Your firm is not bound by its initial decision, and if you decide to reverse your stated intention at a later date, you are requested to advise us by a separate letter.
9. Prospective Bidders are advised that the NCI Agency reserves the right to cancel this RFQ at any time in its entirety and bears no liability for bid preparation costs incurred by firms or any other collateral costs if bid cancellation occurs.
10. The The NCI Agency points of contact for all information concerning this RFQ are Mr. Peter Kowalski, Senior Contracting Officer, and Ms. Dorina Cani, Principal Contracting Assistant, who may be reached at Peter.Kowalski@ncia.nato.int and Dorina.Cani@ncia.nato.int.

FOR THE DIRECTOR OF ACQUISITION:

[Original Signed By]

Peter Kowalski
Senior Contracting Officer

Enclosures:

Attachment A: Acknowledgement of Receipt of Request for Quotation

Distribution List

All Prospective Bidders 1

NATO Delegations (Attn: Infrastructure Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
United Kingdom	1
United States	1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1

Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
United Kingdom	1
United States (electronic copy to brussels.office.box@mail.doc.gov)	1
Belgian Ministry of Economic Affairs	1

Distribution for information

NATO HQ

NATO Office of Resources

Management and Implementation Branch – Attn: Deputy Branch Chief 1

Director, NATO HQ C3 Staff

Attn: Executive Co-ordinator 1

SACTREPEUR

Attn: Infrastructure Assistant 1

Strategic Commands

ACT

HQ SACT CAPDEV IAMD BMD

Program Director BMD - Attn: CDR Eric Schuurmans 1

SHAPE

SHAPE SDP SDF COR COO

Attn: LTC Marcus Nieswand 1

NCI Agency – All NATEXs

NCI Agency

Chief of Acquisition 1

Deputy Chief of Acquisition 1

Contract Award Board Administrator 1

Chief of Contracts	1
Principal Contracting Officer	1
Princial Contracting Assistant	1
Director AMDC2	1
Chief C2 Centre	1
C2 Centre – Senior Supplier	1
C2 Centre – Project Manager	1
C2 Centre – Technical Lead	1
Liaison Officer to the Investment Committee	1
Legal Office	1

Attachment A**Acknowledgement of Receipt of Request for Quotation****RFQ-CO-115114-ETEE**

Please complete, sign and return by email (scanned to PDF) within 14 days
to: Peter.Kowalski@ncia.nato.int **and** Dorina.Cani@ncia.nato.int.

We hereby advise that we have received Request for Quotation RFQ-CO-115114-ETEE
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 bid.
- { } We do not intend to submit a bid.
- { } 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: _____

REQUEST FOR QUOTATION

RFQ-CO-115114-ETEE

**Provision Of Ballistic Missile Defence (BMD) Information
Management Portal Within Education, Training, Exercise and
Evaluation (ETEE) Functional Services (FS)**

**AUTHORISATION/SERIAL NO.
2013/OIS03074-05/58/59**



GENERAL INDEX

BOOK I - THE BIDDING INSTRUCTIONS

Section I	Introduction
Section II	General Bidding Information
Section III	Bid Preparation Instructions
Section IV	Bid Evaluation
Annex A	Bidding Sheets
Annex B	Bidding Sheets - Instructions
Annex C	Certificates
Annex D	Cross Reference/Compliance Table
Annex E	Clarification Requests forms
Annex F	RESERVED

BOOK II - THE PROSPECTIVE CONTRACT

	Signature Sheet
Part I	Schedule of Supplies and Services
Part II	Contract Special Provisions
Part III	Statement of Work



RFQ-CO-115114-ETEE

BOOK I

BIDDING INSTRUCTIONS

CONTENTS

1	INTRODUCTION	1
2	GENERAL BIDDING INFORMATION	2
2.1	DEFINITIONS	2
2.2	ELIGIBILITY	2
2.3	BID DELIVERY AND BID CLOSING	3
2.4	REQUESTS FOR EXTENSION OF BID CLOSING DATE	4
2.5	PURCHASER POINTS OF CONTACT	4
2.6	REQUESTS FOR RFQ CLARIFICATIONS	5
2.7	REQUESTS FOR WAIVERS AND DEVIATIONS	5
2.8	AMENDMENT OF THE REQUEST FOR QUOTATION	6
2.9	MODIFICATION AND WITHDRAWAL OF BIDS	6
2.10	BID VALIDITY	6
2.11	BID GUARANTEE	7
2.12	CANCELLATION OF REQUEST FOR QUOTES	7
2.13	ELECTRONIC TRANSMISSION OF INFORMATION AND DATA	7
2.14	NOTICE TO BIDDERS OF CONTRACT DISTRIBUTION AND DISCLOSURE OF INFORMATION	8
3	BID PREPARATION INSTRUCTIONS	9
3.1	GENERAL	9
3.2	PREPARATION OF THE ADMINISTRATIVE PACKAGE (PART 1)	10
3.3	PREPARATION OF THE PRICE QUOTATION (PART 2)	11
3.4	PREPARATION OF THE TECHNICAL PROPOSAL (PART 3)	14
3.5	PACKAGING AND MARKING OF BIDS	16
4	BID EVALUATION	17
4.1	GENERAL	17
4.2	ADMINISTRATIVE CRITERIA	18
4.3	PRICE CRITERIA	18
4.4	TECHNICAL CRITERIA	21
	ANNEX A – BIDDING SHEETS	23
	ANNEX B - INSTRUCTIONS FOR THE PREPARATION OF BIDDING SHEETS	24
	ANNEX C – CERTIFICATES	25
	ANNEX D – Bid-Requirements Cross Reference Matrix (BRCM)	44
	ANNEX E – Clarification Request Forms	46
	ANNEX F – RESERVED	49

1 INTRODUCTION

- 1.1 The purpose of this Request for Quote (RFQ) is to obtain the provision of services to deliver and implement a Ballistic Missile Defence (BMD) Information Management (IM) portal that fits into the NATO portal environment and is configured to meet the Education, Training, Exercise And Evaluation (ETEE) Functional Services (FS) requirements.
- 1.2 The Contractor shall provide and implement the performance requirements as set forth in the relevant Statement of Work (Book II Part IV) and in the Schedule of Supplies and Services (Book II Part I) in the manner, and at times and the place, stated in the prospective Contract.
- 1.3 This RFQ is issued and shall be conducted under the revised NATO Procedure: *“Procedure Governing the Use of Basic Ordering Agreements concluded by the NATO Communications and Information Agency – 2019 version”*, Ref: AC/4-D(2019)0004 (INV).
- 1.4 The security classification of this RFQ is “NATO UNCLASSIFIED”.
- 1.5 With the aim to prevent an organizational conflict of interest in industrial roles under the overarching “BMD Increment 1 Functions in ETEE FS” project, Bidders on this RFQ and their prospective Sub-Contractors shall be excluded from participation in the companion NCI Agency ETEE FS project under RFQ-CO-115115-ETEE entitled *“BMD Increment 1 Functions In ETEE FS - WP4 Operational Assurance & Test”*.
- 1.6 Basis of Award: The contract resulting from this RFQ shall be awarded to the lowest priced compliant offer.
- 1.7 The Bidder shall refer to the Purchaser all queries for a resolution of conflicts found in information contained in this document in accordance with the procedures set forth in §2.6 of the Bidding Instructions entitled “Requests for RFQ Clarifications”.
- 1.8 The target date for Contract Award is November 2022.

2 GENERAL BIDDING INFORMATION

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 “Bidder” as used herein refers to a firm, consortium, or joint venture which submits an offer in response to this solicitation.
- 2.1.3 The term “Compliance” as used herein means strict conformity to the requirements and standards specified in this Request for Quote.
- 2.1.4 The term “Contractor” refers to a firm of a participating country which has signed a Contract under which it will perform a service, manufacture a product, or carry out work for NATO.
- 2.1.5 The term “Participating Country” as used herein means one of the contributory NATO nations in the project, namely, (in alphabetical order):
- ALBANIA, BELGIUM, BULGARIA, CANADA, CROATIA, CZECH REPUBLIC, DENMARK, ESTONIA, FRANCE, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, MONTENEGRO, NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TURKEY, UNITED KINGDOM, UNITED STATES OF AMERICA.**
- 2.1.6 The term “Purchaser” refers to the authority issuing the RFQ and/or awarding the Contract (the NATO Communications and Information Agency, NCIA).
- 2.1.7 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 Only firms which hold an active BOA stipulated with the NCI Agency are eligible to take part in this RFQ. In addition, all contractors, sub-contractors and manufacturers, at any tier, must be from Participating Countries.
- 2.2.2 None of the work, including project design, labour and services shall be performed other than by firms from and within Participating Countries.
- 2.2.3 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.
- 2.2.4 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.

- 2.2.5 Bidders are at liberty to constitute themselves into any form of contractual arrangements or legal entity they desire, bearing in mind that in consortium-type arrangements a single judicial personality shall be established to represent that legal entity. A legal entity, such as an individual, Partnership or Corporation, herein referred to as the “Prime Contractor”, shall represent all members of the consortium with the NCI Agency and/or NATO. The “Prime Contractor” shall be vested with full power and authority to act on behalf of all members of the consortium, within the prescribed powers stated in an irrevocable Power of Attorney issued to the “Prime Contractor” by all members associated with the consortium. Evidence of authority to act on behalf of the consortium by the “Prime Contractor” shall be enclosed and sent with the Bid. Failure to furnish proof of authority shall be a reason for the Bid being declared non-compliant.

2.3 BID DELIVERY AND BID CLOSING

- 2.3.1 All Quotations shall be in the possession of the Purchaser at the e-mail address given below in Paragraph 2.3.2 below before **12:00 Hours (BRUSSELS TIME) on Monday, 11 JULY 2022** at which time and date Quotations shall be closed.
- 2.3.2 Offerors are requested to submit their quotation electronically **solely and only** to the following email address:
Email: RFQCO115114ETEEWP3@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-115114-ETEE – Official Bid for [company name] – Part 1 - Administrative Envelope**”. The e-mail content shall be as described in Paragraph 3.1.4 (a) below, with no password or encryption protection to the file and shall be **not larger than 10MB total**.
- 2.3.3.2 For the **second e-mail** the subject line shall read: “**RFQ-CO-115114-ETEE – Official Bid for [company name] – Part 2 - Price Quotation**”. The e-mail content shall be as described in Paragraph 3.1.4 (b) below, with no password protection or encryption to the file, and shall be **not larger than 10MB total**.
- 2.3.3.3 For the **third e-mail** the subject line shall read: “**RFQ-CO-115114-ETEE – Official Bid for [company name] – Part 3 – Technical Proposal**”. The e-mail content shall be as described in Paragraph 3.1.4 (c) below, with no password protection to the file, and shall be **not larger than 10MB total** per e-mail. For large Technical Proposals, multiple e-mails may be required and are allowed to submit the entire package. In such case, Bidders 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 Bid Closing are “Late Bids” and shall not be considered for award.
- 2.3.5 It is the responsibility of the Offeror to ensure that the quotation submission is

duly completed by the specified quotation closing time and date. If a quotation received at the NCI Agency's facility by electronic submission 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.

2.3.6 Consideration of Late Bid. It is the responsibility of the Bidder to ensure that the bid submission is duly completed by the specified bid closing time. A late bid shall only be considered for award under the following circumstances:

- 2.3.6.1 A contract has not already been awarded pursuant to the Request for Quotation, and,
- 2.3.6.2 The bid was sent **only** to the correct email specified in Section address specified in Section 2.3.2 (RFQCO115114ETEEWP3@ncia.nato.int) and the delay was due solely to the fault of the Purchaser.

2.4 REQUESTS FOR EXTENSION OF BID CLOSING DATE

The Purchaser does not accept, except in exceptional cases, Bidder requests to extend the Bid Closing Date. In any event, all questions and requests for extension of bid closing date must be submitted in writing by fax or e-mail. Such questions shall be forwarded to the Point of Contact specified in § 2.5 and shall arrive **not later than fourteen (14) days** before the closing date of the bid. The Purchaser is under no obligation to consider or answer requests submitted after this time. Extensions to the Bid Closing Date are at the sole discretion of the Purchaser.

2.5 PURCHASER POINTS OF CONTACT

- 2.5.1. The Purchaser Points of Contact (POC) for all information and questions/clarification requests concerning this RFQ is:

Mr. Peter Kowalski, Senior Contracting Officer
Acquisition
E-mail: peter.kowalski@ncia.nato.int

With a Copy to:

Ms. Dorina Cani, Principal Contracting Assistant
Acquisition
E-mail: dorina.cani@ncia.nato.int

- 2.5.2. Bid Delivery: all bids shall be delivered by email as stated in paragraph 2.3.2. and only to that email address.

2.6 REQUESTS FOR RFQ CLARIFICATIONS

- 2.6.1 Bidders, 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 in writing using the format in Annex E, 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 POC specified in § 2.5 and shall arrive **not later than 30 days after RFQ release 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 Bidder for any given area, as the Bidder will generally not be permitted to revisit areas of the RFQ for additional clarification as noted in §2.6.3.
- 2.6.3 Bidders are advised that subsequent questions and/or requests for clarification included in a bid 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 (anonymized to remove the identity of the questioner) shall be issued in writing to all prospective bidders.
- 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 Bidder in its offer.

2.7 REQUESTS FOR WAIVERS AND DEVIATIONS

- 2.7.1 Bidders are informed that requests for alteration to, waivers of, or deviations from the Schedules, the Special Contract Provisions, the Technical Specifications, the Statement of Work and any other Terms and Conditions of the Prospective Contract shall not be considered after the closing date and time for Requests for Clarification from bidders.
- 2.7.2 Requests for alterations to the other requirements, terms or conditions of the Request for Quote or the Prospective Contract may only be considered as part of the clarification process set forth in §2.6. Requests for alterations to the specifications, terms and conditions of the Contract which are included in a Bid as submitted may be regarded by the Purchaser as a qualification or condition of the Bid and may be grounds for a determination of non-compliance.

2.8 AMENDMENT OF THE REQUEST FOR QUOTATION

- 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 Bid Closing. Any and all modifications will be transmitted to all prospective bidders by an official amendment designated as such and issued by the Contracting Authority. Such amendment shall be recorded in the Acknowledgement of Receipt (Annex C-6) which the bidder shall complete and enclose as part of its bid. This process may be part of the clarification procedures set forth in §2.6 or may be an independent action on the part of the Purchaser.
- 2.8.2 The Purchaser may consider the potential impact of amendments on the ability of prospective Bidders to prepare a proper bid within the allotted time. The Purchaser may extend the "Bid Closing Date" at its discretion and such extension shall be set forth in the amendment document.
- 2.8.3 In no case, however, shall the closing date for receipt of bids be less than seven (7) days from the date of issuance of any amendment to the RFQ.

2.9 MODIFICATION AND WITHDRAWAL OF BIDS

- 2.9.1 Bids, once submitted, may be modified by Bidders, 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 Bid Closing. Such modifications shall be considered as an integral part of the submitted bid.
- 2.9.2 Modifications to bids which arrive after the Bid Closing Date shall be considered as "Late Modifications" and shall be processed in accordance with the procedure set forth above concerning "Late Bids", except that unlike a "Late Bid", the Purchaser shall retain the modification until a selection is made. A modification to a bid which is determined to be late shall not be considered in the evaluation and selection process. If the Bidder submitting the modification is determined to be the successful Bidder on the basis of the unmodified bid, the modification may then be opened. If the modification makes the terms of the bid more favourable to the Purchaser, the modified bid may be used as the basis of Contract award. The Purchaser, however, reserves the right to award a Contract to the apparent successful Bidder on the basis of the bid submitted and disregard the late modification.
- 2.9.3 A Bidder may withdraw its bid at any time prior to Bid Opening without penalty. In order to do so, an authorised agent or employee of the Bidder must provide an original statement of the firm's decision to withdraw the bid.

2.10 BID VALIDITY

- 2.10.1 Bidders shall be bound by the term of their bids for a period of nine (9) months starting from the Bid Closing Date specified in §2.3.1.

2.10.2 In order to comply with this requirement, the Bidder shall complete the Certificate of Bid Validity set forth in Annex C-3 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 in §2.10.1. 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 bids which remain under consideration for award.

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

(a) accept this extension of time in which case Bidders shall be bound by the terms of their offer for the extended period of time and the Certificate of Bid Validity extended accordingly; or

(b) refuse this extension of time and withdraw the bid without penalty.

2.10.5 Bidders shall not have the right to modify their bids due to a Purchaser request for extension of the bid validity unless expressly stated in such request.

2.11 BID GUARANTEE

2.11.1 Responses against this Request for Quotation do not require the submission of a Bid Guarantee.

2.12 CANCELLATION OF REQUEST FOR QUOTES

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 shall any Bidder have cause for action against the Purchaser for the recovery of costs incurred in connection with preparation and submission of a bid in response to this RFQ.

2.13 ELECTRONIC TRANSMISSION OF INFORMATION AND DATA

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

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

2.13.3. Bidders are cautioned that electronic transmission of documentation which contains classified information is not allowed.

2.14 NOTICE TO BIDDERS OF CONTRACT DISTRIBUTION AND DISCLOSURE OF INFORMATION

- 2.14.1. The resulting Contract is subject to release to the applicable NATO Resource Committee through the NATO Office of Resources (NOR).
- 2.14.2. The resulting Contract may be subject to release to (i) NATO Resource Committees for audit purposes (including audits carried out using third party companies- See Book II, Special Provisions Article entitled, "Notice of Authorized Disclosure of Information for Mandated NATO Third Party Audits"; and (ii) to the customer holding a Service Level Agreement with the Agency related to this requirement, upon request from that customer.

3 BID PREPARATION INSTRUCTIONS

3.1 GENERAL

- 3.1.1 Bids shall be prepared in accordance with the instructions set forth herein. Failure to comply with these instructions may result in the Bid being declared non-compliant.
- 3.1.2 Bidders shall prepare a complete bid which comprehensively addresses all requirements stated herein. The Bid shall demonstrate the Bidder's understanding of the RFQ and its ability to provide all the deliverables and services listed in the Schedule of Supplies and Services. Bids which are not complete may be declared non-compliant.
- 3.1.3 The Bidder shall not restate the RFQ requirements in confirmatory terms only. The Bidder must clearly describe what is being offered and exactly how the Bidder will meet all RFQ requirements. Statements in confirmatory terms only shall be sufficient grounds for determining the bid to be non-compliant.
- 3.1.4 **Bidders shall prepare their bid in 3 parts in the following quantities**

- | | |
|--------------------------------------|---|
| (a) Administrative Package (Part 1): | Electronic: Scanned PDF copies of the certificates with physical (non-digital) signatures of the prescribed certifications detailed in §3.2.
No password protection or encryption. |
| (b) Price Quotation (Part 2): | Electronic: The Price Quotation shall contain one (1) ZIP file containing one (1) electronic copy in Microsoft Excel (readable and searchable) of the completed Schedule of Supplies and Services and one (1) PDF copy of the completed Schedule of Supplies and Services as detailed in § 3.3.
No password protection or encryption. |
| (c) Technical Proposal (Part 3): | Electronic: The Technical Proposal shall be self-contained as a separate electronic file in one (1) ZIP file, named as described in Section §3.4.
No password protection or encryption. |

3.1.5 Documents submitted in accordance with §3.1.4 shall be classified no higher than “NATO UNCLASSIFIED”.

3.1.6 Partial Bids and/or bids containing conditional statements may be declared non-compliant.

3.1.7 Where a PDF format is mandated in these instructions, electronic bid 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.

3.1.8 All bidding documents submitted shall be only in the English language.

3.2 PREPARATION OF THE ADMINISTRATIVE PACKAGE (PART 1)

3.2.1 The Bid Administrative Package shall include in accordance with § 3.1.4(a) one ZIP file submitted by email comprised of the required documents.

3.2.2 The Package shall include the Certificates set forth in Annexes to these Bidding Instructions, signed in the original by an authorised representative of the Bidder. Within the Package the bidder shall also include the signed electronic copies of the **certifications** – with physical, not electronic signatures - **set forth in Annex C** hereto, specifically:

- (a) C-1 Certificate of Legal Name of Bidder
- (b) C-2 Certificate of Independent Determination
- (c) C-3 Certificate of Bid Validity
- (d) C-4 Certificate of Understanding
- (e) C-5 Certificate of Exclusion of Taxes, Duties and Charges
- (f) C-6 Acknowledgement of Receipt of RFQ Amendments
- (g) C-7 Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements
- (h) C-8 Certification of NATO Member Country of Origin of Delivered Equipment, Services, Material and Intellectual Property Rights
- (i) C-9 Comprehension and Acceptance of Contract Special Provisions and BOA Provisions
- (j) C-10 List of Prospective Sub-Contractors / Consortium members

- (k) C-11 Certificate of AQAP 2110 or ISO-9001:2015 Compliance.
- (l) C-12 List of Key Personnel with Security Clearance Information
- (m) C-13 Disclosure of Involvement of Former NCI Agency Employment
- (n) C-14 Bidder Background Intellectual Property Rights (IPR)
- (o) C-15 List of 3rd Party Intellectual Property Rights (IPR)

3.2.3 Concerning Certificate C-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 Bidder shall state this separately. **The subcontractors listed in this certificate shall be traceable in the Price Bidding Sheets.**

3.2.4 Concerning Certificate C-7, Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements, Bidders shall note especially the following:

- 3.2.4.1 If supplemental agreements, such as End-User Certificates or Technical Assistance Agreements, are required by national regulations, a draft of these must be submitted with the Bidders Bid. Supplemental agreements submitted after the Bid Closing Date shall not be considered.
- 3.2.4.2 The terms of supplemental agreements, if necessary, are the Bidders / Contractors responsibility and shall be fully 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.
- 3.2.4.3 A problem with the supplemental agreement in any of the areas mentioned previously in this provision may result in a determination that the Bid is not compliant with the terms of the RFQ, and in rejection of the Bid, or termination for default of the Contract if the supplemental agreement is submitted after Contract award.
- 3.2.5 The Bidder shall include 1 (one) additional copy of the Technical Proposal Cross-Reference/Compliance Table (see §3.4.4) in the Administrative Package. A copy shall also be included in the Technical Proposal.

3.3 PREPARATION OF THE PRICE QUOTATION (PART 2)

- 3.3.1 Bidders shall prepare their Price Proposal in accordance with § 3.1.4(b) by submitting one (1) ZIP file containing the completed electronic copy of the Bidding Sheets (Excel) provided with this RFQ under Book I, Annex A and B. The Bidder shall propose an accurate and complete

price quotation in completing the Schedule of Supplies and Services as defined in these Bidding Instructions. No alteration of the form and pre-filled content of the Bidding Sheets is allowed, unless otherwise specified in these instructions.

- 3.3.2 The prices provided shall be intended as the comprehensive total price offered for the fulfilment of all requirements as expressed in the RFQ documentation including but not limited to those expressed in the SOW.
- 3.3.3 Bidders shall furnish Firm Fixed Prices for all required items in accordance with the format set forth in the Instructions for preparation of the Bidding Sheets.
- 3.3.4 Bidders shall prepare their Price Quotation by completing the yellow highlighted sections of the Bidding Sheets in accordance with the instructions specified in Annex B.
- 3.3.5 Bidders shall quote in their own national currency or in EUR, the host nation currency. Bidders may also submit bids in multiple currencies including other NATO member states' currencies under the following conditions:
- (a) the currency is of a "Participating Country" in the project, and
 - (b) the Bidder can demonstrate, either through sub-contract arrangements or in its proposed work methodology, that it will have equivalent expenses in that currency. All major sub-contracts and their approximate anticipated value should be listed on a separate sheet and included with the Price Quotation.
- 3.3.6 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 Contractor, therefore, shall certify that the prices stipulated in this Contract do not include amounts to cover such direct taxes or customs duties.
- 3.3.7 The Contractor shall be responsible for ensuring that its respective Sub-contractors are aware that the Purchaser is exempt from taxes and customs duties. The Contractor (and its 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. Bidders are reminded of the requirement to complete the certification to this effect in Annex C-5.
- 3.3.8 Unless otherwise specified in the instructions for the preparation of bidding sheets, 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.

- 3.3.9 The Bidder's attention is directed to the fact that their Price Quotation shall contain no document and/or information other than the priced copies of the Bidding Sheets. 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.
- 3.3.10 When completing the Bidding Sheets, a unit price and total firm fixed price for each proposed element must be supplied on each and every CLIN line item **including all options provided for this RFQ, if any**. Prices should not be grouped. The prices and quantities entered on the document shall reflect the amount of the total items required to meet the contractual requirements. Partial quotations shall be rejected. 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, Bidders 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 Bidding Sheets is the responsibility of the Bidder. The Purchaser in its favour may resolve ambiguous computation of prices.
- 3.3.11 The Bidding Sheets shall clearly illustrate the totals per CLIN and the grand total price of the bid in accordance with the format set out in the Annex A of these Bidding Instructions.
- 3.3.12 The Bidder shall furnish firm fixed price quotations, for all proposed items. Partial and/or contingent quotations shall be rejected. See Section 1, Para 1.5 through 1.7.
- 3.3.13 The Bidder understands that there is no obligation under this Contract for the Purchaser to exercise any part of the contract designated as an Option. The Purchaser bears no liability should it decide not to exercise such options.
- 3.3.14 The Contractor shall be fully liable for all other taxes, assessments, fees, licenses, work permits, 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 itself of its liability in each country where such liability may arise. The Purchaser does not provide, sponsor, or arrange for any privileges or immunities for the Contractor or the Contractor's staff in the nation(s) where the work under this RFQ is to be performed.
- 3.3.15 Price Proposals specifying delivery or performance dates in variance dates exceeding the deadlines for completion of works indicated in the Schedule of Supplies and Services may be declared non-compliant. Price Proposals that are offered as contingent may be deemed to be non-compliant (see Para

1.5).

- 3.3.16 The Bidder 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 C-10.

3.4 PREPARATION OF THE TECHNICAL PROPOSAL (PART 3)

- 3.4.1 Bidders shall submit their **Technical Proposal** in an electronic package with separate documents in PDF or MS Office formats as required, containing all the information addressing the technical specifications and requirements of the **Statement of Work (SOW)**. The Technical Proposal shall have a confirmation that all requirements in SOW, Book II Part III are included in the proposed solution.
- 3.4.2 The Technical Proposal package shall not exceed 100 pages when printed on A4 paper.
- 3.4.3 “Times New Roman” fonts in size 12 shall be used for normal text, and “Arial Narrow” fonts not smaller than size 10 for tables and graphics.
- 3.4.4 Bid-Requirements Cross-Reference Matrix (BRCM). The Bidder shall include a completed BRCM according to the format described at Annex D of Book I.
- 3.4.5 Software Engineering Section:
- 3.4.5.1 Reserved.
- 3.4.5.2 The Bidder shall confirm that the offered Software Engineering Team for the intermediate delivery phase shall be available in line with the capacity and performance period requirements described for the intermediate delivery in Section 2.3.1 of the SoW.
- 3.4.5.3 For the intermediate delivery phase, the Bidder shall provide evidence of the required qualifications of the proposed Senior Software Engineer and two (2) proposed personnel for the role of Software engineer (all Key Personnel). For each person, the bidder shall provide evidence that the personnel meet at least the required essential qualifications specified in the Sections 2.3.3, 2.3.4 and 2.3.5 of the SOW by describing per person the role that they match, the software development projects that they have worked on within the past five (5) years: a short, less than 240 words, description of the project including at least the following items: the approach applied to deliver the project outcome, their role, their time assigned to the project, the technologies employed by the person to contribute to the implementation of the project, the software development and collaboration environment, the coding principles and guidelines applied and their role in designing, executing and documenting unit testing. The information shall be presented in a tabular format in descending chronological order.

- 3.4.5.4 For the intermediate delivery phase, the Bidder shall provide, in addition to the personnel referenced in Section 3.4.5.3, a similar description as defined in Section 3.4.5.3 for one alternate Senior Software Engineer and one alternate person for the role of Software Engineer, in support of Section 2.3.6 of the SOW.
- 3.4.5.5 The Bidder shall confirm that the offered Senior Software Engineer for the final delivery phase shall be available in line with the capacity and performance period requirements described for the final delivery in Section 2.3.1 of the SoW.
- 3.4.5.6 For the final delivery phase, the Bidder shall provide evidence of the required qualifications of the proposed Senior Software Engineer (Key Personnel). If the proposed person is already referenced in response to Section 3.4.5.3 or Section 3.4.5.4, a clear reference to the already provided evidence is sufficient. If an alternate person is proposed, the bidder shall provide evidence that the person meets at least the required essential qualifications specified in the Sections 2.3.3 and 2.3.4 of the SOW by describing this person: the software development projects that he or she has worked on within the past five (5) years: a short, less than 240 words, description of the project including at least the following items: the approach applied to deliver the project outcome, their role, their time assigned to the project, the technologies employed by the person to contribute to the implementation of the project, and the software development and collaboration environment. The information shall be presented in a tabular format in descending chronological order.
- 3.4.5.7 The Bidder shall provide evidence, for example via TOEFL certificate, that all the Software Engineering Key Personnel offered in the Sections 3.4.5.3, 3.4.5.4 and 3.4.5.6 meet the English language proficiency requirement described in Section 2.3.3.4 of the SoW.
- 3.4.6 Training Material Section:
- 3.4.6.1 The Bidder shall confirm that the offered Contractor Training SME for the Training Material Support shall be available in line with the capacity and performance period requirements described in Section 3.1.3 of the SoW.
- 3.4.6.2 The Bidder shall provide evidence of the required qualifications of one (1) proposed personnel to provide the required Training SME Support. The evidence shall demonstrate compliance with the Section 3.2 of the SoW by describing the training and training material development experience of the person in the past three (3) years. The description shall contain at least the following items: a description of the system to be trained, a description of the training materials that they have developed, the training events that they have conducted, the language in which the training was delivered and the training approach that was employed e.g. classroom, electronically, remotely. The Bidder shall provide evidence, for example via TOEFL certificate, that the proposed Contractor Training SME meets the English language proficiency requirement equivalent to that described in Section 3.2.3 of the SoW.

- 3.4.7 Additional materials such as brochures, sales literature, product endorsements and unrelated technical or descriptive narratives shall not be included in the Technical Proposal.

3.5 PACKAGING AND MARKING OF BIDS

- 3.5.1 The Administrative Package, Price Quotation and the Technical Proposal shall be segregated and **not password protected or encrypted**. Three separate emails shall be sent in accordance to § 2.3.3 of Book I.

4 BID EVALUATION

4.1 GENERAL

- 4.1.1 The evaluation of bids shall be made by the Purchaser solely on the basis of the requirements in this RFQ. Failure to address any of the bidding requirements in this RFQ or omission of the critical information may result in a determination of non-compliance for the entire Bid.
- 4.1.2 The evaluation of bids and the determination as to the compliance or technical adequacy of the supplies and services offered shall be based only on that information furnished by the Bidder and contained in its bid. The Purchaser shall not be responsible for locating or securing any information which is not included in the bid.
- 4.1.3 The information provided shall be to a level of detail necessary for the Purchaser to determine exactly what the Bidder proposes to furnish and whether the offer meets the technical, administrative and contractual requirements of this RFQ.
- 4.1.4 During the evaluation, the Purchaser may request clarification of the bid from the Bidder, and the Bidder 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 shall be to resolve ambiguities in the bid and to permit the Bidder to state its intentions regarding certain statements contained therein. The Bidder is not permitted any cardinal alteration of the bid regarding technical matters and shall not make any change to its price quotation at any time.
- 4.1.5 The Bidder'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 bid to be deemed non-compliant.
- 4.1.6 The evaluation will be conducted 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 the NATO document AC/4-D(2019)0004 (INV), or in accordance with any variation specifically authorized by the relevant NATO authority for this acquisition.
- 4.1.7 The administrative compliance of the Bids will be evaluated first. Bids 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: Part 2 - Price, Part 3 - Technical.
- 4.1.8 All administrative compliant Bids shall be reviewed for price compliancy. The

Contract resulting from this RFQ shall be awarded to the bidder whose offer, as evaluated by the Purchaser, is the lowest priced bid and compliant with the requirements of this RFQ.

4.2 ADMINISTRATIVE CRITERIA

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

- (a) The Bid was received by the Bid Closing Date and Time,
- (b) The Bid was packaged and marked properly (as per §3.5).
- (c) The Administrative Package contains all the requested and required Certificates in Annex C hereto.

4.2.2 A Bid 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 Bidder has taken exception to the Terms and Conditions of the Prospective Contract, or has qualified and/or otherwise conditioned its offer on a modification or alteration of the Terms and Conditions or the language of the Statement of Work, the Bidder may be determined to have submitted a non-compliant bid.

4.3 PRICE CRITERIA

4.3.1 The Bidder's Price Quotation

4.3.1.1 The Bidder's Price Quotation shall be first assessed for compliance against the standards detailed in the following paragraphs. A bid 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.

4.3.1.2 The Price Quotation meets the requirements for preparation and submission of the Price Quotation set forth in the Bid Preparation Section (§3) and the Instructions for Contractor's Bidding Sheets (Annex B hereto), in particular:

- a. The Bidder has prepared the Price Proposal in the form of the Bidding Sheets provided under Annex A of these Bidding Instructions, by completing the yellow highlighted sections in accordance with the instructions specified in Annex B.
- b. The Bidder has furnished Firm Fixed Prices for all items listed.
- c. All pricing data, i.e., quantities, unit prices, has been provided as reflected in the Bidding Sheets.

- d. Bid prices include all costs for items supplied, delivered, and supported.
- e. All prices have been accurately entered into appropriate columns, and accurately summed up.
- f. The Bidder has provided accurate unit price, and total price for each line item and sub-item (if any). The prices of the sub-items (if any) total the price of the major item of which they constitute a part.
- g. The totals per CLIN and the bid grand total are accurate.
- h. The currency of all line items has been clearly indicated. Line items with multiple currencies contain as many totals on that line item as there are identified currencies.
- i. The Bidder 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 §3.3.4 are met.
- j. The Bidder 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.
- k. Price quotes for each individual item(s) and totalled prices are accurate, realistic (based on historic data, and/or market and competitive trends in the specified industrial sector(s)), adequate and traceable.

4.3.1.3 Price Quotation does not contain any document and/or information other than the priced copies of the Bidding Sheets. 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.

4.3.1.4 The Price Quotation meets requirements for price realism as described in §4.3.4.

4.3.1.5 Completed Bidding Sheets shall show that the offered delivery schedule meets the mandatory delivery requirements of the Prospective Contract.

4.3.2 Basis of Price Comparison and Award(s)

4.3.2.1 The Purchaser shall convert all prices quoted into EURO for purposes of comparison and computation of price scores. The exchange rate to be utilised by the Purchaser shall 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 Bid Closing Date.

4.3.2.2 Basis of Award: The contract shall be awarded to the Bidder with the

proposal evaluated as offering the lowest priced compliant offer.

4.3.3 Inconsistencies and discrepancies in bid price quotation

4.3.3.1 In case of inconsistencies, discrepancies and/or contradictory pricing information in the different parts of the bid price submission and notwithstanding the possibility for the Purchaser, at its sole discretion to obtain clarification from the bidder, for the purpose of determining the total price of the Bid, the following order of precedence shall apply:

- a. Bidding Sheet Total to be Evaluated Bid Price as indicated by the Bidder,
- b. Total of the Bid calculated from the indicated Total Prices(s) indicated per CLIN(s).

4.3.4 Price Realism

4.3.4.1 Otherwise successful Bidders that submit a price quotation so low that it is not a realistic reflection of the objective cost of performance of the associated technical proposal may be considered by the Purchaser to have submitted an unrealistic offer and that offer may be determined to be non-compliant.

4.3.4.2 Indicators of an unrealistically low bid may be the following, amongst others:

- a. Labour Costs that, when amortised over the expected or proposed direct labour hours, indicate average labour rates far below those prevailing in the Bidders locality for the types of labour proposed.
- b. 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.
- c. Numerous Line Item prices for supplies and services that are provided at no cost or at nominal prices.

4.3.4.3 If the Purchaser has reason to suspect that a Bidder has artificially debased its prices in order to secure contract award, the Purchaser will request clarification of the bid in this regard and the Bidder shall provide explanation on one of the following bases:

- a. An error was made in the preparation of the Price Quotation. In such a case, the Bidder 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 Bidder. In such a case, the Bidder shall petition the Purchaser to both remain in the competition and accept the Contract at the offered price, or to withdraw from the competition.

- b. The Bidder has a competitive advantage due to prior experience or industrial/technological processes that demonstrably reduce the costs of Bidder 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.
 - c. The Bidder recognises that the submitted Price Quotation is unrealistically low compared to its cost of performance and, for business reasons, the Bidder is willing to absorb such a loss. Such a statement can only be made by the head of the business unit submitting the Bid and will normally be made at the level of Chief Operating Officer or Chief Executive Officer. In such a case, the Bidder shall estimate the potential loss and show that the financial resources of the Bidder are adequate to withstand such reduction in revenue.
- 4.3.4.4 If a Bidder fails to submit a comprehensive and compelling response on one of the bases above, the Purchaser may determine the Bid submitted as non-compliant. If the Bidder responds on the basis of a) above and requests to withdraw from the competition, the Purchaser may, depending on the nature and gravity of the mistake, allow the Bidder to withdraw.
- 4.3.4.5 If the Purchaser accepts the Bidder's explanation of mistake in §4 . 3 . 4 . 3 (a) and allows the Bidder to accept the Contract at the offered price, or the Purchaser accepts the Bidder's explanation pursuant to §4 . 3 . 4 . 3 (c), the Bidder shall agree that the supporting pricing data submitted with its Bid may be incorporated by reference in the resultant Contract. The Bidder 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.
- 4.3.4.6 If the Bidder presents a convincing rationale pursuant to §4 . 3 . 4 . 3 (b), no additional action may be warranted. The Purchaser, however, reserves its right to reject such an argument if the rationale, in the Purchaser's opinion, is not compelling or capable of objective analysis. In such a case the Bid may be determined to be non-compliant.

4.4 TECHNICAL CRITERIA

- 4.4.1 Upon determination of the lowest-priced Bid as described above, the Bid shall be evaluated to confirm compliance with the criteria in Table 1 associated with the respective sections of the Technical Proposal.

EVALUATION CRITERIA	RFQ REFERENCE
Provided confirmation of the availability of the Software Engineering Team for the intermediate delivery phase as requested in the SoW	Book I 3.4.5.2 SoW 2.3.1
Provided proof that the proposed Senior Software Engineer Key Personnel for the intermediate delivery phase fulfils all essential qualifications listed in the SoW Section 2.3.3 and 2.3.4	Book I 3.4.5.3, 3.4.5.7, SOW 2.3.3, 2.3.4
Provided proof that the Software Engineers of the proposed team for the intermediate delivery phase fulfils all essential qualifications listed in the SoW Section 2.3.3	Book I 3.4.5.3, 3.4.5.7, SOW 2.3.3
Provided proof that one of the Software Engineers of the proposed team for the intermediate delivery phase fulfils all essential qualifications listed in the SOW Section 2.3.5	Book I 3.4.5.3, SOW 2.3.5
Provided proof that the alternate Senior Software Engineer Key Personnel for the intermediate delivery phase fulfils all essential qualifications listed in the SoW Section 2.3.3 and 2.3.4	Book I 3.4.5.4, 3.4.5.7, SOW 2.3.3, 2.3.4, 2.3.6
Provided proof that the alternate Software Engineer for the intermediate delivery phase fulfils all essential qualifications listed in the SoW Section 2.3.3	Book I 3.4.5.4, 3.4.5.7, SOW 2.3.3, 2.3.6
Provided confirmation of the availability of the Senior Software Engineer for the final delivery phase as requested in the SoW	Book I 3.4.5.5 SoW 2.3.1
Provided proof that the proposed Senior Software Engineer Key Personnel for the final delivery phase fulfils all essential qualifications listed in the SoW Section 2.3.3 and 2.3.4	Book I 3.4.5.6, 3.4.5.7, SOW 2.3.3, 2.3.4
Provided confirmation of the availability of the Contractor Training SME as requested in the SoW	Book I 3.4.6.1 SoW 3.1.3.
Provided proof that the proposed Contractor Training SME Key Personnel fulfils all essential qualifications listed in the SoW Section 3.2	Book I 3.4.6.2, SOW 3.2

Table 1 – Criteria for Technical Evaluation

ANNEX A – BIDDING SHEETS

[Provided under separate MS Excel File:
*“02_RFQ-CO-115114-ETEE WP3 Portal Book I
Annex A Bidding Sheets FINAL”.*

ANNEX B - INSTRUCTIONS FOR THE PREPARATION OF BIDDING SHEETS

1. Bidders are required, in preparing their Price Quotation to utilise the Bidding Sheets following the instructions detailed in Section 3 – Bid Preparation Instructions and CLIN Bidding sheet instructions within the Bidding sheets itself.
2. Detailed instructions for preparation of the Bidding Sheets may be found in the MS Excel spreadsheet tab entitled “Instructions” of the RFQ file “02_RFQ-CO-115114-ETEE WP3 Portal Book I Annex A Bidding Sheets FINAL”.

ANNEX C – CERTIFICATES

This page is left blank intentionally

ANNEX C-1

This Bid 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: _____

TELEFAX No: _____

POINT OF CONTACT REGARDING THIS BID:

NAME: _____
POSITION: _____
TELEPHONE: _____

ALTERNATIVE POINT OF CONTACT:

NAME: _____
POSITION: _____
TELEPHONE: _____

Date

Signature of Authorised Representative

Printed Name

Title

Company

ANNEX C-2**CERTIFICATE OF INDEPENDENT DETERMINATION**

1. Each Bidder shall certify that in connection with this procurement:
 - a. This Bid has been arrived at independently, without consultation, communication or agreement, for the purpose of restricting competition, with any other Bidder or with any competitor;
 - b. The contents of this bid have not been knowingly disclosed by the Bidder and shall not knowingly be disclosed by the Bidder prior to award, directly or indirectly to any other Bidder or to any competitor, and
 - c. No attempt has been made, or will be made by the Bidder to induce any other person or firm to submit, or not to submit, a Bid for the purpose of restricting competition.

2. Each person signing this Bid shall also certify that:
 - a. He/she is the person in the Bidder's organisation responsible within that organisation for the decision as to the bid and that he/she has not participated and shall not participate in any action contrary to 1(a) through 1(c) above, or
 - b. (i) He/she is not the person in the Bidder's organisation responsible within that organisation for the bid but that he/she has 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 shall not participate in any action contrary to 1(a) through 1(c) above, and as their agent does hereby so certify, and
 - (ii) He/she has not participated and shall not participate in any action contrary to 1(a) through 1(c) above.

.....
Date

.....
Signature of Authorised Representative

.....
Printed Name and Title

.....
Company

ANNEX C-3

CERTIFICATE OF BID VALIDITY

I, the undersigned, as an authorised representative of the firm submitting this bid, do hereby certify that the pricing and all other aspects of our Bid shall remain valid for a period of nine (9) months from the Bid Closing Date of this Request for Quote.

.....
Date	Signature of Authorised Representative

	Printed Name and Title

	Company

ANNEX C-4

CERTIFICATE OF UNDERSTANDING

I certify that

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

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

.....
Date

.....
Signature of Authorised Representative

.....
Printed Name and Title

.....
Company

ANNEX C-5

CERTIFICATE OF EXCLUSION OF TAXES, DUTIES AND CHARGES

I hereby certify that the prices offered in the price quotation of this Bid 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 C-6

ACKNOWLEDGEMENT OF RECEIPT OF RFQ AMENDMENTS

I confirm that the following Amendments to Request for Quote No RFQ-CO-115114-ETEE have been received and the Bid as submitted reflects the content of such Amendments:

Amendment Number	Date Issued	Date of Receipt
[Bidder list all amendments here]		

.....
Date

.....
Signature of Authorised Representative

.....
Printed Name and Title

.....
Company

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

I, the undersigned, as an authorised representative of
.....(*insert Company Name*), certify the following statement:

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 NCIA as a condition of my firm's performance of the Contract, have been identified, as part of the Bid.
2. These supplemental agreements are listed as follows: [*Bidder Insert here any supplemental agreements or "N/A" if none*]
3. 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 or indicate n/a*). 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.
4. 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*).
5. 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 Bidder may be cause for the NCIA to determine the submitted bid to be non-compliant with the requirements of the RFQ.
- 6 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 C-8**CERTIFICATION OF NATO MEMBER COUNTRY ORIGIN OF
DELIVERED EQUIPMENT, SERVICES, MATERIALS AND
INTELLECTUAL PROPERTY RIGHTS**

The Bidder 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 C-9**COMPREHENSION AND ACCEPTANCE OF CONTRACT SPECIAL
PROVISIONS AND BOA PROVISIONS**

The Bidder hereby certifies that it has reviewed the Contract Special Provisions set forth in the Prospective Contract, Book II of this Request for Quote. The Bidder 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 Bidder additionally certifies that the offer submitted by the Bidder is without prejudice, qualification or exception to any of the Terms and Conditions and it shall accept and abide by the stated Special Contract Provisions and the BOA agreement provisions if awarded the contract as a result of this Request for Quote.

.....
Date.....
Signature of Authorised Representative.....
Printed Name and Title.....
Company

ANNEX C-10

LIST OF PROSPECTIVE SUB-CONTRACTORS/CONSORTIUM MEMBERS

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

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

I hereby certify that _____ (*insert Company name*)
possesses and applies Quality Assurance Procedures/Plans that are equivalent to
the AQAP 2110 or ISO 9001:2015 as evidenced through the attached
documentation¹.

A copy of the certification is attached herewith.

.....
Date

.....
Signature of Authorised Representative

.....
Printed Name and Title

.....
Company

¹ Bidders must attach copies of any relevant quality certification.

ANNEX C-12**LIST OF KEY PERSONNEL WITH SECURITY CLEARANCE INFORMATION**

Key Personnel Name	Level of NATO Clearance	Dates of Clearance Validity	National Certifying Authority	Expected date of obtaining the required Security Clearance

ANNEX C-13**Disclosure of Involvement of Former NCI Agency Employment**

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

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

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

- ☐ 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 in Excerpt of NCI Agency AD. 05.00, Code of Conduct dated May 2017):

Employee Name	Former NCIA Position	Current Company Position

The Bidder 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 :

Name & Title :

Company :

Bid Reference :

Excerpt of NCI Agency AD. 05.00, NCIA 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 bids / 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

- 17.1 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.
- 17.2 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 he/she was 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.

- 17.3 In addition to Section 17.2 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.
- 17.4 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.
- 17.5 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.
- 17.6 NCI Agency Personnel leaving the Agency shall sign a statement that they are aware of the post-employment measures set out in this Directive.
- 17.7 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 C-14**BIDDER BACKGROUND INTELLECTUAL PROPERTY RIGHTS (IPR)**

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

ITEM	DESCRIPTION
[Bidder list IPR or indicate "none"]	

The Bidder 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 6 of Prospective Contract Special Provisions.

ANNEX C-15**LIST OF 3rd PARTY INTELLECTUAL PROPERTY RIGHTS (IPR)**

The 3rd Party IPR specified in the table below will be used for the purpose of carrying out work pursuant to the Contract.

ITEM	DESCRIPTION
[Bidder list IPR or indicate "none"]	

The Bidder 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 Bidder's obligations under the Contract.

The 3rd Party IPR stated above complies with the terms specified in Article 6 of Prospective Contract Special Provisions.

ANNEX D – Bid-Requirements Cross Reference Matrix (BRCM)

Bidders shall provide the BRCM in Excel format according to the template “02B_RFQ-CO-115114-ETEE WP3 Portal Book I Annex D BRCM FINAL”.

Purpose: The BRCM is an instrument for the Bidder to cross-link the relevant sections of their technical proposal with the RFQ requirements, instructions and evaluation criteria. Bidders taking care to carefully and thoroughly complete the BRCM will ensure that all relevant sections of their proposal are taken into account during Purchaser evaluation and to ensure the best possible evaluation result.

The Sections 3.4.5 through 3.4.6 of the Bidding Instructions provide guidance on the build-up and content of the bid. The section 4.4.1 of the Bidding Instructions provide the criteria that will be applied for the evaluation of the bid. Both areas are relevant for the BRCM. The items already filled-in in the provided BRCM sheet is to ensure that Bidders have considered, at an absolute minimum, the traceability from the content requirements to the bid sections. Adding extra elaboration in the BRCM to reference the Section 4.4.1 of the Bidding Instructions and the specific requirements in the Statement of Work (SoW) provides extra granularity to the Purchaser for the traceability of RFQ requirements to your technical proposal.

The BRCM shall be completed as per the following instructions:

- **“Reference Document”**, the document from which the requirement is defined.
- **“Reference ID”**, the reference of the Section/requirement under consideration. The “Reference ID” column shall cover:
 - o “Bidding Instruction” references covering Sections 3.4.5 through 3.4.6 of this document. “Bidding Instruction” references shall be provided in the format [BI - #] where “#” represents the actual paragraph number.
 - o “SOW Requirement” references covering all ‘shall’ statement of the SOW. Requirement References shall be provided in the following format:
 - § For the SOW: [SOW - #] where “#” represents the actual requirement (i.e. paragraph) number
- **“Description”**: the actual text of the Section/requirement under consideration.
-
- **“Bid Reference”** indicating where in their Bid the associated Bid Instruction Reference and/or SOW Requirement Reference is/are addressed. Bid Reference shall be provided in the form “Doc # - Section #”

- **“Remarks”**, as applicable. The column “Remarks” might be used by the Bidders to provide a brief description of how the Bidder meets the requirement, to facilitate the reading, but any such descriptions will not form part of the formal evaluation.
- **“Compliance statement”**: the way and extent the Bid covers and complies with the Section/requirement under consideration, using the following classifications:
 - **“Provided/Detailed”**: The Bidder states providing a document or details at the mentioned reference. Such a classification is expected for all BIs and the majority of the SOW and SOW Annexes requirements.
 - **“Partial”**: The Bidder states fulfilling the requirement but only describes part of it. Such a classification is expected only for a small number of SOW and SOW Annexes requirements.

One copy of the duly completed BRCM shall be included in the Technical Proposal Package.

As noted in *“Purpose”* above, Bidders shall note that, to facilitate the bidding process, the BRCM template already contains the core of Book I (BI) and associated descriptions in the columns “Reference ID” and “Description” respectively. However, it is the Bidders’ sole responsibility to ensure that all BI references (together with SOW references) are properly addressed and complete in the BRCM.

ANNEX E – Clarification Request Forms

INSERT COMPANY NAME

HERE INSERT SUBMISSION

DATE HERE

ADMINISTRATION or CONTRACTING			
Serial Nr	RFQ Book	RFQ Section Ref.	QUESTION
A.1			
A.2			
A.3			

INSERT COMPANY NAME HERE

INSERT SUBMISSION DATE HERE

PRICE			
Serial Nr	RFQ Book	RFQ Section Ref.	QUESTION
P.1			
P.2			
P.3			

INSERT COMPANY NAME

HERE INSERT SUBMISSION

DATE HERE

TECHNICAL			
Serial Nr	RFQ Book	RFQ Section Ref.	QUESTION
T.1			
T.2			
T.3			

ANNEX F – RESERVED

CO-115114-ETEE



NATO Communications and Information Agency
Agence OTAN d'information et de communication

PROSPECTIVE CONTRACT

RFQ-CO-115114-ETEE

**PROVISION OF BALLISTIC MISSILE DEFENCE INFORMATION
MANAGEMENT PORTAL WITHIN EDUCATION, TRAINING, EXERCISE
AND EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

NATO UNCLASSIFIED

Book II – The Prospective Contract
RFQ-CO-115114-ETEE

Page Intentionally Left Blank

NATO UNCLASSIFIED

SIGNATURE SHEET

NCI Agency PURCHASE ORDER	
1. Original Number ___ of	2. PO Number : [TBD]
3. Contract Number: CO-115114-ETEE	4. Effective date (EDC): SEE BLOCK 17
5. Contractor: [TBD]	6. Purchaser: The General Manager NATO Communications and Information Agency Boulevard Leopold III B-1110 Bruxelles Tel: +32(0)2 707 8282 Fax: +32(0)2 707 87.70
7. CONTRACT SCOPE: This is a Contract for the provision of a BMD Information and Management Portal within ETEE Functional Services, to be delivered in accordance with the terms and conditions specified herein.	
8. TOTAL AMOUNT OF CONTRACT : _____ Currency – Excluding VAT Firm Fixed Price	
9. PERIOD OF PERFORMANCE As stated in Schedule of Supplies and Services and Special Provisions	10.DELIVERY SITE As stated in Schedule of Supplies and Services and Special Provisions
11.CONTRACT This Contract consists of the following parts and named documents: a) Part I. Schedule of Supplies and Services b) Part II. Special Contract Provisions and Annexes c) Part III. Statement of Work and Annexes d) NCI Agency Basic Ordering Agreement General Provisions and Appendix 1, of the Basic Ordering Agreement NCIA/BOA/XXXXXX XX Month 20xx, incorporated herein by reference. e) In the event of any conflict or inconsistencies between or among any of the documents comprising this Contract, the order of priority specified in Clause 2 of Part II shall apply.	
12. Signature of Contractor	13. Signature of Purchaser
14. Name and Title of Signer	15. Name and Title of Signer
16. Date signed by the Contractor	17. Date signed by the Purchaser

NATO UNCLASSIFIED

Book II – The Prospective Contract
RFQ-CO-115114-ETEE

Page Intentionally Left Blank

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Book II – The Prospective Contract
RFQ-CO-115114-ETEE

TABLE OF CONTENTS

1. Part I, Schedule of Supplies and Services
2. Part II, Contract Special Provisions
3. Part III, Statement of Work & Annexes

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Book II – The Prospective Contract
RFQ-CO-115114-ETEE

Page Intentionally Left Blank

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Book II – The Prospective Contract
RFQ-CO-115114-ETEE



CO-1115114-ETEE

**PROVISION OF BALLISTIC MISSILE DEFENCE (BMD) INFORMATION
MANAGEMENT PORTAL WITHIN EDUCATION, TRAINING, EXERCISE
AND EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

**PART I - CONTRACT SCHEDULES OF SUPPLIES AND
SERVICES**

NATO UNCLASSIFIED



NATO Communications and Information Agency
Agence OTAN d'information et de communication

**PROVISION OF BALLISTIC MISSILE DEFENCE (BMD)
INFORMATION MANAGEMENT PORTAL WITHIN
EDUCATION, TRAINING, EXERCISE AND EVALUATION
(ETEE) FUNCTIONAL SERVICES (FS)**

RFQ-CO-115114-ETEE WP3

BOOK II - PART II

CONTRACT SPECIAL PROVISIONS

This Page Intentionally left blank

TABLE OF CONTENTS

1.	DEFINITIONS.....	2
2.	SCOPE.....	2
3.	PARTICIPATING COUNTRIES.....	3
4.	CONTRACT ADMINISTRATION.....	3
5.	SECURITY	4
6.	INTELLECTUAL PROPERTY	5
7.	INTELLECTUAL PROPERTY RIGHT INDEMNITY AND ROYALTIES	6
8.	ROLES AND RESPONSIBILITIES IN AGILE/SCRUM PROCUREMENT	6
9.	INDEMNITY.....	7
10.	KEY PERSONNEL AND CONTRACTOR TEAM ADEQUACY	7
11.	OWNERSHIP AND TITLE	9
12.	ORDER OF PRECEDENCE.....	9
13.	ACCEPTANCE PROCEDURES – AGILE DEVELOPMENT	10
14.	INVOICES AND PAYMENT	10
15.	FORCE MAJEURE.....	11
16.	INDEPENDENT CONTRACTOR	11
17.	PRICING OF CHANGES, AMENDMENTS AND CLAIMS	12
18.	RESERVED.....	12
19.	WARRANTY.....	12
20.	SUPPLEMENTAL AGREEMENT(S), DOCUMENTS AND PERMISSIONS	12
21.	CONFLICT OF INTEREST.....	13
22.	THIRD PARTIES.....	14
23.	TECHNICAL DIRECTION	15
24.	NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR MANDATED NATO THIRD PARTY AUDITS	15

1. DEFINITIONS

- 1.1 For the purpose of this contract and unless otherwise explicitly indicated, the following definitions shall apply:
- 1.2 Acceptance: The act of an authorized representative of the Purchaser by which the Purchaser assumes title and ownership of delivered Works rendered as partial or complete performance of the Contract. "Acceptance" in this regard, unless specifically provided otherwise in the Contract Special Provisions, means final Acceptance where the Contract provides for Provisional or Partial Acceptance.
- 1.3 Basic Ordering Agreement (BOA): Means the separate agreement the Contractor holds with the NCI Agency under the auspices of the NCI Agency BOA Program.
- 1.4 Contracting Authority: The General Manager of the NCI Agency, the Director of Acquisition of the NCI Agency, the Chief of Contracts of the NCI Agency or the authorised representatives of the Chief of Contracts of the NCI Agency.
- 1.5 Contractor: The person or legal entity from a Participating Country which has signed this Contract and is a Party thereto.
- 1.6 General Provisions: Means the General Provisions contained in the Contractor's BOA.
- 1.7 Person Day: Means eight (8) hours of effort by Contractor's personnel, to be performed during the project's normal business hours as defined by the Purchaser's authorized representative.
- 1.8 Purchaser: NCI Agency, as represented by the General Manager, NCI Agency. The Purchaser is the legal entity who awards and administers the Contract and stands as one of the Contracting Parties.

2. SCOPE

- 2.1 The purpose of this Contract is to obtain the provision of services to deliver and implement a Ballistic Missile Defense (BMD) Information Management (IM) portal template system that fits into the NATO portal environment and that is configured to meet the Education, Training, Exercise and Evaluation (ETEE) Functional Services (FS) requirements.
- 2.2 This Contract covers all performance and deliverables necessary to design, implement, and support the capability.

3. PARTICIPATING COUNTRIES

- 3.1 The following NATO member nations have agreed to fund this acquisition effort: (in alphabetical order): ALBANIA, BELGIUM, BULGARIA, CANADA, CROATIA, CZECH REPUBLIC, DENMARK, ESTONIA, FRANCE, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, MONTENEGRO, THE NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TURKEY, THE UNITED KINGDOM and THE UNITED STATES.
- 3.2 The Contractor may issue sub-contracts to firms and purchase from qualified vendors in any participating NATO Nation. None of the work, including project design, labour and services, shall be performed other than by firms from and within participating countries, as per NATO policy.
- 3.3 The Contractor shall notify in writing to the Purchaser immediately upon being informed of any change in the nationality of its Subcontractor(s) which would prevent the Contractor from further complying with Clause 3.3 above. Upon receipt of this information from the Contractor, the Purchaser may, within three months from this notification, require the Contractor to find an alternate subcontractor, complying with the requirements set out in Clause 3.2 above.
- 3.4 Unless authorized by NATO Policy, no material or items of equipment down to and including identifiable sub-assemblies delivered under this Contract shall be manufactured or assembled by a firm other than from and within a participating country.
- 3.5 The Intellectual Property Rights to all designed documentation and system operating software shall reside in participating 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 community.

4. CONTRACT ADMINISTRATION

- 4.1 The Purchaser is the NATO CI Agency (NCI Agency). The Purchaser 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.
- 4.2 All notices and communications between the Contractor and the Purchaser shall be written and conducted in English.
- 4.3 Formal letters and communications shall be personally delivered or sent by mail, registered mail, email, courier or other delivery service, to the official points of contact quoted in this Contract.

4.4 Informal notices and informal communication for normal project management may be exchanged by any other means, including telephone.

4.5 All notices and communication shall be effective upon receipt.

4.6 Official Points of Contact are:

Purchaser	Contractor
NCI Agency	
For contractual matters: Attn: Mr Peter Kowalski Senior Contracting Officer E-mail: Peter.Kowalski@ncia.nato.int	For contractual matters: Attn: Tel: E-mail:
For technical/project management matters: Attn. Senior Project Manager Tel: E-mail:	For technical/project management matters: Attn: Project Manager Tel: E-mail:

5. SECURITY

5.1 The Contractor is responsible, in accordance with NATO and National Security regulations, for the proper handling, storage and control of any classified documents and information as may be furnished to the Contractor in relation to the performance of the present contract.

5.2 The security classification of this contract is "NATO UNCLASSIFIED".

5.3 Contractor's personnel working in the execution of this contract shall hold and maintain a NATO SECRET security clearance valid for the duration of the Contract. This requirement applies to all sub-contracts issued by the Contractor for the effort under this prime Contract.

5.4 The Contractor's facilities shall hold and maintain a facility clearance to permit handling and storage of information classified up to and including NATO RESTRICTED.

- 5.5 It is the responsibility of the Contractor to ensure that his 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.
- 5.6 The Contractor is advised that the personnel security clearance 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.
- 5.7 Failure of the Contractor to obtain proper security clearances to perform the work under this contract, and to have access to any NATO sites to perform the work, and any attendant delay in the project which results from this access refusal, is not the basis for excusable delay under the terms of the contract concerning default. The Contractor bears full responsibility and liability under the contract for delays arising from the failure of the Contractor to adhere to the security requirements.
- 5.8 In the absence of valid security clearances for the Contractor's personnel and facility, the Purchaser reserves the right to terminate the Contract for "Default".
- 5.9 The Contractor shall note that there are restrictions regarding the carriage and use of electronic devices (e.g. laptops, cellular phones, smart-phones and the like) in NATO designated Security Areas. The Contractor shall be responsible for satisfying and obtaining from the appropriate NATO Authorities the necessary clearance to introduce and utilize any such equipment into the facility.

6. INTELLECTUAL PROPERTY

- 6.1 All rights arising out of the results of work undertaken by or on behalf of the Purchaser for the purposes of this Contract, including any and all technical data specifications, reports, drawings, computer software data, computer programmes, computer databases, computer software, computer source code, documentation including software documentation, design data, specifications, instructions, test procedures, training material, produced or acquired in the course of such work and, in particular, all rights, including copyright therein, shall from its creation vest in and be the sole and exclusive property of the Purchaser in both object and source code.
- 6.2 The Purchaser will accept no constraints or limitations on the use of Contract deliverables. Accordingly, the Contractor shall not include any Background Intellectual Property or third party software in the code provided to the Purchaser. In the event that any such code would have to be included, the Contractor shall seek Purchaser's prior agreement and ensure that unlimited rights are secured for the Purchaser to use the deliverables under the Contract.

7. INTELLECTUAL PROPERTY RIGHT INDEMNITY AND ROYALTIES

- 7.1 The Contractor shall assume all liability and indemnify the Purchaser, its officers, agents and employees against liability, including costs for the infringement of any patents or copyright in force in any countries arising out of the manufacture, services performed or delivery of supplies, or out of the use or disposal by or for the account of the Purchaser of such supplies. The Contractor shall be responsible for obtaining any patent or copyright licences necessary for the performance of this Contract and for making all other arrangements required to indemnify the Purchaser from any liability for patent or copyright infringement in said countries.
- 7.2 The Contractor shall exclude from his prices any royalty pertaining to patents which in accordance with agreements reached between NATO countries may be utilised free of charge by member nations of NATO and by NATO organisations.
- 7.3 The Contractor shall report in writing to the Purchaser during the performance of this Contract:
- 7.3.1 The royalties excluded from his price for patent utilised under the agreements mentioned in the Para 7.3 above;
- 7.3.2 The amount of royalties paid or to be paid by the Contractor directly to others in performance of this Contract.

8. ROLES AND RESPONSIBILITIES IN AGILE/SCRUM PROCUREMENT

- 8.1 The Purchaser and Contractor will work collaboratively using roles and elements of agile/Scrum development to execute the project and achieve all stated effort using the methodology described in the Contract Statement of Work.
- 8.2 Agile development is a software development approach based on iterative development, early and frequent inspection, and incremental deliveries in which user stories and solutions evolve through collaboration in cross-functional teams and through continuous stakeholder feedback. All user epic software requirements stated in this Contract are a guidance for the volume of the required end product. The actual delivery will be based on the required and allocated effort levels as described in the Contract Statement of Work.
- 8.3 Neither the Purchaser's Project Manager, nor the Integrated Project Management Team or any other NATO personnel, other than the Purchaser's Contracting Authority, is authorized to make changes to any part of the Contract.

- 8.4 The Purchaser's Project Manager may provide guidance and direction to the Contractor related to the methodology, planning, review, integration and prioritization of requirements as detailed in the Contract Statement of Work, Part II, "Task 1: Software Engineering" and "Task2: Training Material".

9. INDEMNITY

- 9.1 The Contractor will indemnify and hold harmless NATO, its servants or agents, against any liability, loss or damage arising out of or in connection of the Supplies and Services under this Contract, including the provisions set out in Clause 22, "Patent and Copyright Indemnification" of the BOA General Provisions.
- 9.2 The parties will indemnify each other against claims made against the other by their own personnel, and their Subcontractor/Subcontractors (including their personal representatives) in respect of personal injury or death of such personnel or loss or destruction of or damage to the property of such personnel.
- 9.3 NATO will give the Contractor immediate notice of the making of any claim or the bringing of any action to which the provisions of this Clause may be relevant and will consult with the Contractor over the handling of any such claim and conduct of any such action and will not without prior consultation and without the consent of the Contractor settle or compromise any such claim or action.
- 9.4 In the event of an accident resulting in loss, damage, injury or death arising from negligence or wilful intent of an agent, officer or employee of NATO for which the risk has been assumed by the Contractor, the cause of the accidents will be investigated jointly by the Parties and the extent to which NATO will be liable to recompense the Contractor will be determined together.
- 9.5 This indemnification applies only to the extent that the claim is not compensated for by insurance or otherwise.

10. KEY PERSONNEL AND CONTRACTOR TEAM ADEQUACY

- 10.1 The individuals listed below are considered to be key to the performance of this contract and shall not be replaced by the Contractor with substitute personnel without the prior written approval of the Purchaser. The Key Personnel are as follows:

POSITION	NAME
Senior Software Engineer (Intermediate Delivery Phase)	[TBD]
Software Engineer 1 (Intermediate Delivery Phase)	[TBD]
Software Engineer 1 (Intermediate Delivery Phase)	[TBD]
Senior Software Engineer (Final Delivery Phase)	[TBD]
Training SME	[TBD]

- 10.2 In such cases where the services of the Key Personnel are lost to the Contractor beyond the reasonable control of the Contractor (e.g., resignation, sickness, incapacity, etc.), the Contractor must nominate a substitute(s) of equivalent or higher qualification and experience within 15 working days of the date at which the Contractor has knowledge of the loss of service of such key personnel. The replacement personnel shall be in place within a reasonable time.
- 10.3 If the Contractor is unable to nominate and/or replace the lost personnel within the timeframe mentioned in 10.2 above, the Purchaser may conclude that the loss of the Key Personnel endangers progress under the Contract to the extent that the Purchaser may resort to the Clause 19 – “Termination for Default” of the Contract BOA General Provisions for redress of the situation.
- 10.4 The Purchaser has the right to refuse any proposed substitution if not meeting the qualifications and request the Contractor to offer another qualified individual in lieu thereof. The Purchaser will confirm any consent given to a substitution in writing and only such written consent shall be deemed as valid evidence of Purchaser consent.
- 10.5 The Purchaser reserves the right, even after acceptance of Contractor personnel on the basis of his/her CV and/or interview, to require the Contractor immediately to cease to employ any Key Personnel under the present contract if, in the sole opinion of the Purchaser, the individual is not meeting the required level of competence and/or his/her employment as Key Personnel is considered undesirable. The Purchaser will inform the Contractor, in writing, in cases where such a decision is taken and the Contractor shall propose and make qualified substitute Key Personnel available within 15 working days after the written notification. The Purchaser's removal of Contractor Key Personnel shall in no way relieve the Contractor of his responsibility to achieve the contractual and

technical requirements of this Contract nor imply any responsibility of the Purchaser.

- 10.6 The Contractor shall guarantee that suitable backup personnel will be available to promptly remedy situations of key personnel non-availability that may endanger the performance of services or Deliverables set in the Contract.
- 10.7 The Contractor shall provide and maintain an adequately sized and appropriately skilled agile development team, to include, but not limited to, the personnel listed in Para 10.1, to meet the requirements of the Contract. If The Contractor fails to do so, the Purchaser may terminate this Contract in whole or in part as provided in Clause 19 (“Termination for Default”) of the BOA General Contract Provisions, and in that event the Contractor shall be liable, in addition to the excess costs provided in Clause 18, “Liquidated Damages” of these Special Provisions, for such liquidated damages accruing until such time as the Purchaser may reasonably obtain delivery or performance of similar services.

11. OWNERSHIP AND TITLE

- 11.1 Ownership and title for all works conducted under the agile/Scrum software development portion of this contract, including any and all technical data specifications, reports, drawings, computer software data, computer programmes, computer databases, computer software, computer source code, documentation including software documentation, design data, specifications, instructions, test procedures, training material produced or acquired in the course of such work, shall from its creation, pass to the Purchaser, in both object and source code.
- 11.2 Ownership and title to all deliverables not covered under Para 11.2 above shall pass to the Purchaser upon written notification of acceptance by the Purchaser but at the latest on Final Contract Acceptance.

12. ORDER OF PRECEDENCE

- 12.1 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 as follows:
- a. The Signature Page
 - b. The Contract Schedules
 - c. These Contract Special Provisions
 - d. Basic Ordering Agreement NCIA/BOA/XXXXX dated XX Month 20XX, incorporated by reference
 - e. The Statement of Work
 - f. The Annexes to the Statement of Work

13. ACCEPTANCE PROCEDURES – AGILE DEVELOPMENT

- 13.1 “Acceptance” is the action by which the Purchaser formally acknowledges that the Contractor has fully demonstrated that the sprints and subsequent baseline releases, or individual CLINs, are “complete” in accordance with the criteria and definitions in Section 2 and Section 3 of the Statement of Work, and that Contract Deliverables are complete or have been performed according to the requirements set forth.
- 13.2 Contract payment milestones, as designated in the Schedule of Supplies and Services, shall only be considered as complete and eligible for payment when all milestone entry and exit criteria, and any works or events as defined in this contract as associated and underlying the payment milestone has been formally delivered in both object and source code and acknowledged as completed by the Purchaser. Payment milestones shall only be considered as confirmed and fully achieved when the Purchaser has advised the Contractor formally in writing that all conditions necessary for milestone completion have been successfully met.

14. INVOICES AND PAYMENT

- 14.1 No payment shall be made with respect to undelivered supplies; works not performed, services not rendered and/or incorrectly submitted invoices.
- 14.2 The Contractor shall be entitled to submit invoices as shown in the “Milestones and Payment” Tab in the Schedule of Supplies and Services.
- 14.3 Evidence of the acceptance by the Purchaser shall be attached to all invoices.
- 14.4 The Purchaser is released from paying any interest to the Contractor resulting from any reason whatsoever.
- 14.5 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:
- 14.5.1 Contract number CO-115114-ETEE
- 14.5.2 Purchase Order numbers: **[TBD]**;
- 14.5.3 Contract Amendment number (if any);
- 14.5.4 Contract Line Item(s) (CLIN) as they are defined in the priced Schedule of Supplies and Services

14.5.5 Bank Account details for international wire transfers.

- 14.6 The invoice shall contain the following certificate: “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.” The certificate shall be signed by a duly authorised company official on the designated original.
- 14.7 Invoices referencing “CO-115114-ETEE/ PO [TBD] shall be submitted in electronic format to: accountspayable@ncia.nato.int, with an electronic copy to the Purchaser’s Contracting Officer at the email address specified at the Para 4.6 of these Special Contract Provisions.
- 14.8 The Purchaser shall make payment within 45 days of receipt by NCI Agency of a properly prepared and documented invoice.

15. FORCE MAJEURE

- 15.1 If the performance of this Contract, or any obligation hereunder is prevented, restricted or interfered with by reason of fire, flood, earthquake, explosion or other casualty or accident, strikes or labour disputes, war or other violence, including acts of terrorism, any law, order, proclamation, regulation, ordinance, demand or requirement of any governmental agency, or any other act, event or condition whatsoever beyond the reasonable control of the affected Party, the Party so affected, upon giving prompt notice to the other Party, shall be excused from such performance to the extent of such prevention, restriction or interference, provided, however, that the Party so affected shall take all reasonable steps to avoid or remove such cause of non-performance and shall resume performance hereunder with dispatch whenever such causes are removed.

16. INDEPENDENT CONTRACTOR

- 16.1 The Personnel provided by the Contractor 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.
- 16.2 It is the sole responsibility of the Contractor to ensure their employees, subcontractors, and any other person assigned for the implementation of this contract are acting in full accordance with applicable national law, to include without limitation work permits, residence permits, tax and social legislation obligations, driving permits, etc. Contractor staff performing under this Contract are not eligible for any privileges & immunities or NATO employee benefits.

17. PRICING OF CHANGES, AMENDMENTS AND CLAIMS

- 17.1 Contractor's pricing proposals for Changes, Amendments and Claims shall be priced in accordance with the schedules of forward labour rates which were submitted in the Contractor's bid incorporated in the Contract by reference;
- 17.2 The Contractor shall be bound by the stated labour rates for the entire duration of this Contract;

18. RESERVED**19. WARRANTY**

- 19.1 The Contractor warrants to the Purchaser that all deliverables furnished hereunder will be merchantable, free from defects in design, material and workmanship, fit and sufficient for the purposes intended by the Purchaser, free from all liens and encumbrances and will strictly conform to and perform in accordance with applicable specifications, drawings and samples for a period of 12 months starting from final contract acceptance.
- 19.2 The Contractor also warrants to the Purchaser that any Services provided hereunder will be performed to the best practices of the Contractor's profession or industry, in a professional and well organized manner, in strict compliance with the specifications, and with care, skill, and diligence. If the Contractor fails to meet applicable professional standards, the Contractor will, without additional compensation, promptly correct or revise any errors or deficiencies in the services furnished hereunder.

20. SUPPLEMENTAL AGREEMENT(S), DOCUMENTS AND PERMISSIONS

- 20.1 If any supplemental agreements, documents and permissions are introduced after Contract award, the execution of which by the Purchaser is/ are required by national law or regulation, and it is determined that the Contractor failed to disclose the requirement for the execution of such agreement from the Purchaser prior to Contract signature, the Purchaser may terminate this Contract for Default, in accordance with Clause 19 (Termination for Default) of the Contract BOA General Provisions.
- 20.2 Supplemental agreement(s), documents and permissions, the execution of which by the Purchaser is/are required by national law or regulation and that have been identified by the Contractor prior to the signature of this contract, but have not yet been finalised and issued by the appropriate governmental authority, are subject to review by the Purchaser. If such supplemental agreement(s), documents and permissions are contrary to cardinal conditions of the signed contract between the Parties, and the Purchaser and the appropriate governmental authority cannot reach a mutual satisfactory resolution of the

contradictions, the Purchaser reserves the right to terminate this contract and the Parties agree that in such case the Parties mutually release each other from claim for damages and costs of any kind, and any payments received by the Contractor from the Purchaser will be refunded to the Purchaser by the Contractor.

21. CONFLICT OF INTEREST

- 21.1 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.
- 21.2 The Contractor is responsible for maintaining and providing up-to-date conflict of interest information to the Purchaser. If, after award of this Contract or task order 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 as set forth below.
- 21.3 If, after award of this Contract herein, the Purchaser discovers a conflict of interest with respect to this Contract or task order, 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 19 (Termination for Default) of the Contract BOA General Provisions.
- 21.4 The Contractor's notice called for in Para 22.2 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 in analysing the situation. Any changes to the Contractor's Conflict of Interest Mitigation Plan, if any is incorporated in the contract, should be also detailed.
- 21.5 The Contractor has the responsibility of formulating and forwarding a proposed mitigation plan to the Purchaser, for review and consideration. This responsibility

arises when the Contractor first learns of an actual, apparent, or potential conflict of interest.

- 21.6 If the Purchaser 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 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 has the discretion to terminate the Contract for default or alternatively refrain from exercising any further Option or Work Package under the contract.
- 21.7 The Contractor's misrepresentation of facts in connection with a conflict of interest reported or a Contractor's failure to disclose a conflict of interest as required shall be a basis for default termination of this contract
- 21.8 With the aim to prevent an organizational conflict of interest in industrial roles under the BMD Functions in ETEE Functional Services project, the Contractor and their prospective Sub-Contractors shall be excluded from participation of any kind in the companion NCI Agency project under contract CO-115115-ETEE entitled "*BMD Functions In ETEE FS - WP4 Operational Assurance & Test*".

22. THIRD PARTIES

- 22.1 The Contractor shall be aware of and support the need to work closely with and participate in meetings and reviews to be held jointly with third parties who perform work which contributes to, or is strongly related to, work conducted under this Project. This will include, but not be limited to, working with and exchanging data under a data processing arrangement with the Contractor chosen to perform the Operational Assurance Work Package for the ETEE FS project. Such Contractor work with third parties is inherent in the existing contract scope and the industrial structure of the overall ETEE FS project implementation.
- 22.2 The Contractor shall have no rights to raise claims, ask for excusable delays or interrupt the performance of the Contract on the basis of, or in connection with, his responsibilities to work/co-ordinate with third parties running work on or related to this Project.
- 22.3 The above described effort is already included in the Total Firm Fixed price of this Contract and the Contractor shall have no recourse for additional costs, claims, or delays in the performance of this Contract on the basis of the above described effort.

- 22.4 The Purchaser reserves the right to make technical documentation produced under this Contract, even in draft version, available to any third parties.

23. TECHNICAL DIRECTION

- 23.1 The Contract will be administered by the Purchaser in accordance with the Clause 4 of these Contract Special Provisions entitled “Contract Administration”.
- 23.2 The individuals working on this Contract shall perform the effort within the general scope of work identified in the Contract Part III - Statement of Work (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.
- 23.3 The Purchaser reserves his 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.
- 23.4 Neither the Purchaser’s Project Manager as identified in Clause 4 of these Contract Special Provisions, nor any Technical Representative, nor any Third Party as mentioned in Clause 22 above, 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 products and services 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 under the authority of the Contract shall render any subsequent claim null and void.
- 23.5 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.

24. NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR MANDATED NATO THIRD PARTY AUDITS

- 24.1 Definitions. As used in this clause:

- 24.1.1 “*Resource Committees*” means committees under the North Atlantic Council (NAC) that are responsible, within the broad policy guidance provided by the Resource Policy and Planning Board (RPPB) on matters of resource allocation, for the implementation of the NATO Security Investment Programme (NSIP) or Budget/Civil budgets.
- 24.1.2 “*Mandated Third Party Audits*” means audits mandated by a resource committee.
- 24.1.3 “*Third Party Auditor*” means an independent, external audit body for NATO such as the International Board of Auditors for NATO (IBAN) or an appointed private contractor (including its experts, technical consultants, subcontractors, and suppliers) providing audit support under a Resource Committee Appointment based on an agreed mandate.
- 24.1.4 “Sensitive information” means information of a commercial, financial, technical, proprietary, or privileged nature. The term does not include information that is lawfully, publicly available without restriction. Third Party Audits” means audits mandated by a resource committee.
- 24.2 The Purchaser may disclose to a mandated third party auditor, for the sole purpose of audit support activities, any information, including sensitive information, received - (1) within or in connection with a bid, quotation or offer; or, (2) in the performance of or in connection with a contract.
- 24.3 Flowdown. Include the substance of this clause, including this paragraph, in all subcontracts, including subcontracts for commercial items.

THIS PAGE INTENTIONALLY LEFT BLANK



NATO Communications and Information Agency
Agence OTAN d'information et de communication

**PROVIDE BMD EXERCISE INFORMATION MANAGEMENT PORTAL
TEMPLATE SYSTEM WITHIN BALLISTIC MISSILE DEFENCE (BMD)
FUNCTIONS IN EDUCATION, TRAINING, EXERCISE AND
EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

RFQ-CO-115114-ETEE PORTAL

**BOOK II – PART III
STATEMENT OF WORK**

Table of Contents

1. Introduction.....	3
1.1. Introduction to the ETEE FS BMD Project:	3
1.2. Purpose and Scope of this Contract.....	5
1.3. Statement of Work Organization.....	5
1.4. High-level Contract Requirements.....	6
1.5. Contract Requirements	7
2. Task 1: Software Engineering (CLIN 1).....	7
2.1. Scope	7
2.2. Software Engineering Start Date and Schedule.....	7
2.3. Software Engineering Team requirements.....	8
2.4. BMD ETEE IM Portal Template System requirements.....	9
2.5. Purchaser Responsibilities.....	9
2.6. Software development methodology	9
2.7. Software implementation location of work, environment and tools (CLIN 3)	10
2.8. Software development configuration management.....	11
2.9. Software implementation and Test plan	12
2.10. Test scenario data.....	13
2.11. Cyber Security requirements	13
2.12. Quality assurance.....	13
2.13. Coding principles and guidelines	13
2.14. On-line Help	13
2.15. Contribution to training for system administrators.....	14
2.16. Prohibition of Software licenses	14
3. Task 2: Training Material (CLIN 2 and CLIN 3)	14
3.1. Scope	14
4. Definitions.....	15
ANNEX A: Software Requirement Specifications	17
ANNEX B: Technology and non-functional requirements.....	17
ANNEX C: Coding principles and guidelines	17
ANNEX D: Purchaser Furnished Property	17

1. Introduction

1.1. Introduction to the ETEE FS BMD Project:

1.1.1. The Education, Training, Exercises and Evaluation Functional Services (ETEE FS) Ballistic Missile Defence (BMD) project is included in the Capability Package CP 0A1303 Revision 1 “*Provide Ballistic Missile Defence Capabilities.*” It will provide collective training and exercise capabilities to the BMD community for the preparation, conduct and analysis of their weekly training and of their periodic exercises. All stages of the Collective training and exercises process defined in the BI-SC Directive 75-3 will be supported.

1.1.2. The ETEE FS BMD will be used by BMD exercise planners and BMD Exercise Control Organisations located at Headquarters Air Command (HQ AIRCOM), Combined Air Operations Centre (CAOC) Torrejón, CAOC Uedem and Supreme Headquarters Allied Powers Europe (SHAPE) to plan and conduct BMD exercises in close coordination with national BMD organisations. It will provide an integrated tool suite based on existing and proven software that will remain in use in other NATO Command Structure (NCS) and NATO Force Structure (NFS) commands: JEMM (Joint Exercise Management Module) and ITC (Integrated Training Capability).

1.1.3. The aim of the overarching ETEE FS BMD project is to provide an enhanced JEMM system, an Air and Missile Defence (AMD) simulation system including simulation federation management on the basis of ITC and a BMD Exercise Information Management Portal Template system. A specific Work Package for each of these systems is a part of the ETEE FS BMD project. The Work Packages for the systems are numbered 1 through 3. The scope of this Contract is only for Work Package Number 3. In addition the ETEE FS BMD project includes a fourth Work Package that will support the operational assurance of the systems that are delivered through testing and integration as well as Hand-over to the User, training and mentoring.

1.1.4. The ETEE FS JEMM, ITC/AMD and Portal systems aim to provide a logical grouping of functionality from a User perspective which are referred to as User Applications as shown in Figure 1.1.

1.1.5. The interactions between the systems are shown in Figure 1.1

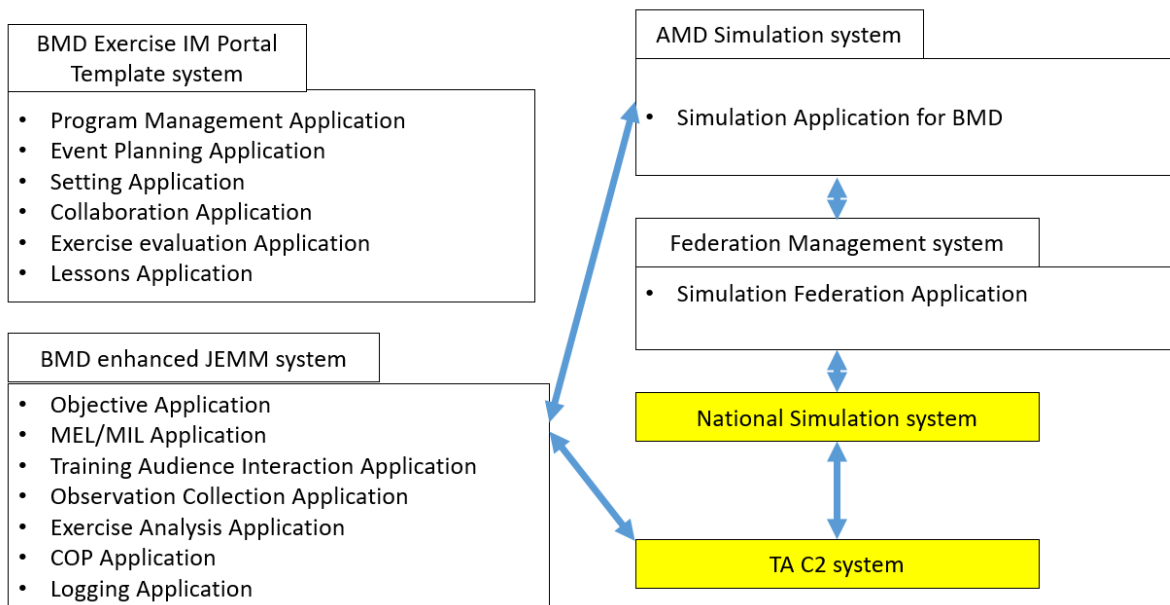


Figure 1.1 System Interaction Diagram

1.1.6. As the JEMM and ITC/AMD systems are already in operational use in the NATO command structure and will remain under maintenance during the period of performance of the ETEE FS BMD project, the Purchaser will act as the integrator of the software delivered by Work Packages 1 and 2 into the existing and evolving system baselines.

1.1.7. The ETEE FS BMD overarching project schedule is shown in Figure 1.2. It should be noted that the project will be executed in two phases. Phase 1 aims to produce an intermediate delivery after twelve (12) to eighteen (18) months which includes the associated acceptance tests: Factory Acceptance Test (FAT), System Integration Test (SIT), User Acceptance Test (UAT) and Site Acceptance Test (SAT). The intermediate and the final delivery are both intended to meet all the software requirements of the systems. The second delivery aims to refine the first based on the feedback from actual usage and on insights gained during the development of the first delivery. In addition, the ETEE FS BMD project will contribute to the BMD Programme Tranche defined Integration Tests, such as the Ensemble Test (ET), the Ensemble Operator Test (EOT) and the System of Systems Integration Test (SoSIT). For Work Package 3, the object of this Contract, the intermediate delivery is scheduled to take place 12 months after the Effective Date of Contract (EDC) for WP3. The final delivery is scheduled to take place 12 months after the intermediate delivery.

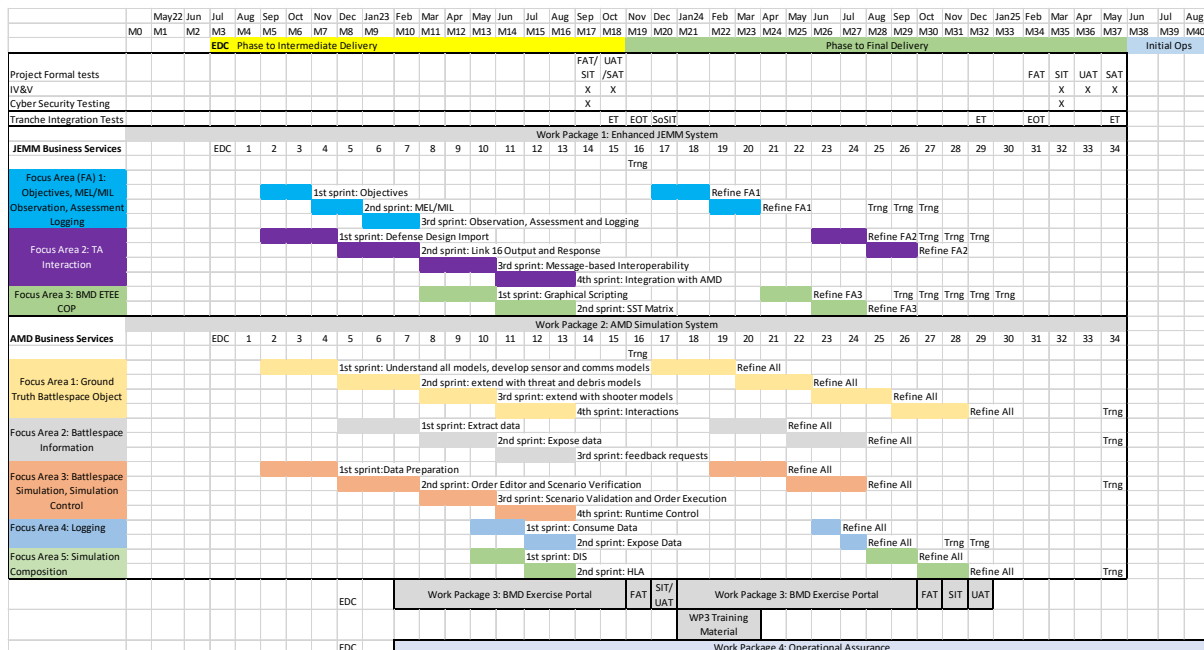


Figure 1.2: Project Schedule

1.1.8. The WP3 BMD Exercise IM Portal Template system will be deployed on NATO operational networks and is therefore required to comply with NATO cyber security regulations and NATO portal guidelines.

1.2. Purpose and Scope of this Contract

1.2.1. The purpose and scope of this Contract for ETEE WP3 is to implement the BMD Exercise IM Portal Template system to meet the BMD requirements for exercise portals.

1.2.2. The Contract will be executed using the roles and responsibilities as defined by the Scrum framework at www.scrum.org. Agile development is a software development approach based on iterative development, early and frequent inspection, and incremental deliveries in which requirements and solutions evolve through collaboration in cross-functional teams and through continuous stakeholder feedback.

1.3. Statement of Work Organization

1.3.1. The Statement of Work (SoW) describes in detail the exact work to be done to fulfil the purpose of this Contract and is organised as follows:

1.3.1.1. Section 1 introduces the ETEE FS BMD project and defines the work that needs to be accomplished under this Contract.

1.3.1.2. Section 2 specifies the Software Engineering tasks that the Contractor shall undertake under the direction and guidance of the Purchaser.

1.3.1.3. Section 3 describes the Training Material support tasks that the Contractor shall undertake under the direction and guidance of the Purchaser.

1.3.1.4. Section 4 contains a set of relevant definitions.

1.4. High-level Contract Requirements

1.4.1. Provide an effective and competent Software Engineering team of subject matter experts throughout the full period of performance of this Contract. The requirements for the team will include:

1.4.1.1. Contribute to the design, implementation and testing of the required software for the BMD Exercise IM Portal Template system according to an agile development methodology in a distributed working environment overseen by the Purchaser.

1.4.1.2. Contribute to the design, implementation and testing of the following BMD Exercise IM Portal Template system services:

1.4.1.2.1. Program Management Service

1.4.1.2.2. Event Planning Management Service

1.4.1.2.3. Setting Management Service

1.4.1.2.4. Exercise Evaluation Management Service

1.4.1.2.5. Lessons Management Service

1.4.1.3. Support development Sprints that deliver software that in the end fulfils the agreed set of functionalities for each of the services listed in Section 1.4.1.2. A list of the foreseen software requirements for the BMD Exercise IM Portal Template system is added for info at Annex A. Consecutive Sprints will be conducted leading to the intermediate delivery. A defined set of twelve (12) standalone Sprints with a duration of one (1) week are anticipated to be conducted for bug fixing and refinement leading to the final delivery. Sprints will focus on specific areas of related functionality and will normally consist of a number of iterations that progress as follows:

1.4.1.3.1. The first iteration focuses on achieving an understanding by the Contractor-provided team of the software requirements, of the intended User interface, business process and associated business objects and logic.

1.4.1.3.2. The subsequent iterations refine the elements of the first iteration and expands on the data services, storage and administration aspects.

1.4.1.4. Contribute to the design, implementation and testing of the software user epic requirements for the BMD Exercise IM Portal Template system with a 3 (three) person Software Engineering team for the intermediate delivery phase

and a single person part-time Senior Software Engineer for the final delivery phase in an agile manner

1.4.1.5. Contribute to the development of on-line help with the delivered software.

1.4.1.6. Contribute to the development of training material for system administrators.

1.4.2. Provide an effective and competent Training Subject Matter Expert (SME) for 50 person-days to contribute to the development of training materials for operational users starting from the end of the intermediate delivery phase.

1.5. Contract Requirements

1.5.1. The requirements for the Software Engineering Team are described in Section 2.

1.5.2. The requirements for the Training SME are described in Section 3.

1.5.3. The user epic software requirements for the BMD Exercise IM Portal Template system are described in ANNEX A.

1.5.4. The technology and non-functional requirements for the BMD Exercise IM Portal Template system are described in ANNEX B.

1.5.5. The requirements for the coding principles and guidelines are described in ANNEX C.

1.5.6. The requirements for training material support are described in Section 2.

1.5.7. The requirements for documentation are described in Section 4.

2. Task 1: Software Engineering (CLIN 1)

2.1. Scope

2.1.1. The scope of the software engineering work consists of the support by a Software Engineering Team furnished by the Contractor on a time and material basis for the design, implementation, testing and integration of the Work Package scope defined in Section 1.4 and detailed in ANNEX A in accordance with the schedule defined in Section 1 and in compliance with the development and implementation methodology described in Sections 2.6 through 2.9 and with the requirements expressed in Section 2.11 through 2.16.

2.2. Software Engineering Start Date and Schedule

2.2.1. The Software Engineering Project Start Date (SE PSD) under this Work Package shall be the Effective Date of Contract (EDC).

2.3. Software Engineering Team requirements

- 2.3.1. For the intermediate delivery phase of Work Package 3, the Contractor shall provide a Software Engineering Team of three (3) Software Engineers including a Senior Software Engineer. Each Software Engineer shall work for up to 240 person-days in a consecutive period of twelve (12) to fourteen (14) months. For the phase leading to final delivery, the Contractor shall provide a single Senior Software Engineer for five (5) consecutive days during the second week of each month for a period of twelve (12) months, not to exceed 60 person-days in total.
- 2.3.2. The role of the Software Engineering Team will be to contribute, under the direction and guidance of the Purchaser, to the design, implementation and testing of software that supports the User epics associated with the service requirements described in ANNEX A in an agile manner and bound by the contractually defined resource levels and by the duration of the phases described in Section 2.3.1. User epics will be broken down by the Purchaser into user stories or features and features will be broken down into backlog items. The Purchaser will assign to the Software Engineering Team a set of tasks to implement backlog items of user stories in a priority order.
- 2.3.3. All members of the Software Engineering Team are identified as Key Personnel and shall all meet the following essential qualifications:
- 2.3.3.1. A minimum of three (3) years of proven experience within the last 5 years of developing software using the following technologies: MS SharePoint, HTML5, CSS, JavaScript, .Net and C#, or one of its predecessors, not older than five (5) years from the date of bid submission.
- 2.3.3.2. A minimum of three (3) years of proven experience within the last 5 years in developing software using the software implementation environment described in Section 2.7.7, or one of its predecessors, not older than five (5) years from the date of bid submission.
- 2.3.3.3. A minimum of three (3) years of proven experience within the last 5 years in developing software using the Collaboration environment described in Section 2.7.6 or one of its predecessors not older than five (5) years from the date of bid submission.
- 2.3.3.4. A thorough knowledge of the English language equivalent to the proficiency of at least Level 3 as specified in STANAG 6001 for all language aspects.
- 2.3.3.5. At least two (2) years of experience in developing software according to the coding principles and guidelines as specified at Annex C.
- 2.3.4. The Senior Software Engineer shall have in addition at least three (3) years of proven working experience within the last 5 years of developing software in an agile development approach.

- 2.3.5. At least one member of the Software Engineering Team shall have at least two (2) years of proven working experience within the last 5 years with the design, execution and documentation of unit testing.
- 2.3.6. The uninterrupted availability to the project of the entire Software Engineering Team at the required level of capacity is essential for the progress and success of the Sprints and Iterations. The Contractor is responsible to ensure uninterrupted SME support in accordance with the terms of the contract.
- 2.3.7. For the intermediate delivery phase and the specific performance periods of the final delivery phase, all members of the Software Engineering Team shall be available for a daily SCRUM meeting of around 30 minutes within the time window of 09:00 and 16:00 CET.
- 2.3.8. In addition to the SCRUM meetings, all members of the Software Engineering Team shall be available for a weekly progress meeting of around 1 hour on a working day within the time window of 09:00 and 16:00 CET

2.4. BMD ETEE IM Portal Template System requirements

- 2.4.1. The intended user epic software requirements supported by Work Package 3 (this Contract) are described in ANNEX A. Based on priority, minor deviation could be agreed by the Purchaser within the Agile development methodology.
- 2.4.2. The Purchaser will refer to the document in ANNEX A to perform the role of Scrum Product Owner and of Scrum Master.

2.5. Purchaser Responsibilities

- 2.5.1. The Purchaser Technical Lead or appointed members of his team shall perform the roles of Product Owner, of Scrum Master and of Tester as defined by the Scrum framework at www.scrum.org.
- 2.5.2. The Purchaser shall produce regular releases for release testing and for end User testing as described in Section 2.9.

2.6. Software development methodology

- 2.6.1. For each of the portal template system services, a number of iterations will be executed. The iterations will be executed in a way that initially targets the presentation aspect of the business services, the supported business process and the business objects and their logic. Subsequently the data services, associated data storage and the administration services will be addressed in a more complete and consistent manner while further refinement is done for the presentation, business process, business objects and logic.
- 2.6.2. Each iteration will result in a working software solution that fulfils a set of User stories set for the iteration according to an agile development way of working. Each iteration shall utilise the assigned time fully with the assigned Software

Engineering Team to implement the specified user stories as software features and the associated Software Engineering Team-assigned prioritised tasks.

- 2.6.3. At the end of each iteration and Sprint, the Purchaser will build and test a release. At the end of a Sprint or iteration, the associated User stories will be marked as met, requiring to be incorporated in on-going or follow-on Sprints or iterations, or logged for later attention.
- 2.6.4. At EDC, a refined design of the various business service features and User stories will have been developed by the Purchaser to start the development effort in the most efficient manner.
- 2.6.5. The Purchaser shall involve appropriate operational Users for review, feedback or testing of the project deliverables throughout the life span of the project.
- 2.6.6. The Purchaser, supported by the Contractor of Work Package 4 (Operational Assurance), shall perform testing as an integral part of each iteration and Sprint.
- 2.6.7. At the end of each iteration and sprint the Senior Software Engineer will provide to the Purchaser a timesheet per Software Engineer specifying per calendar day the back log items that were addressed and the amount of time spent on each backlog item. Purchaser approved timesheets will be the basis for the generation of periodic Contractor payment invoices.
- 2.7. Software implementation location of work, environment and tools (CLIN 3)
 - 2.7.1. Unless otherwise specified or approved by the Purchaser, the main effort for this task shall be carried out remotely on the Contractor's premises.
 - 2.7.2. The Purchaser will make provisions at the Effective Date of Contract to provide the Contractor as Purchaser Furnished Material with 3 virtual development machines for the intermediate delivery phase and 1 virtual development machines for the final delivery phase that are fully configured to support the required development work for the duration of the Contract on the NATO Software Factory (NSF), an internet facing Azure DevOps environment.
 - 2.7.3. The Contractor shall provide a physical development workstation to each member of the WP3 Contractor Software Engineering Team to connect to the NSF. The Contractor shall also provide to each member of the Software Engineering Team uninterrupted internet connectivity with sufficient bandwidth for efficient online development on the NSF. The physical development workstation shall meet at least the following specifications:
 - 2.7.3.1. 64-bit CPU
 - 2.7.3.2. Full disk encryption for mobile devices including laptops
 - 2.7.3.3. 64-bit Operating System supported to run McAfee Endpoint Security and VPN Client

- 2.7.3.4. Weekly software patching,
 - 2.7.3.5. McAfee Endpoint Security with daily updates,
 - 2.7.3.6. VPN Client (will be specified at Contract Award) equivalent to Cisco AnyConnect.
 - 2.7.3.7. Peripherals for video and voice collaboration.
- 2.7.4. The physical development workstation shall be dedicated to this project and not be used for any other activities.
- 2.7.5. The Contractor shall provide the necessary networking facilities and supporting software, necessary to comply with the requirements of Section 2.7.3, to connect into the Purchaser's collaborative development environment.
- 2.7.6. The collaboration environment is based on the integrated use of Microsoft Teams and of the Azure DevOps Services.
- 2.7.7. The software development environment shall be based on the Azure DevOps Services and on Visual Studio Code. The virtual development environment will be provided by the Purchaser as part of the Purchaser Furnished Material as described in Section 2.7.2.
- 2.8. Software development configuration management
- 2.8.1. A Sprint will start with an identified development branch and result in functioning software that has been verified to fulfil the set of Sprint software requirements. The functioning software and associated documentation will be referred to as a Sprint release. The Purchaser will be able to include a Sprint release in a system baseline.
- 2.8.2. An iteration within a Sprint will start with an identified development branch and result in functioning software that has been verified to fulfil the set of iteration software requirements. The functioning software will be referred to as an iteration release.
- 2.8.3. The development branches will be produced by the Purchaser and provided to the Software Engineering Team. The Contractor shall be responsible for managing the development branches used by the Software Engineering Team. The Purchaser will merge the branches based on pull requests submitted by the Contractor Senior Software Engineer. At the beginning of each Iteration or Sprint the Contractor and the Purchaser shall fix a schedule for submitting pull requests. The Purchaser will build the releases.
- 2.8.4. The Contractor shall not share any work or effort produced under this Work Package 3 with any other parties without prior written approval of the Purchaser's contracting authority.

2.8.5. The Contractor shall provide the Purchaser with a list of physical development workstations dedicated to this project and provide updates as necessary throughout the performance period of the Contract.

2.8.6. Upon completion of the usage of the physical development workstations, the Contractor shall wipe the workstations completely. The Contractor shall provide to the Purchaser a statement of conformity for the wiping signed by the Contractors Corporate Security Officer. After wiping, the Contractor is free to use the physical development workstations for any other purpose

2.9. Software implementation and Test plan

2.9.1. The Scope is defined in Section 2.3 and 2.4. The schedule shall be as specified in Section 1.

2.9.2. All software code developed by the Contractor shall be successfully unit tested by the Contractor before it is included in a pull request by the Contractor Senior Software Engineer.

2.9.3. All software code developed by the Contractor shall conform to the coding principles defined in Section 2.13 before it is included in a pull request by the Contractor Senior Software Engineer.

2.9.4. Integration Testing will be conducted as part of the agile development process as a part of each Sprint and iteration.

2.9.5. Any bugs reported after the intermediate delivery shall be addressed during the development for the final delivery according to the priorities set by the Purchaser.

2.9.6. The FAT, SIT and UAT will be performed by the Purchaser and will verify that all the agreed BMD Exercise IM Portal Template system requirements associated with the business processes described at ANNEX A can be executed successfully on the Purchaser's operational network by the intended users. The test results will be logged by the Purchaser including the test data, outcome and comments. The tests will be classed as successful, partially successful or failed. Partially successful or failed tests will be addressed by the Purchaser and may be assigned to the Contractor during the final delivery phase within the scope defined for the final delivery phase.

2.9.7. The following intermediate delivery validation steps will be performed by the Purchaser as part of the FAT, SIT and UAT:

2.9.7.1. Verify and validate that the Contractor-delivered software complies with the cyber security requirements.

2.9.7.2. Independent Validation & Verification testing on Contractor-delivered software by the NCIA IV&V team.

2.9.7.3. Verify and validate that the baseline release meets the performance and usability quality criteria described in Section 2.12.

- 2.9.7.4. Verify and validate that all specified on-line help as described in Section 2.14 is available.
- 2.9.7.5. Verify and validate that the system administration documentation as specified in Section 2.16 is complete and correct.
- 2.9.8. The additional FAT, SIT and UAT verification and validation failures will be scheduled by the Purchaser for resolution during the final delivery phase.
- 2.10. Test scenario data
 - 2.10.1. Relevant test scenario data will be provided by the Purchaser at the start of each development Sprint and may be amplified during the Sprint.
- 2.11. Cyber Security requirements
 - 2.11.1.1. The cyber security non-functional requirements are described in ANNEX B.
 - 2.11.1.2. The cyber security requirements for secure coding are described in ANNEX C.
 - 2.11.1.3. The developed software will be subject to a cyber-security test executed by the Purchaser (Ref. Section 2.9.7.1).
- 2.12. Quality assurance
 - 2.12.1. The quality of Contractor developed software releases will be tested by the Purchaser using the following criteria:
 - 2.12.1.1. Performance: all User interaction shall respond within less than two (2) seconds under a load that is defined by the Purchaser as being representative.
 - 2.12.1.2. Test Reliability: At least 80% of the requirements to be validated for a Sprint release are tested with immediate successful result and 90% after one (1) additional re-test.
 - 2.12.1.3. Usability: at least 90% of presentation aspects shall be deemed intuitive in their usage and navigation by an operational User supporting the business process described in ANNEX A including consistent presentation and behaviour and on-line help.
- 2.13. Coding principles and guidelines
 - 2.13.1. The coding principles and guidelines are described at ANNEX C.
- 2.14. On-line Help
 - 2.14.1. The Contractor Software Engineering Team shall contribute to the incorporation of tool tips for each presentation aspect of the services that are implemented by the Contractor. The tool tip shall include the description of the requirement and how the functionality is to be used as a part of the User story.

2.15. Contribution to training for system administrators

2.15.1. The Contractor shall contribute to the training for system administrators by producing a specific text document that describes the global configuration variables, file system locations or URLs that affect the operation of the BMD Exercise IM Portal Template system that the Contractor has implemented.

2.16. Prohibition of Software licenses

2.16.1. The Contractor shall not include without the prior written approval of the Purchaser any software requiring a license agreement or any software with background Intellectual Property.

3. **Task 2: Training Material (CLIN 2 and CLIN 3)**

3.1. Scope

3.1.1. The Contractor Training SME shall contribute, within the parameters and resources available under this Contract, to the training of operational Users by including an interactively accessible description of the business process that the implemented component supports at the level of detail as described in Annex A.

3.1.2. The Contractor Training SME shall contribute to the production of training materials for operational users for each service specified in ANNEX A. The training materials shall be organised according to the process and role descriptions in ANNEX A and provide a step-by-step description of the way to employ the 5 portal services listed in section 1.4.1.2 to achieve operational user outcomes using annotated service screen captures.

3.1.3. The Contractor Training SME shall work on the production of training materials for the BMD Exercise Portal Template system for up to 50 person-days in a period of three (3) months starting at the end of the intermediate delivery phase.

3.1.4. Unless otherwise specified or approved by the Purchaser, the main effort for this task shall be carried out remotely on the Contractor's premises.

3.1.5. The Purchaser will make provisions to provide the Contractor as Purchaser Furnished Material with 1 virtual development machine that is fully configured to support the required development work for the duration of the Training Material production on the NATO Software Factory (NSF), an internet facing Azure DevOps environment.

3.1.6. The Contractor shall provide a physical development workstation to the WP3 Contractor Training SME to connect to the NSF. The Contractor shall also provide to the Training SME uninterrupted internet connectivity with sufficient bandwidth for efficient online development on the NSF. The physical development workstation shall meet at least the following specifications:

3.1.6.1. 64-bit CPU

- 3.1.6.2. Full disk encryption for mobile devices including laptops
 - 3.1.6.3. 64-bit Operating System supported to run McAfee Endpoint Security and VPN Client
 - 3.1.6.4. Weekly software patching,
 - 3.1.6.5. McAfee Endpoint Security with daily updates,
 - 3.1.6.6. VPN Client (will be specified at Contract Award) equivalent to Cisco AnyConnect.
 - 3.1.6.7. Peripherals for video and voice collaboration.
- 3.1.7. The physical development workstation shall be dedicated to this project and not be used for any other activities.
- 3.1.8. The Contractor shall provide the necessary networking facilities and supporting software, necessary to comply with the requirements of Section 3.1.6, to connect into the Purchaser's collaborative development environment.
- 3.1.9. The collaboration environment is based on the integrated use of Microsoft Teams and of the Azure DevOps Services.
- 3.1.10. Upon completion of the usage of the physical development workstation, the Contractor shall wipe the workstation completely. The Contractor shall provide to the Purchaser a statement of conformity for the wiping signed by the Contractors Corporate Security Officer. After wiping, the Contractor is free to use the physical development workstation for any other purpose.
- 3.2. The Contractor Training SME is identified as Key Personnel shall meet the following essential qualifications:
- 3.2.1. A minimum of 6 months of proven experience producing training materials for interactive portal systems.
 - 3.2.2. A minimum of a proven delivery of at least 25 days of training classes for these types of applications within the past three (3) years in the English language.
 - 3.2.3. A thorough knowledge of the English language equivalent to the proficiency of at least Level 3 as specified in STANAG 6001 for all language aspects.

4. Definitions

4.1. The following definition of terms shall be used for this project:

- 4.1.1. Development Branch: A development or develop branch is created from the master. The development branch is the main branch where the source code of HEAD always reflects a state with the latest delivered development changes for

the next release. Feature branches are created from a develop branch. When a feature is complete it is merged into the develop branch. The DEVELOP branch is one of the branches with infinite lifetime.

- 4.1.2. Iteration Release: All the software that fulfils the requirements of the iteration.
- 4.1.3. Sprint Release: all the software that fulfils the requirements of the Sprint and all the documentation that is required for the software to be included in a system baseline.
- 4.1.4. Product Baseline: all the software and documentation that is required to meet the Purchaser change management requirements for acceptance as a new approved fielded system.

ANNEX A: Software Requirement Specifications

ANNEX B: Technology and non-functional requirements

ANNEX C: Coding principles and guidelines

ANNEX D: Purchaser Furnished Property



NATO Communications and Information Agency
Agence OTAN d'information et de communication

**PROVIDE BMD EXERCISE INFORMATION MANAGEMENT PORTAL
TEMPLATE SYSTEM WITHIN BALLISTIC MISSILE DEFENCE (BMD)
FUNCTIONS IN EDUCATION, TRAINING, EXERCISE AND
EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

RFQ-CO-115114-ETEE PORTAL

BOOK II – PART III

STATEMENT OF WORK

Annex A: BMD IM Portal Software Requirements Specification

Annex A: BMD IM Portal Software Requirements Specification

Contents

1	BMD IM Portal Concept of Utilization	3
2	Program Management Service	3
3	Event Planning Management Service.....	3
4	Setting Management Service	4
5	Exercise Evaluation Management Service	5
6	Lessons Management Service	6

1 BMD IM Portal Concept of Utilization

- 1.1 (BMD-IMP-ROLE-01) The BMD exercise portal manager shall be able to specify that domain users can belong to the following groups of users for the exercise program portal:
 - 1.1.1 Exercise program contributor
 - 1.1.2 Exercise program viewer
- 1.2 (BMD-IMP-ROLE-02) For a particular exercise, the BMD exercise portal manager shall be to instantiate an exercise portal from two template types:
 - 1.2.1 Yearly exercise template
 - 1.2.2 Recurring exercise template
- 1.3 (BMD-IMP-ROLE-03) For a particular exercise portal, the BMD exercise portal manager shall be able to specify that domain users can belong to the following groups of users:
 - 1.3.1 Exercise Planner
 - 1.3.2 Exercise viewer
 - 1.3.3 Setting Builder
 - 1.3.4 Setting viewer
 - 1.3.5 Exercise Evaluation Manager
 - 1.3.6 Exercise Evaluator
 - 1.3.7 Evaluation Viewer
 - 1.3.8 Exercise Lessons Manager
 - 1.3.9 Lessons Viewer

2 Program Management Service

- 2.1 (BMD-IMP-PMS-01) The BMD program management service shall be structured according to the same format as the Military Training and Exercise Planning (MTEP) in order to be able to import MTEP data and to export exercise data to the eMTEP.
- 2.2 (BMD-IMP-PMS-02) The program shall enable the BMD exercise program contributors to add, modify exercise events sponsored by NATO and by nations according to the same organisation in chapters as the MTEP.
- 2.3 (BMD-IMP-PMS-03) For recurring exercise events, the exercise planner shall be able to specify which units are participating and in what mode, simulated or live in training mode.

3 Event Planning Management Service

- 3.1 (BMD-IMP-EPMS-01) For a particular exercise, the exercise planner shall be able to instantiate a specific portal that is organised according to the following structure:
 - 3.1.1 Exercise Specification (EXSPEC)
 - 3.1.2 Training Objectives
 - 3.1.3 Setting: as a reference to the base setting that is used for the exercise

- 3.1.4 Exercise Plan (EXPLAN) with sub-sections corresponding to the structure of the EXPLAN as defined in Bi-SC directive 75-3
- 3.1.5 For recurring exercises: a specific section shall be added for the Distributed Exercise Simulation and C2 Interoperability plan
- 3.2 (BMD-IMP-EPMS-02) The exercise viewer shall be able to consult site information.

4 Setting Management Service

- 4.1 (BMD-IMP-SMS-01) The setting management service will enable the portal manager to instantiate an exercise setting site structured according to the scenario modules specified in the Bi-SC 75-3 directive including but not limited to the following sub-sections:
 - 4.1.1 Theatre of operations information
 - 4.1.2 Strategic initiation with the option to add sub-sections for:
 - 4.1.2.1 Road to Crisis (Narrative summary of the main events leading to planning situation, to be included in MEL/MIL database).
 - 4.1.2.2 UNSC Resolutions and/or other documents providing the legal basis for the operation.
 - 4.1.2.3 NAC Request for Advice.
 - 4.1.2.4 SACEUR's Strategic Warning Order.
 - 4.1.2.5 SACEUR's Strategic Assessment.
 - 4.1.2.6 NAC Decision Sheet Requesting Options. SACEUR's Military Response Options.
 - 4.1.2.7 NAC Initiating Directive.
 - 4.1.3 Crisis Response Planning Information with the option to add sub-sections for:
 - 4.1.3.1 Current Intelligence Summary.
 - 4.1.3.2 Friendly Forces. Provides forces available for planning based on NRF Readiness Reporting System (RRS) and NATO ORBAT as well as current disposition of friendly and neutral forces in the theatre area. Data for generic forces available for planning should be provided in the same formats and level of detail as real forces available for planning would be.
 - 4.1.3.3 Target Integrated Data Base (IDB).
 - 4.1.3.4 Civil military data and information sufficient to support TA development of the production of the Civil Assessment and the CIMIC Estimate as well as the CIMIC input to an Operation Plan.
 - 4.1.3.5 Environmental Assessment.
 - 4.1.3.6 Operational Liaison Reconnaissance Team (OLRT) Recce Reports.
 - 4.1.3.7 NATO Crisis Response System (NCRS) messages.
 - 4.1.3.8 TOPFAS dataset.
 - 4.1.3.9 LogBase dataset.

- 4.1.3.10 Intelligence dataset, including regional forces' data and scenario-specific Crisis Response Intelligence Package (CRIP).
- 4.1.3.11 BMD Threat characteristics
- 4.1.3.12 BMD Threat Situation
- 4.1.4 Force Activation and Deployment with the option to add sub-sections for:
 - 4.1.4.1 ACTWARN/ACTREQ messages.
 - 4.1.4.2 FORCEPREP messages. Allied Force List (AFL)
 - 4.1.4.3 Force Balancing Results.
 - 4.1.4.4 SOFAs/MOUs/TAs.
 - 4.1.4.5 Multinational Detailed Deployment Plan (MNDDP)/Flow Execution Plan (FEP).
 - 4.1.4.6 ACTORD message(s).
 - 4.1.4.7 ORBATTOA messages.
 - 4.1.4.8 Current Intelligence Summary (INTSUM)/Intelligence Report (INTREP)(as required).
 - 4.1.4.9 Joint Targets List.
 - 4.1.4.10 NCRS messages.
 - 4.1.4.11 Rules of Engagement Authorisation (ROEAUTH)/Implementation (ROEIMPL) messages.
- 4.1.5 BMD Unit Status specifying the various units available for BMD planning
- 4.1.6 Reference to the exercise geographic information source
- 4.2 (BMD-IMP-SMS-02) Setting builders shall be able to create, modify and delete setting information products.
- 4.3 (BMD-IMP-SMS-03) Setting builders and portal managers shall be able to add sections to the portal.
- 4.4 (BMD-IMP-SMS-04) The portal manager shall be able to save a specific complete or partial portal as a new template.
- 4.5 (BMD-IMP-SMS-05) A setting viewer shall be able to consult setting information products.

5 Exercise Evaluation Management Service

- 5.1 (BMD-IMP-EEM-01) The exercise evaluation management service shall enable the portal manager to manage graded and qualitative evaluation exercise templates.
- 5.2 (BMD-IMP-EEM-02) For both types of evaluation, the templates will consist of an evaluation criteria section, an evaluation plan section and an evaluation observation and lessons section.
- 5.3 The differences between both types of portal are:
 - 5.3.1 (BMD-IMP-EEM-03) The portal manager shall be able to extract qualitative evaluation criteria from a specific qualitative evaluation portal and update the reference list of qualitative evaluation criteria.

- 5.3.2 (BMD-IMP-EEM-04) The qualitative exercise evaluation manager shall be able to extend the list of qualitative evaluation criteria for a particular exercise.
- 5.3.3 (BMD-IMP-EEM-05) Quantitative evaluation criteria will be associated at their lowest of granularity with quantifiable performance measures that have a weight.
- 5.3.4 (BMD-IMP-EEM-06) Quantitative evaluation criteria scores are derived from their underlying criteria structure and performance measures.
- 5.3.5 (BMD-IMP-EEM-07) Qualitative evaluation criteria do not have a fixed scoring mechanism.
- 5.4 (BMD-IMP-EEM-08) An evaluation criteria section will be created by the exercise evaluation manager using a reference list of evaluation criteria.
- 5.5 (BMD-IMP-EEM-09) Criteria may have a nested structure of sub-criteria.
- 5.6 (BMD-IMP-EEM-10) For quantitative evaluation they may be associated a number of performance measures that have a specific weight.
- 5.7 (BMD-IMP-EEM-11) The evaluation exercise manager shall define evaluation tasks related to evaluation criteria
- 5.8 (BMD-IMP-EEM-12) The evaluation exercise manager shall be able to assign evaluation tasks to exercise evaluators.
- 5.9 (BMD-IMP-EEM-13) The evaluation manager shall be able to assess the evaluator workload by reviewing an evaluator's task assignment in time.
- 5.10 (BMD-IMP-EEM-14) An exercise evaluator shall be able to manage own exercise observations and inputs to the achievement of an exercise criterion by grading or commenting on the criterion.
- 5.11 (BMD-IMP-EEM-15) The exercise evaluation manager shall be able to aggregate the exercise observations and grades to develop overall lessons identified.
- 5.12 (BMD-IMP-EEM-16) The portal manager shall be to extract exercise criteria evaluations across multiple exercises.
- 5.13 (BMD-IMP-EEM-17) Evaluation viewers shall be able to consult all or specifically authorised evaluations.

6 Lessons Management Service

- 6.1 (BMD-IMP-LMS-01) The portal manager shall be to instantiate a specific lessons portal for an exercise from a template for lessons management.
- 6.2 (BMD-IMP-LMS-02) The lessons portal template shall consist of a lessons identified section, of a remedial action section, of a best practices section.
- 6.3 (BMD-IMP-LMS-03) The exercise lessons manager shall be able to associate lessons identified with remedial actions or proposals for best practices.
- 6.4 (BMD-IMP-LMS-04) The exercise lessons manager shall be able to manage the assignment of remedial actions to specific units.
- 6.5 (BMD-IMP-LMS-05) The exercise lessons manager shall be able to capture the outcome of remedial actions.

- 6.6 (BMD-IMP-LMS-06) The exercise lessons viewer shall be able to consult all or specifically authorised lessons portals.



NATO Communications and Information Agency
Agence OTAN d'information et de communication

**PROVIDE BMD EXERCISE INFORMATION MANAGEMENT PORTAL
TEMPLATE SYSTEM WITHIN BALLISTIC MISSILE DEFENCE (BMD)
FUNCTIONS IN EDUCATION, TRAINING, EXERCISE AND
EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

RFQ-CO-115114-ETEE PORTAL

BOOK II – PART III

STATEMENT OF WORK

**Annex B: IM Portal Technologies and Non-Functional
Requirements**

ANNEX B: IM PORTAL Technologies and Non-Functional Requirements

Contents

1	Applicable Technologies	3
2	Non-Functional Requirements.....	3
3	Presentation Services.....	3
4	Web Services.....	6
5	Time Behaviour.....	8
6	Scalability.....	9
7	Maintainability	9
8	Reliability	11
9	Usability	15
10	Security	16
11	Web Security.....	20
12	Interface Requirements.....	30
13	Architectural Constraints.....	31
14	Graphical User Interface (GUI)	32

1 Applicable Technologies

1.1 The technologies that shall be employed to implement the services of the BMD Exercise Information Management Portal Template system are:

- MS SharePoint version 2016 or above
- HTML 5
- CSS
- JSON

2 Non-Functional Requirements

2.1 The following chapters describe the Non-Functional Requirements that are applicable to all NATO IKM tools including the BMD Exercise Information Management Portal Template system.

3 Presentation Services

3.1 These services provide the IKM Tools visual interaction with the user by depicting the IKM Tools system operations and results on web pages.

3.2 As described in the C3 Taxonomy:

3.2.1 “The Web Presentation Services allow combining rich content from different data sources into a single client web page or desktop, using a combination of Web 2.0 technologies such as HTML snippets, scripting code (JavaScript), on demand code (AJAX, JSON), web service calls and proprietary code.”

3.3 Therefore enables the user to customize the web pages by combining widgets (portlets, web parts and alike web components). The purpose is to achieve a better User eXperience (UX) via a flexible and standard User Interface. For example adhering to the UX aspects for a proper UX design:

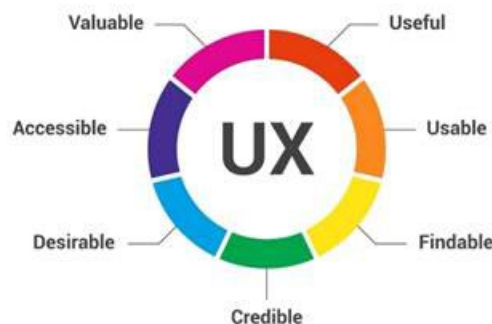


Figure 1 The 7 Factors that Influence User Experience (ref: Interaction Design Foundation)

- 3.4 The combination of widgets that Share Point offers facilitates this purpose. For the IKM Tools to deliver the required UX some more features need to be implemented following the industry standards.
- 3.5 Requirement ID: IKM-SRS-20
- 3.5.1 The IKM Tools shall provide the functionality to support the addition, update, deletion and visualisation of web widgets.
- 3.5.2 Verification Method: Test
- 3.6 Requirement ID: IKM-SRS-21
- 3.6.1 The IKM Tools shall provide the ability to customize the web widgets for the look and feel, security and similar functional aspects.
- 3.6.2 Verification Method: Test
- 3.7 Requirement ID: IKM-SRS-22
- 3.7.1 The IKM Tools shall be able to discover web widgets and make them available for use.
- 3.7.2 Verification Method: Inspection
- 3.8 Requirement ID: IKM-SRS-23
- 3.8.1 The IKM Tools shall provide functionality to manage the complete web widgets lifecycle. This includes deployment, modification, maintenance, un-deployment and archiving.
- 3.8.2 Verification Method: Analysis
- 3.9 Requirement ID: IKM-SRS-24
- 3.9.1 The IKM Tools shall provide inter-web widgets communication and remote web widgets communication.
- 3.9.2 Verification Method: Analysis
- 3.10 Requirement ID: IKM-SRS-25
- 3.10.1 The IKM Tools shall provide the functionality to render the visualization of the web widget according to user customization and user input.
- 3.10.2 Verification Method: Test
- 3.11 Requirement ID: IKM-SRS-26
- 3.11.1 The IKM Tools shall follow the Web 2.0 standards when applicable:
- NISP Standard - HTML version 5.0 - "HyperText Markup Language (HTML), Version 5.0, Reference Specification"
 - NISP Standard - RFC 2616: HTTP v1.1 - "HyperText Transfer Protocol (HTTP), version 1.1"
 - NISP Standard - RSS 2.0 - "RSS 2.0 Specification"
 - RFC 2318 - "The text/css Media Type"
 - RFC 4287 - "The Atom Syndication Format"
 - RFC 4329 - "Scripting Media Types"
 - RFC 4627 - "The application/json Media Type for JavaScript Object Notation (JSON)"

- RFC 5023 - "The Atom Publishing Protocol"
- RFC 3986, 2005 - URI to identify resources
- CSS3: CSS2.1 <http://www.w3.org/TR/CSS2/> , CSS Style Attributes, Media Queries Level 3, CSS Namespaces, Selectors Level 3, CSS Color Level 3

3.11.2 Verification Method: Analysis

3.12 Requirement ID: IKM-SRS-27

3.12.1 The IKM Tools shall comply with the NATO Visual Identity Guidelines [ref. NATO Visual Identity Guidelines v. 3 (on-line)]

3.12.2 Verification Method: Inspection

3.13 Requirement ID: IKM-SRS-28

3.13.1 While it is advisable that the IKM Tools GUI should be not so far from the current IKM Tools so that the user sees a similar and familiar look and feel (e.g.: colors, layout and navigational behaviour), the Contractor shall propose a new modern UX and UI design that will be approved by the Purchaser during the Design Phase.

3.13.2 Verification Method: Inspection

3.14 Requirement ID: IKM-SRS-29

3.14.1 The IKM Tools shall provide all capability responsive for desktop devices and also for mobile devices (aka tablet and mobile phone).

3.14.2 Verification Method: Inspection

3.15 Requirement ID: IKM-SRS-30

3.15.1 The IKM Tools shall provide all capability optimized for the device is operating on.

3.15.2 Verification Method: Inspection

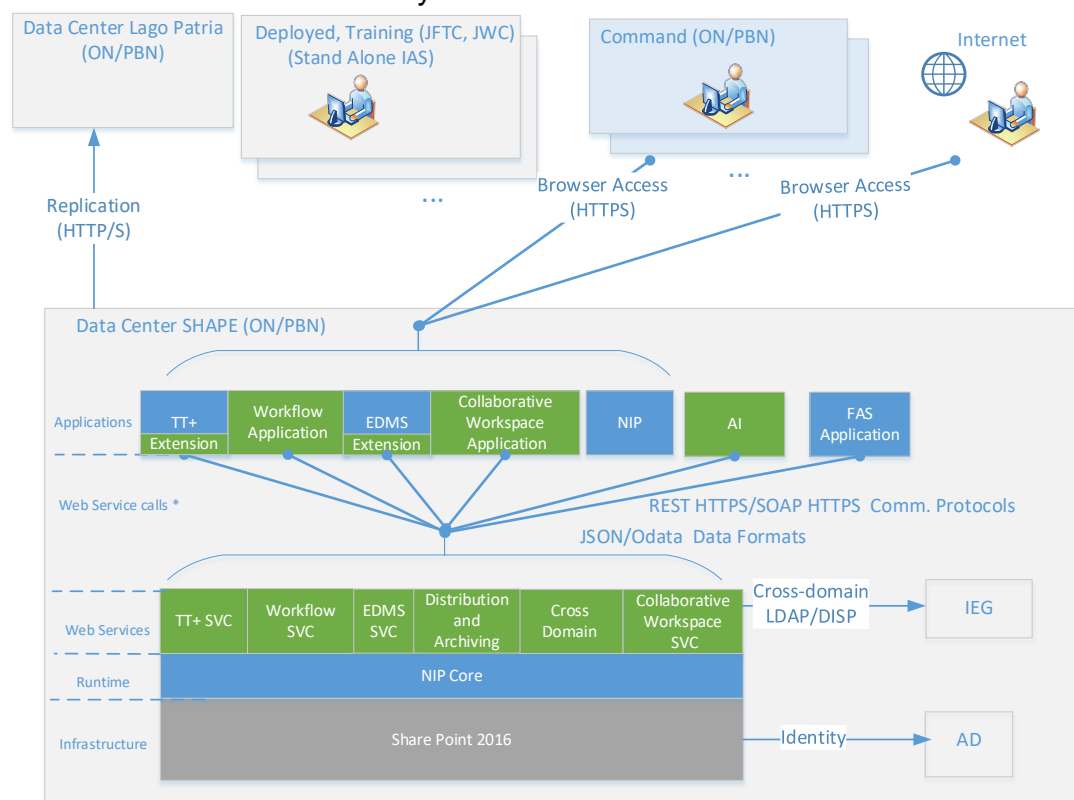
4 Web Services

4.1 In order to enhance the flexibility of the IKM applications a modular design needs to be considered to logically separate the applications from the underlying services they use. This separation will guarantee the replacement of the applications or update of services without much impact between each other.

4.2 Requirement ID: IKM-SRS-31

4.2.1 For that whenever possible the contractor shall use web services instead of native calls which are tightly bounded to the particular version of the API. Specifically the following interfaces depicted in the Figure 2 Internal Interfaces:

4.2.2 Verification Method: Analysis



* IAS shall support these protocols in addition to the direct native calls

Figure 2 Internal Interfaces

4.3 Requirement ID: IKM-SRS-32

4.3.1 The IKM Tools Web Services using the REST Style when invoking other Web Services shall conform to the SIP for REST Messaging (see [NCIA AI 06.02.07, 2015]).

4.3.2 Verification Method: Analysis

4.4 Requirement ID: IKM-SRS-33

4.4.1 The IKM Tools Web Services using the SOAP Style when invoking other Web Services shall comply with the SIP for SOAP Messaging (see [NCIA AI 06.02.06, 2015]).

4.4.2 Verification Method: Analysis

4.5 Requirement ID: IKM-SRS-34

4.5.1 For each API Component the Contractor shall provide a “Web Service Reference Guide” to fully document the interface, including:

4.5.1.1 *Server Application (the application that is exposing the service)*

4.5.1.2 *Client Application (the application that is invoking the service)*

4.5.1.3 *Authentication method*

4.5.1.4 *Logging mechanism*

4.5.1.5 *Mechanisms for securely invoking the API*

4.5.1.6 *Available methods and functionality*

- Name
- Description
- Inputs
 - Name
 - Description
 - Type
 - Mandatory/Optional
 - Eventual enumeration values
 - Example of correct/incorrect values
- Error messages
- Elaboration rules

4.5.2 Verification Method: Analysis

4.6 Requirement ID: IKM-SRS-35

4.6.1 The IKM Tools shall expose the APIs using open standards or widely accepted industry standards.

4.6.2 Verification Method: Analysis

4.7 Requirement ID: IKM-SRS-36

4.7.1 The IKM Tools API mechanism shall limit access of authenticated and Authorised Users/Systems to information products and workspaces required to perform the authorised function.

4.7.2 Verification Method: Analysis

4.8 Requirement ID: IKM-SRS-37

4.8.1 The IKM Tools GUI's shall make use of web services API to interact with a service whenever possible and when performance is not degraded below the accepted KPIs (see performance section).

4.8.2 Verification Method: Analysis

4.9 Requirement ID: IKM-SRS-38

4.9.1 The IKM Tools GUI's using web services API shall be designed to allow for future GUI enhancement or replacement with a modular and component design

4.9.2 Verification Method: Analysis

5 Time Behaviour

5.1 Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

5.2 Requirement ID: IKM-SRS-275

5.2.1 The IKM Tools functionality: web pages load, button click reaction and general user interaction with the IKM Tools GUI shall be available for an authorised user within 1 second the 95% of the times and within 2 seconds the 100% of the times. The time will be calculated from the instant that the user hits the button to the complete rendering of the page on the client machine (in order to measure the “end-to-end user experience”), with at least 50 items showed in the page (documents, list items, events, etc.)

5.2.2 Verification Method: Test

5.3 Requirement ID: IKM-SRS-276

5.3.1 The IKM Tools shall execute the log-in and log out functions within 2 seconds (excluding dependant ADFS services execution time).

5.3.2 Verification Method: Test

5.4 Requirement ID: IKM-SRS-277

5.4.1 The IKM Tools web services shall respond to authorised users within 0.1 seconds of submitting the request the 95% of the times and within 0.2 seconds the 100% of the times. The time will be calculated from the instant that the request is arrived to the server to the instant that the servers sends the response.

5.4.2 Verification Method: Test

5.5 Requirement ID: IKM-SRS-278

5.5.1 The IKM Tools search services shall respond within 2 seconds of submitting the search query the 95% of the times and within 3 seconds the 100% of the times. The time will be calculated from the instant that the user hits the button to the complete rendering of the page on the client machine (in order to measure the “end-to-end user experience”), with at least 50 search results and at least 20% of the users performing concurrently different searches.

5.5.2 Verification Method: Test

6 Scalability

6.1 Scalability is defined as the capability of a system to increase (or decrease) total throughput under an increased load when resources (typically hardware) are added (or subtracted), so the scalability quality figures are defined accordingly

6.2 Requirement ID: IKM-SRS-279

6.2.1 The IKM Tools shall be able to support a throughput increase of 10% every year with a response time degradation of not more than 5%.

6.2.2 Verification Method: Analysis

6.3 Requirement ID: IKM-SRS-280

6.3.1 The IKM Tools shall be Horizontal Scalable by allowing the deployment of system components on different instances.

6.3.2 Verification Method: Analysis

6.4 Requirement ID: IKM-SRS-281

6.4.1 The IKM Tools shall be Vertical Scalable.

6.4.2 Verification Method: Analysis

7 Maintainability

7.1 Degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers.

7.2 Modifications can include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications. Modifications include those carried out by specialized support staff, and those carried out by business or operational staff, or end users.

7.3 Maintainability includes installation of updates and upgrades.

7.4 Maintainability can be interpreted as either an inherent capability of the product or system to facilitate maintenance activities, or the quality in use experienced by the maintainers for the goal of maintaining the product or system.

7.5 General

7.5.1 MTTR is the Mean Time for the system To be Repaired after a failure.

7.5.2 MaxTTR is defined as the Maximum Time required To perform a maintenance Repair.

Service Type	MTTR	MaxTTR
Level 1	2 hours	4 hours
Level 2	4 hours	8 hours
Level 3	7 hours	24 hours

Table 1 Maintainability by Service Level

7.5.3 Requirement ID: IKM-SRS-282

7.5.3.1 The IKM Tools shall provide a Mean Time To Repair (MTTR) according to the Table 3 Maintainability by Service Level.

7.5.3.2 Verification Method: Test

7.5.4 Requirement ID: IKM-SRS-283

7.5.4.1 The MaxTTR for the IKM Tools shall not exceed the times stated in the Table 3 Maintainability by Service Level.

7.5.4.2 Verification Method: Analysis

7.6 Modularity

7.6.1 Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components

7.6.2 Requirement ID: IKM-SRS-284

7.6.2.1 IKM Tools shall be composed of discrete components such that a change to one component has minimal impact on other components, specifically: IKM Tools Framework, NIP, EDMS, TT+, Workspace and Workflow.

7.6.2.2 Verification Method: Analysis

7.6.3 Requirement ID: IKM-SRS-285

7.6.3.1 IKM Tools shall allow to update and deploy individual services and components without the need to re-install the full IKM Tools.

7.6.3.2 Verification Method: Test

7.6.4 Requirement ID: IKM-SRS-285b

7.6.4.1 IKM Tools shall allow to update and deploy individual services and components independently to each IKM tool, so that the update in one IKM Tool doesn't impact another IKM Tool.

7.6.4.2 Verification Method: Test

7.6.5 Requirement ID: IKM-SRS-286

7.6.5.1 The 99.9% of the time a maintenance action is required on a SW component of the IKM Tools, this action shall not cause any possible fault/error in other components of the system.

7.6.5.2 Verification Method: Analysis

7.6.6 Requirement ID: IKM-SRS-287

7.6.6.1 IKM Tools shall be modular enough so that the failure of one module or application (due to heavy processing or storage outage) doesn't affect the other modules.

7.6.6.2 Verification Method: Test

7.7 Analysability

7.7.1 Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

7.7.2 Implementation can include providing mechanisms for the product or system to analyse its own faults and provide reports prior to a failure or other event.

7.7.3 Requirement ID: IKM-SRS-288

7.7.3.1 The system shall be effective and efficient in the possibility to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

7.7.3.2 Verification Method: Analysis

7.7.4 Requirement ID: IKM-SRS-289

7.7.4.1 The system shall be able to detect the 99.5% of the possible fault/error which can occur, triggering the user with a message.

7.7.4.2 Verification Method: Analysis

7.7.5 Requirement ID: IKM-SRS-290

7.7.5.1 The system shall be able to diagnose the 95% of the possible fault/error which can occur, triggering the user with a message which identifies the happened failure/error.

7.7.5.2 Verification Method: Analysis

7.7.6 Requirement ID: IKM-SRS-291

7.7.6.1 The IKM Tools messages (e.g., error, warning, notification and informational messages) shall contain initiating module information, context sensitive help or directives on where to find answers and solutions.

7.7.6.2 Verification Method: Analysis

7.7.7 Requirement ID: IKM-SRS-292

7.7.7.1 The IKM Tools log messages shall contain:

- initiating module information
- Date/Time(Z)
- system instance
- (log) message
- category/severity
- user (invoker of function)
- context information (like mission/session, service/function, parameters, and trace-log)

7.7.7.2 Verification Method: Analysis

8 Reliability

8.1 Degree to which a system, product or component performs specified functions under specified conditions for a specified period of time.

8.2 General

8.2.1 MTBF (Mean Time Between Failures) is defined as the mean time between two consecutive faults which generate a failure.

8.2.2 MTBCF (Mean Time Between Critical Failures) is defined as the mean time between two consecutive faults which generate critical failures.

8.2.3 A critical failure is a failure which cause the complete system unavailability with consequent loss of the provided service/capability.

8.2.4 Requirement ID: IKM-SRS-293

8.2.4.1 IKM Tools shall exhibit a Mean-Time-Between-Failure (MTBF) as depicted in the following table:

Service Type	MTBF
L1	365 days
L2	180 days
L3	30 days

8.2.4.2 Verification Method: Analysis

8.2.5 Requirement ID: IKM-SRS-294

8.2.5.1 IKM Tools shall exhibit a Mean-Time-Between-Critical-Failures (MTBCF) of more than 730 consecutive days.

8.2.5.2 Verification Method: Analysis

8.3 Availability

8.3.1 Degree to which a system, product or component is operational and accessible when required for use.

8.3.2 Here considered only the Inherent Availability (Intrinsic): assumes ideal support (i.e., unlimited spares, no delays, etc.), only design related failures are considered.

8.3.3 Inherent Availability

8.3.4 Inherent Availability (Intrinsic) assumes ideal support (i.e., unlimited spares, no delays, etc.); only design related Failures are considered.

8.3.5 Requirement ID: IKM-SRS-295

8.3.5.1 The IKM Tools shall have a System Inherent Availability at Data Centres and Standalone modes (static and deployed) as depicted in the table below:

Service Type	Inherent Availability
L1	99.97 %
L2	99.9 %
L3	99 %

8.3.5.2 Verification Method: Analysis

8.4 Fault Tolerance

8.4.1 Degree to which a system, product or component operates as intended despite the presence of hardware or software faults.

8.4.2 Requirement ID: IKM-SRS-296

8.4.2.1 For the 99% of the possible fault/error in one of the system node, the system shall be able to switch to another equivalent node in less than 5 seconds without loss of data.

8.4.2.2 Verification Method: Analysis

8.5 Adaptability

8.5.1 Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.

8.5.2 Requirement ID: IKM-SRS-312

8.5.2.1 The IKM Tools web capability shall be able to be run at least in the AFPL web browsers and versions: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari. Especially for the ITM provided web browser.

8.5.2.2 Verification Method: Test

8.6 Installability

8.6.1 Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

8.6.2 Requirement ID: IKM-SRS-315

8.6.2.1 The IKM Tools shall be successfully installed and/or uninstalled in a specified environment effectively and efficiently.

8.6.2.2 Verification Method: Analysis

8.6.3 Requirement ID: IKM-SRS-315b

8.6.3.1 The IKM Tools shall be automatically installed via a Graphical User Interface (GUI).

8.6.3.2 Verification Method: Analysis

8.6.4 Requirement ID: IKM-SRS-315c

8.6.4.1 The IKM Tools components and/or patches shall be capable of being installed in an automated way, e.g: by a Windows Installer or similar service/product installation package.

8.6.4.2 Verification Method: Analysis

8.6.5 Requirement ID: IKM-SRS-318

8.6.5.1 The IKM Tools shall detect, during installation and uninstallation, if the user has sufficient privileges required for the action. The IKM Tools shall report the details of the access failure to the user before aborting the (un)installation.

8.6.5.2 Verification Method: Test

8.6.6 Requirement ID: IKM-SRS-319

8.6.6.1 The IKM Tools shall be equipped with an Installation Guide.

8.6.6.2 Verification Method: Analysis

8.6.7 Requirement ID: IKM-SRS-320

8.6.7.1 The IKM Tools Installation Guide shall explain all actions to take in order to install and configure the IKM Tools, including COTS components, and underlying needed services and hardware configurations (i.e. Share Point farm). Every action shall be followed by a description (text and/or screenshots) of the feedback which will be displayed.

8.6.7.2 Verification Method: Analysis

8.6.8 Requirement ID: IKM-SRS-321

8.6.8.1 The IKM Tools Installation Guide shall describe:

- Prerequisites for installing the IKM Tools. (e.g., the necessary OS access right to be able to install the IKM Tools).
- The necessary software, drivers, etc. to install the IKM Tools.
- How to address integration in the 'environment' (node) - like configuration of monitoring and backup functions.
- The (environment specific) configuration changes necessary on the system and the environment.

- The required disc space.

8.6.8.2 Verification Method: Analysis

8.6.9 Requirement ID: IKM-SRS-322

8.6.9.1 The IKM Tools Installation Guide shall describe how to configure the system backbone to be able to run the IKM Tools.

8.6.9.2 Verification Method: Analysis

8.6.10 Requirement ID: IKM-SRS-323

8.6.10.1 The IKM Tools Installation Guide shall describe how to configure the DBMS for the IKM Tools. This shall include both the data model and any access/replication mechanism.

8.6.10.2 Verification Method: Analysis

8.6.11 Requirement ID: IKM-SRS-324

8.6.11.1 The IKM Tools Installation Guide shall contain a description of all configuration files. The following points shall be described:

- The location of the configuration file
- The content of the configuration file
- The available settings of the items in the configuration file and their meaning
- How to change the configuration file

8.6.11.2 Verification Method: Analysis

8.6.12 Requirement ID: IKM-SRS-325

8.6.12.1 The IKM Tools shall provide a GUI automated capability to completely uninstall the IKM Tools application(s)/component(s).

8.6.12.2 Verification Method: Test

8.6.13 Requirement ID: IKM-SRS-326

8.6.13.1 The IKM Tools shall allow, as appropriate, "Complete" and "Stand alone" (un)installation options to perform complete (i.e., all components) and Standalone (i.e., reduced-selected components), respectively.

8.6.13.2 Verification Method: Analysis

8.7 Internationalisation

8.7.1 Requirement ID: IKM-SRS-327

8.7.1.1 The IKM Tools shall change effectively and efficiently to deal with additional international conventions in terms of language, time zones and alike localization functionalities.

8.7.1.2 Verification Method: Analysis

8.8 Replaceability

8.8.1 Degree to which a product can replace another specified software product for the same purpose in the same environment

9 Usability

- 9.1 Degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. Usability can either be specified or measured as a product quality characteristic in terms of its sub characteristics, or specified or measured directly by measures that are a subset of quality in use.
- 9.2 Requirement ID: IKM-SRS-328
 - 9.2.1 The content and information within the system shall be presented to the user in a consistent, standardized manner.
 - 9.2.2 Verification Method: Test
- 9.3 Requirement ID: IKM-SRS-329
 - 9.3.1 Every input by a user shall consistently produce some perceptible response output from the computer.
 - 9.3.2 Verification Method: Test
- 9.4 Requirement ID: IKM-SRS-330
 - 9.4.1 Only data essential to the user's needs shall be displayed.
 - 9.4.2 Verification Method: Inspection
- 9.5 Requirement ID: IKM-SRS-331
 - 9.5.1 Given a simple Test Suite relative to the major functionalities of the IKM Tools (e.g. a search, the upload of a document, the completion of a workflow task), after an introductory training of no more than 1 hour, the 95% of a population of at least 50 users (randomly selected from the population of the real users that has never been exposed to the new KM Tools developed by the Contractor) will be able to complete the Test Suite in less than 5 minutes
 - 9.5.2 Verification Method: Test
- 9.6 Requirement ID: IKM-SRS-332
 - 9.6.1 The dedicated user roles for the IKM Tools shall adhere to the minimum user rights needed to operate the tools, so that no more than needed rights are assigned to a particular user role (i.e. : End User doesn't need to have System Administration permissions to simply operate the IKM Tools basic functions).
 - 9.6.2 Verification Method: Test

10 Security

- 10.1 Security is defined as the capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and such that authorised persons or systems are not denied access to them. As well as data stored in or by a product or system, security also applies to data in transmission.
- 10.2 For purposes of this document, the following definitions are used:
 - 10.2.1 Confidentiality: the property that information is not made available or disclosed to unauthorised individuals or entities.

- 10.2.2 Integrity: the property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
- 10.2.3 Non-repudiation: the measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients.
- 10.2.4 Accountability: the degree to which actions of an entity can be traced uniquely to the entity.
- 10.2.5 Authenticity: the degree to which the identity of a subject or resource can be proved to be the one claimed.
- 10.3 The following CIS Security functionalities will be provided by the BI-SC AIS:
 - 10.3.1 Confidentiality: Military-grade NATO IP cryptographic equipment (NICE) will provide confidentiality to User data as well as cryptographic separation between security Domains (for example, NATO SECRET, NATO UNCLASSIFIED, MISSION SECRET). Information exchange between these security domains will be achieved through appropriate boundary protection services (BPS). As a minimum, NICE will be located at each boundary between the local area networks (LANs) and the NATO wide area network (WAN). This will ensure that all User data will be encrypted prior to transmission across the NATO WAN. Software application layer mechanisms will be used for Community-of-Interest (COI) separation.
 - 10.3.2 Integrity: Digital signatures and authentication services will be used by various protocols (e.g., SNMP, IPSEC) to provide integrity and strong authentication to User data and network configurations. The NATO Public Key Infrastructure (NPKI) will enable these specific security services.
- 10.4 Infrastructure security as provided by the Bi-SC AIS Infrastructure will be transparent to the IKM Tools.
- 10.5 Requirement ID: IKM-SRS-333
 - 10.5.1 The IKM Tools shall be compliant with NATO document [C-M(2002)49] for the protection of NATO classified information, supporting systems services and resources in CIS, or other storing devices, processing and transmitting systems.
 - 10.5.2 Verification Method: Analysis
- 10.6 Requirement ID: IKM-SRS-334
 - 10.6.1 The IKM Tools components shall be configured with the latest security patches and updated with the latest security guidelines from the NATO Information Assurance Technical Centre (NIATC). This shall be enforced on all environments (e.g. operational environment, training environment, reference systems environment), while applying the appropriate CM process and procedures.
 - 10.6.2 Verification Method: Analysis
- 10.7 Requirement ID: IKM-SRS-335

10.7.1 The IKM Tools shall be capable of operating within the NS and MS WAN environment (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.

10.7.2 Verification Method: Test

10.8 Requirement ID: IKM-SRS-336

10.8.1 The IKM Tools shall adhere to the "CIS Security Technical and Implementation Directive for the Security of Web Applications" (NHQC3S(C3CAM)0014-2019 (INV), 26 Sept. 2019) for securing the web services and applications.

10.8.2 Verification Method: Analysis

10.9 Confidentiality

10.9.1 Requirement ID: IKM-SRS-337

10.9.1.1 The IKM Tools shall ensure that a confidentiality label (policy, classification, releasability) is automatically included into each the IKM Tools information <element or product>, showing the highest classification of information it contains.

10.9.1.2 Verification Method: Analysis

10.9.2 Requirement ID: IKM-SRS-338

10.9.2.1 In line with C-M(2002)49-COR12 , the Security Classification in the IKM Tools shall include:

- Policy Identifier/ Information Ownership: e.g. NATO, NATO/EAPC (Euro-Atlantic Partnership Council), ISAF (International Security Assistance Force)
- Classification Marking: e.g. Unclassified, Restricted, Confidential, Secret
- Category/Caveats: e.g. Releasable to AUS/FIN, Releasable to RS, Releasable to Coalition

10.9.2.2 Verification Method: Analysis

10.9.3 Requirement ID: IKM-SRS-339

10.9.3.1 The machine readable structure of the Security Label in the IKM Tools shall be in accordance with INFOSEC Technical & Implementation Guidance for Electronic Labelling of NATO Information [AC/322-D (2004)0021].

10.9.3.2 Verification Method: Analysis

10.9.4 Requirement ID: IKM-SRS-340

10.9.4.1 The IKM Tools shall provide visual confirmation to Users (on-screen) of the security classification including any releasability caveats (e.g., Releasable to RS) of the displayed data.

10.9.4.2 Verification Method: Inspection

10.9.5 Requirement ID: IKM-SRS-341

- 10.9.5.1 The IKM Tools shall include a configurable colour-based visual cue in addition to text to indicate security classification in screens, reports and prints.
- 10.9.5.2 Verification Method: Test
- 10.9.6 Requirement ID: IKM-SRS-342
- 10.9.6.1 The IKM Tools 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.
- 10.9.6.2 Verification Method: Inspection
- 10.9.7 Requirement ID: IKM-SRS-343
- 10.9.7.1 The IKM Tools 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.
- 10.9.7.2 Verification Method: Test
- 10.9.8 Requirement ID: IKM-SRS-344
- 10.9.8.1 The IKM Tools 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, and releasability.
- 10.9.8.2 Verification Method: Test
- 10.10 Integrity
- 10.10.1 Requirement ID: IKM-SRS-345
- 10.10.1.1 The IKM Tools shall maintain referential integrity between entities across all services avoiding orphan entities (e.g.: deletion of a workflow results in deletion of all related entities: sub activities, sub-workspaces, documents and alike).
- 10.10.1.2 Verification Method: Analysis
- 10.10.2 Requirement ID: IKM-SRS-346
- 10.10.2.1 The IKM Tools shall implement a two-phase deletion process (i.e., a logical/soft delete with User-controlled permanent deletion/purging) for entities.
- 10.10.2.2 Verification Method: Analysis

11 Web Security

11.1 Authentication

11.1.1 Requirement ID: IKM-SRS-380

11.1.1.1 Authentication shall be through an authorized identity provider. Where appropriate, other authentication requirements shall be enforced by the authorized identity provider.

11.1.1.2 Verification Method: Analysis

11.1.2 Requirement ID: IKM-SRS-381

11.1.2.1 Identity Information related to authentication (such as credentials) managed by the website shall not traverse public networks unencrypted.

11.1.2.2 Verification Method: Analysis

11.1.3 Requirement ID: IKM-SRS-382

11.1.3.1 Forgot password functionality and other recovery paths shall do not send the existing or new passwords in clear text to the user.

11.1.3.2 Verification Method: Analysis

11.1.4 Requirement ID: IKM-SRS-383

11.1.4.1 No default passwords shall be used, for the website or any components.

11.1.4.2 Verification Method: Analysis

11.1.5 Requirement ID: IKM-SRS-384

11.1.5.1 Passwords shall never be hard-coded in any source code. Not even in an encrypted/hashed form.

11.1.5.2 Verification Method: Analysis

11.1.6 Requirement ID: IKM-SRS-385

11.1.6.1 All authentication controls shall be enforced on the server side.

11.1.6.2 Verification Method: Analysis

11.1.7 Requirement ID: IKM-SRS-386

11.1.7.1 Account passwords shall be stored encrypted or hashed in such a way it should not be possible to identify identical passwords.

11.1.7.2 Verification Method: Analysis

11.1.8 Requirement ID: IKM-SRS-387

11.1.8.1 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.

11.1.8.2 Verification Method: Analysis

11.1.9 Requirement ID: IKM-SRS-388

11.1.9.1 Authentication credentials shall be configured to expire after an administratively configurable period.

11.1.9.2 Verification Method: Test

11.1.10 Requirement ID: IKM-SRS-389

- 11.1.10.1 All authentication decisions shall be logged, including increased delays between successive unsuccessful logging attempts (linear back-offs) and temporal account locks (soft-locks).
- 11.1.10.2 Verification Method: Test
- 11.1.11 Requirement ID: IKM-SRS-390
- 11.1.11.1 Forgotten password and other recovery paths shall send a time-limited activation token or use two factor proofs
- 11.1.11.2 Verification Method: Test
- 11.1.12 Requirement ID: IKM-SRS-391
- 11.1.12.1 The IKM Tools implementation shall be compatible with FMN Spiral 4 Service Instructions for Web Authentication.
- 11.1.12.2 Verification Method: Analysis
- 11.2 Session Management
- 11.2.1 Requirement ID: IKM-SRS-392
- 11.2.1.1 A session management mechanism shall be used after a successful authentication, and the related security context shall be maintained until the session expires. Any change in the security context shall require re-authentication.
- 11.2.1.2 Verification Method: Test
- 11.2.2 Requirement ID: IKM-SRS-393
- 11.2.2.1 Sessions shall be invalidated when the user logs out.
- 11.2.2.2 Verification Method: Test
- 11.2.3 Requirement ID: IKM-SRS-394
- 11.2.3.1 Sessions shall timeout after a specified period of inactivity.
- 11.2.3.2 Verification Method: Test
- 11.2.4 Requirement ID: IKM-SRS-395
- 11.2.4.1 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.
- 11.2.4.2 Verification Method: Test
- 11.2.5 Requirement ID: IKM-SRS-396
- 11.2.5.1 Session ID shall be changed or cleared on logout or when the session expires.
- 11.2.5.2 Verification Method: Test
- 11.2.6 Requirement ID: IKM-SRS-397
- 11.2.6.1 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)
- 11.2.6.2 Verification Method: Inspection
- 11.2.7 Requirement ID: IKM-SRS-398
- 11.2.7.1 The Session ID shall be changed on re-authentication.

11.2.7.2 Verification Method: Test

11.2.8 Requirement ID: IKM-SRS-399

11.2.8.1 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.

11.2.8.2 Verification Method: Test

11.2.9 Requirement ID: IKM-SRS-400

11.2.9.1 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.

11.2.9.2 Verification Method: Test

11.2.10 Requirement ID: IKM-SRS-401

11.2.10.1 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.

11.2.10.2 Verification Method: Test

11.2.11 Requirement ID: IKM-SRS-402

11.2.11.1 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.

11.2.11.2 Verification Method: Test

11.2.12 Requirement ID: IKM-SRS-403

11.2.12.1 The application shall not permit duplicate concurrent user sessions, originating from different machines.

11.2.12.2 Verification Method: Test

11.3 Access Control

11.3.1 Requirement ID: IKM-SRS-404

11.3.1.1 Access controls shall be enforced on the server side.

11.3.1.2 Verification Method: Analysis

11.3.2 Requirement ID: IKM-SRS-405

11.3.2.1 User and data attributes and policy information used by access controls shall not be manipulated by end users unless specifically authorized.

11.3.2.2 Verification Method: Analysis

11.4 Input validation

11.4.1 Requirement ID: IKM-SRS-406

11.4.1.1 The runtime environment shall not be susceptible to buffer overflows, or there shall be security controls preventing buffer overflows.

11.4.1.2 Verification Method: Test

11.4.2 Requirement ID: IKM-SRS-407

11.4.2.1 The runtime environment shall not susceptible to SQL Injection, or there shall be security controls preventing SQL Injection.

11.4.2.2 Verification Method: Test

11.4.3 Requirement ID: IKM-SRS-408

11.4.3.1 The runtime environment shall not susceptible to Cross Site Scripting (XSS), or there shall be security controls preventing XSS Injection.

11.4.3.2 Verification Method: Test

11.4.4 Requirement ID: IKM-SRS-409

11.4.4.1 The runtime environment shall not susceptible to LDAP Injection, or there shall be security controls preventing LDAP Injection.

11.4.4.2 Verification Method: Test

11.4.5 Requirement ID: IKM-SRS-410

11.4.5.1 The runtime environment shall not susceptible to OS Command Injection, or there shall be security controls preventing OS Command Injection.

11.4.5.2 Verification Method: Test

11.4.6 Requirement ID: IKM-SRS-411

11.4.6.1 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.

11.4.6.2 Verification Method: Test

11.4.7 Requirement ID: IKM-SRS-412

11.4.7.1 All input validation failures shall result in input rejection or input sanitization in accordance with the NCIRC guidance.

11.4.7.2 Verification Method: Analysis

11.4.8 Requirement ID: IKM-SRS-413

11.4.8.1 Input validation or encoding routines shall be performed and enforced on the server side in accordance with the NCIRC guidance.

11.4.8.2 Verification Method: Analysis

11.4.9 Requirement ID: IKM-SRS-414

11.4.9.1 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.

11.4.9.2 Verification Method: Analysis

11.4.10 Requirement ID: IKM-SRS-415

11.4.10.1 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.

11.4.10.2 Verification Method: Analysis

11.5 Cryptography at rest

11.5.1 Requirement ID: IKM-SRS-416

11.5.1.1 All cryptographic functions shall be implemented on the server side unless purposely designed in another manner.

11.5.1.2 Verification Method: Analysis

11.5.2 Requirement ID: IKM-SRS-417

11.5.2.1 Data-at-rest decryption keys shall be protected from unauthorized access.

11.5.2.2 Verification Method: Analysis

11.5.3 Requirement ID: IKM-SRS-418

11.5.3.1 Cryptographic keys shall be managed (e.g., generated, distributed, revoked, expired) using approved NATO policies [AC/322-D/0047, 2009].

11.5.3.2 Verification Method: Analysis

11.5.4 Requirement ID: IKM-SRS-419

11.5.4.1 Cryptographic algorithms used by the application shall be selected from the NATO Type B algorithm suite.

11.5.4.2 Verification Method: Analysis

11.6 Error handling and Logging

11.6.1 Requirement ID: IKM-SRS-420

11.6.1.1 The application shall not output error messages or stack traces containing sensitive data that could assist an attacker, including Session ID and personal information.

11.6.1.2 Verification Method: Test

11.6.2 Requirement ID: IKM-SRS-421

11.6.2.1 Logs events shall include at a minimum:

- Time stamp from a reliable source
- Severity level of the event
- An indication that this is a security relevant event (if mixed with other logs)
- The identity of the user that caused the event (if there is a user associated with the event)
- The source IP address of the request associated with the event
- Status of the event (e.g. succeeded or failed)
- A description of the event

11.6.2.2 Verification Method: Test

11.6.3 Requirement ID: IKM-SRS-422

11.6.3.1 Logging controls shall be implemented on the server.

11.6.3.2 Verification Method: Analysis

11.6.4 Requirement ID: IKM-SRS-423

- 11.6.4.1 Security logging controls shall have the ability to log both success and failure events that are identified as security-relevant.
- 11.6.4.2 Verification Method: Test
- 11.6.5 Requirement ID: IKM-SRS-424
- 11.6.5.1 Security logs shall be protected from unauthorized access and modification.
- 11.6.5.2 Verification Method: Analysis
- 11.6.6 Requirement ID: IKM-SRS-425
- 11.6.6.1 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.
- 11.6.6.2 Verification Method: Test
- 11.7 Data Protection
- 11.7.1 Requirement ID: IKM-SRS-426
- 11.7.1.1 Forms containing sensitive information shall have disabled client side caching, including autocomplete features.
- 11.7.1.2 Verification Method: Test
- 11.7.2 Requirement ID: IKM-SRS-427
- 11.7.2.1 Sensitive data shall be sent to the server in the HTTP message body (i.e., URL parameters are never used to send sensitive data).
- 11.7.2.2 Verification Method: Test
- 11.7.3 Requirement ID: IKM-SRS-428
- 11.7.3.1 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).
- 11.7.3.2 Verification Method: Test
- 11.7.4 Requirement ID: IKM-SRS-429
- 11.7.4.1 The list of sensitive data processed by the 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).
- 11.7.4.2 Verification Method: Test
- 11.7.5 Requirement ID: IKM-SRS-430
- 11.7.5.1 There shall be a method to remove each type of sensitive data from the application at the end of its required retention period.
- 11.7.5.2 Verification Method: Test
- 11.7.6 Requirement ID: IKM-SRS-431
- 11.7.6.1 The integrity of interpreted code, libraries, executables, and configuration files shall be verified using checksums or hashes.
- 11.7.6.2 Verification Method: Test

11.7.7 Requirement ID: IKM-SRS-432

11.7.7.1 Sensitive data shall be rapidly sanitized from memory as soon as it is no longer needed.

11.7.7.2 Verification Method: Test

11.7.8 Requirement ID: IKM-SRS-433

11.7.8.1 The 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.

11.7.8.2 Verification Method: Test

11.8 Communications Security

11.8.1 Requirement ID: IKM-SRS-434

11.8.1.1 IKM Tools certificates shall have a path 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.

11.8.1.2 Verification Method: Inspection

11.8.2 Requirement ID: IKM-SRS-435

11.8.2.1 TLS shall be used for all connections, internal (e.g. backend) or external, that involve sensitive data or functions.

11.8.2.2 Verification Method: Test

11.8.3 Requirement ID: IKM-SRS-436

11.8.3.1 Backend TLS connection failures shall be logged.

11.8.3.2 Verification Method: Test

11.8.4 Requirement ID: IKM-SRS-437

11.8.4.1 Connections to external systems that involve sensitive information or functions shall be authenticated.

11.8.4.2 Verification Method: Test

11.8.5 Requirement ID: IKM-SRS-438

11.8.5.1 Connections to/from external systems shall use accounts configured to have the minimum privileges necessary for the application to function properly.

11.8.5.2 Verification Method: Test

11.8.6 Requirement ID: IKM-SRS-439

11.8.6.1 Failed TLS connections shall not fall back to an insecure connection.

11.8.6.2 Verification Method: Test

11.8.7 Requirement ID: IKM-SRS-440

11.8.7.1 Certificate paths shall be built for all client certificates using configured trust anchors and revocation information.

11.8.7.2 Verification Method: Test

11.8.8 Requirement ID: IKM-SRS-441

11.8.8.1 The application shall use a single standard TLS implementation that is configured to operate in an approved mode of operation

11.8.8.2 Verification Method: Test

11.8.9 Requirement ID: IKM-SRS-442

11.8.9.1 Specific character encodings shall be defined for all connections (e.g., UTF-8).

11.8.9.2 Verification Method: Test

11.9 HTTP Security

11.9.1 Requirement ID: IKM-SRS-443

11.9.1.1 The application shall accept only a defined set of HTTP request methods, such as GET and POST, unused methods shall be explicitly blocked.

11.9.1.2 Verification Method: Test

11.9.2 Requirement ID: IKM-SRS-444

11.9.2.1 Every HTTP response shall contain a single content type header specifying a safe character set (e.g., UTF-8).

11.9.2.2 Verification Method: Test

11.9.3 Requirement ID: IKM-SRS-445

11.9.3.1 HTTP headers, in both requests and responses, and URIs shall contain only printable ASCII characters.

11.9.3.2 Verification Method: Test

11.9.4 Requirement ID: IKM-SRS-446

11.9.4.1 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.

11.9.4.2 Verification Method: Test

11.9.5 Requirement ID: IKM-SRS-447

11.9.5.1 If HTTPS is required, the web application shall make use of "HTTP Strict Transport Security (HSTS)" (previously called STS) to enforce HTTPS connections.

11.9.5.2 Verification Method: Test

11.9.6 Requirement ID: IKM-SRS-448

11.9.6.1 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.

11.9.6.2 Verification Method: Test

11.9.7 Requirement ID: IKM-SRS-449

- 11.9.7.1 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
- 11.9.7.2 Verification Method: Test
- 11.10 Files and resources
 - 11.10.1 Requirement ID: IKM-SRS-450
 - 11.10.1.1 Files, other than static pages and dynamic content (CGI scripts), shall be stored outside the Webroot.
 - 11.10.1.2 Verification Method: Analysis
 - 11.10.2 Requirement ID: IKM-SRS-451
 - 11.10.2.1 The web or application server shall be configured by default to deny access to remote resources or systems outside the web or application server.
 - 11.10.2.2 Verification Method: Analysis
 - 11.10.3 Requirement ID: IKM-SRS-452
 - 11.10.3.1 The application code shall not execute uploaded data.
 - 11.10.3.2 Verification Method: Analysis
 - 11.10.4 Requirement ID: IKM-SRS-453
 - 11.10.4.1 Rich internet applications cross domain resource sharing configuration shall be configured to prevent unauthenticated or unauthorized remote access.
 - 11.10.4.2 Verification Method: Analysis
 - 11.10.5 Requirement ID: IKM-SRS-454
 - 11.10.5.1 Remote IFRAMEs and HTML 5 cross-domain resource sharing shall not allow inclusion of arbitrary remote content.
 - 11.10.5.2 Verification Method: Analysis
- 11.11 Miscellaneous (HTML5/JavaScript/ActiveX)
 - 11.11.1 Requirement ID: IKM-SRS-455
 - 11.11.1.1 Sensitive data shall not be stored in storage area of a thick client, including to system or application logs.
 - 11.11.1.2 Verification Method: Analysis
 - 11.11.2 Requirement ID: IKM-SRS-456
 - 11.11.2.1 3rd-party JavaScript libraries or thick-client shall be hosted within the web application/web server and not hot-linked from external untrusted sources
 - 11.11.2.2 Verification Method: Analysis
 - 11.11.3 Requirement ID: IKM-SRS-457
 - 11.11.3.1 Thick clients shall not request more permissions or access to resources than those strictly required for its correct operation

- 11.11.3.2 Verification Method: Analysis
- 11.11.4 Requirement ID: IKM-SRS-458
- 11.11.4.1 3rd-party JavaScript libraries in use shall be up to date and contain no known vulnerabilities.
- 11.11.4.2 Verification Method: Analysis
- 11.11.5 Requirement ID: IKM-SRS-459
- 11.11.5.1 Thick-client code shall be signed.
- 11.11.5.2 Verification Method: Test
- 11.11.6 Requirement ID: IKM-SRS-460
- 11.11.6.1 Thick-client shall be configured to run in a restricted sandbox, with no access to OS resources, such as file system or native libraries.
- 11.11.6.2 Verification Method: Test
- 11.11.7 Requirement ID: IKM-SRS-461
- 11.11.7.1 The thick-client binary shall be obfuscated.
- 11.11.7.2 Verification Method: Test
- 11.11.8 Requirement ID: IKM-SRS-462
- 11.11.8.1 The thick client shall implement certificate pinning to prevent the proxying of app traffic.
- 11.11.8.2 Verification Method: Test
- 11.11.9 Requirement ID: IKM-SRS-463
- 11.11.9.1 The query string shall not be used for sensitive data. Instead, a POST request via SSL should be used with a CSRF token.
- 11.11.9.2 Verification Method: Test

12 Interface Requirements

- 12.1 Interoperability is defined in ISO 25010 as the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged.
- 12.2 Within NATO, interoperability is defined as, the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.
- 12.3 Requirement ID: IKM-SRS-464
- 12.3.1 The IKM Tools software code and components shall comply with the latest version of the NATO Interoperability Standards and Profiles (NISP). Any deviation is to be justified and reviewed by the Technical Project Board.
- 12.3.2 Verification Method: Analysis
- 12.4 Requirement ID: IKM-SRS-465
- 12.4.1 If new interoperability profiles are to be developed (e.g.: new templates) they shall be compliant and included into the NISP volumes. The interfaces will use the IKM Tools Data Model and be compliant to NATO Core Metadata Specification.
- 12.4.2 Verification Method: Analysis
- 12.5 Interface Mechanisms
- 12.5.1 Requirement ID: IKM-SRS-467
- 12.5.1.1 The following information exchange mechanisms can be used in the IKM Tools:
- Web services
 - File exchange
 - Direct database and file access (justification needed)
 - API (justification needed)
- 12.5.1.2 Verification Method: Analysis

12.6 Interface Security

12.6.1 Requirement ID: IKM-SRS-473

12.6.1.1 The IKM Tools shall use Generic Security Services Application Program Interface (GSS API), as possible, as the application programming interface for accessing security services.

12.6.1.2 Verification Method: Analysis

12.6.2 Requirement ID: IKM-SRS-474

12.6.2.1 The IKM Tools primary security services (access control, confidentiality, integrity, authentication, and non-repudiation) shall be supported by X.509.

12.6.2.2 Verification Method: Analysis

12.6.3 Requirement ID: IKM-SRS-475

12.6.3.1 The IKM Tools X.509 support to primary security services shall be compliant with NPKI.

13 Architectural Constraints

13.1 Requirement ID: IKM-SRS-513

13.1.1 The IKM Tools shall be compliant with the standards given in the SoW section Applicable Documents. Any proposed deviation shall be approved by the Purchaser.

13.1.2 Verification Method: Analysis

13.2 Requirement ID: IKM-SRS-513b

13.2.1 The IKM Tools shall be compliant with the Microsoft supportability limitations so that the recommended limitation are not breached, i.e. maximum number of Sites per Site Collection or maximum Content Database size) (see Ref. [Software boundaries and limits for SharePoint Servers 2016 and 2019]). Any proposed deviation shall be approved by the Purchaser.

13.2.2 Verification Method: Analysis

13.3 Requirement ID: IKM-SRS-514

13.3.1 The IKM Tools shall be designed and implemented with economy of bandwidth (e.g., caching, light-weight previewing, metadata exchange, lazy loading).

13.3.2 Verification Method: Analysis

13.4 Requirement ID: IKM-SRS-515

13.4.1 The proposed software architecture, development environment, middleware system and the separation of components (Human Machine Interface, Business and Data) for the IKM Tools shall be documented and explained in detail.

13.4.2 Verification Method: Analysis

13.5 Requirement ID: IKM-SRS-516

13.5.1 The IKM Tools shall expose selected functionality as Services, as components of a service-oriented architecture to encourage reuse and interoperability with other applications in a distributed way. The criteria used for selection of functionality shall be documented.

13.5.2 The IKM Tools services shall comply with the C3 Classification Taxonomy and applicable Service Interface Profiles.

13.5.3 Verification Method: Analysis

13.6 Requirement ID: IKM-SRS-518

13.6.1 The IKM Tools shall, where applicable, make use of REST architecture to make resources available over a URL in promotion of interoperability.

13.6.2 Verification Method: Analysis

13.7 Requirement ID: IKM-SRS-519

13.7.1 The IKM Tools design process shall balance design implementation with cost for implementation and support to minimise life cycle cost. The IKM Tools design shall take into account the technical, support and cost impacts for NATO.

13.7.2 Verification Method: Analysis

14 Graphical User Interface (GUI)

14.1 NCIA and NATO guidelines

14.1.1 Bi-SC AIS applications are developed as projects within NCIA to be used by NATO users. Both NCIA and NATO have their own standards and guidelines that will influence or directly affect Bi-SC AIS applications' visual design. Although Bi-SC AIS applications can have their own identity, any new application needs to feel like other products NCIA or NATO have previously created and share the same organizational values.

14.1.2 Requirement ID: IKM-SRS-537

14.1.2.1 The IKM Tools visual design shall follow the recommendations and guidelines stated in the following documents:

- NATO Visual Identity Guidelines

- NCIA Visual Identity Guidelines

14.1.2.2 Verification Method: Inspection

14.1.3 Requirement ID: IKM-SRS-538

14.1.3.1 The IKM Tools shall follow the recommendations and guidelines of the HMI Style Guide for C4ISR Rich Applications regarding to windows and layouts, user interactions, user support and feedback, common user interface components design, visual design and text use.

14.1.3.2 Verification Method: Inspection

14.2 ISO standards

14.2.1 Requirement ID: IKM-SRS-539

14.2.1.1 The IKM Tools icons included in the designed solution shall be compliant with the ISO 18152 standard series.

14.2.1.2 Verification Method: Analysis

14.2.2 Requirement ID: IKM-SRS-540

14.2.2.1 The IKM Tools shall be compliant with the ISO 9241 standard series. In particular:

14.2.2.2 Verification Method: Analysis

14.2.3 Requirement ID: IKM-SRS-541

14.2.3.1 The IKM Tools shall be compliant to ISO 9241-125 for the presentation of information.

14.2.3.2 Verification Method: Analysis

14.2.4 Requirement ID: IKM-SRS-542

14.2.4.1 The IKM Tools shall be compliant to ISO 9241-13 for user guidance.

14.2.4.2 Verification Method: Analysis

14.2.5 Requirement ID: IKM-SRS-543

14.2.5.1 The IKM Tools shall be compliant to ISO 9241-14 for menu dialogues.

14.2.5.2 Verification Method: Analysis

14.2.6 Requirement ID: IKM-SRS-544

14.2.6.1 The IKM Tools shall be compliant to ISO 9241-143 for form filling dialogues

14.2.6.2 Verification Method: Analysis

14.2.7 Requirement ID: IKM-SRS-545

14.2.7.1 The IKM Tools shall be compliant to ISO 9241-171 for accessibility.

14.2.7.2 Verification Method: Analysis

14.2.8 Requirement ID: IKM-SRS-546

14.2.8.1 The IKM Tools shall follow the dialogue principles stated in ISO 9241-110 or ISO/DIS 9241-110 (if available)

14.2.8.2 Verification Method: Analysis

14.3 Log-on procedures

14.3.1 Requirement ID: IKM-SRS-547

- 14.3.1.1 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.
- 14.3.1.2 Verification Method: Analysis
- 14.3.2 Requirement ID: IKM-SRS-548
- 14.3.2.1 Appropriate prompts for log-on should be automatically displayed on the user's terminal when accessing the application.
- 14.3.2.2 Verification Method: Analysis
- 14.3.3 Requirement ID: IKM-SRS-549
- 14.3.3.1 User identification procedures shall be as simple as possible, consistent with adequate data protection.
- 14.3.3.2 Verification Method: Analysis
- 14.3.4 Requirement ID: IKM-SRS-550
- 14.3.4.1 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.
- 14.3.4.2 Verification Method: Analysis
- 14.3.5 Requirement ID: IKM-SRS-551
- 14.3.5.1 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.
- 14.3.5.2 Verification Method: Analysis
- 14.3.6 Requirement ID: IKM-SRS-552
- 14.3.6.1 Users should be allowed to change passwords whenever they choose; all passwords should be changed at periodic intervals (not to exceed a configurable number of months).
- 14.3.6.2 Verification Method: Analysis
- 14.3.7 Requirement ID: IKM-SRS-553
- 14.3.7.1 Users shall be provided feedback relevant to the log-on procedure that indicates the status of the inputs.
- 14.3.7.2 Verification Method: Analysis
- 14.3.8 Requirement ID: IKM-SRS-554
- 14.3.8.1 If a user cannot log-on to a system, a prompt should 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.
- 14.3.8.2 Verification Method: Analysis
- 14.4 Log-off procedures
- 14.4.1 Requirement ID: IKM-SRS-555

- 14.4.1.1 When a user signals for system log-off, or application exit or shut-down, the system should 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.



NATO Communications and Information Agency
Agence OTAN d'information et de communication

**PROVIDE BMD EXERCISE INFORMATION MANAGEMENT PORTAL
TEMPLATE SYSTEM WITHIN BALLISTIC MISSILE DEFENCE (BMD)
FUNCTIONS IN EDUCATION, TRAINING, EXERCISE AND
EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

RFQ-CO-115114-ETEE PORTAL

BOOK II – PART III

STATEMENT OF WORK

Annex C: Coding Principles and Guidelines

Annex C: Coding Principles and Guidelines

Contents

1	Coding Convention.....	3
2	User Interface Styling	3
3	Conformance to design best practices.....	3
4	Conformance to coding quality best practices	3

1 Coding Convention

- 1.1 The following coding conventions shall be adopted and applied consistently by the Contractor across all code artefacts for each programming language employed, as specified in the table below.

Language	Coding convention
C#	Microsoft C# Coding Conventions (https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/inside-a-program/coding-conventions) Apply the Java section of CMU SEI Confluence (https://wiki.sei.cmu.edu/confluence)
C++	SEI CERT C++ Coding Standard (https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682) CMU SEI Confluence (https://wiki.sei.cmu.edu/confluence)
C	SEI CERT C Coding Standard (https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard) CMU SEI Confluence (https://wiki.sei.cmu.edu/confluence)
Javascript	Google Javascript Style Guide (https://google.github.io/styleguide/jsguide.html)
Other	CMU SEI Confluence (https://wiki.sei.cmu.edu/confluence)

2 User Interface Styling

- 2.1 Web-based User Interface styling details shall be kept separate from application code using cascading style sheets (css).

3 Conformance to design best practices

- 3.1 The delivered source code shall follow object oriented design principles known by the SOLID¹ acronym for all code written in the C# or C++ language.

4 Conformance to coding quality best practices

- 4.1 The delivered source code shall be written using commonly applied quality standards to ensure maintainability, reusability, readability and efficiency. Error proneness shall be avoided.
- 4.2 The delivered source code shall contain no more than 5 instances per 100 lines of code of potential mistakes as listed in the MITRE Common Weakness Enumeration (<https://cwe.mitre.org/data/definitions/699.html>)
- 4.3 (*Requirement ID: IKM-SRS-583*) The IKM Tools .Net components shall be developed in compliance of the following Microsoft Visual Studio Code Analysis Tool rule sets:

Verification Method: Inspection

¹ Single responsibility, Open-closed, Liskov substitution, Interface segregation, Dependency inversion, see <http://butunclebob.com/ArticleS.UncleBob.PrinciplesOfOod>

- Microsoft Basic Correctness Rules
 - Microsoft Basic Design Guideline Rules
 - Microsoft Extended Correctness Rules
 - Microsoft Extended Design Guideline Rules
 - Microsoft Minimum Recommended Rules
 - Microsoft Security Rules
- 4.4 (Requirement ID: IKM-SRS-584) Valid exceptions to those rules shall be created for each applicable occurrence (e.g. global exclusion is not allowed unless explicitly approved by the Purchaser)
- 4.5 (*Requirement ID: IKM-SRS-587*) Comments for the source code of the IKM Tools shall be used to clarify intent of the code and shall be provided for:
- Verification Method: Inspection*
- Each class definition explaining the purpose of the class
 - Each member function explaining what the function does, its inputs and outputs
 - Each member variable explaining what the variable means
 - Each type definition (enums) explaining what the type represents
- 4.6 (Requirement ID: IKM-SRS-588) Comments for the source code of the IKM Tools shall be able to be automatically extracted and formatted to augment technical documentation.
- 4.7 (Requirement ID: IKM-SRS-588b) Every method of every class shall contain at minimum the following comments on the header of the method, using the following template:

Verification Method: Inspection

```
<summary>
/// short description mentioning the purpose of this method
/// </summary>
/// <param name="FieldInternalName">the value</param>
/// <param name="anotherInternalName">the valueparam>
/// <returns>value returned</returns>
```



NATO Communications and Information Agency
Agence OTAN d'information et de communication

**PROVIDE BMD EXERCISE INFORMATION MANAGEMENT PORTAL
TEMPLATE SYSTEM WITHIN BALLISTIC MISSILE DEFENCE (BMD)
FUNCTIONS IN EDUCATION, TRAINING, EXERCISE AND
EVALUATION (ETEE) FUNCTIONAL SERVICES (FS)**

RFQ-CO-115114-ETEE PORTAL

BOOK II – PART III

STATEMENT OF WORK

Annex D: Purchaser Furnished Property

Annex D: Purchaser Furnished Property

Contents

1	Introduction.....	3
2	Purchaser Furnished Property	3

1 Introduction

- 1.1 This annex contains a summary of the Purchaser Furnished Property (PFP) made available to the Contractor for the execution of the Contract.

2 Purchaser Furnished Property

- 2.1 The table below list the PFPs with a reference to the relevant section(s) of the SOW.

PFP	SOW section	Provided NLT	Provided until
Virtual Development environment inside the NATO Software Factory	2.7.2	At start of the first sprint	Project closure
Development branches	2.8.3	At the start of each iteration	Completion of the integration of the iteration
Virtual Training Material Development environment inside the NATO Software Factory	3.1.5	At start of the agreed period as per the SoW	End of the agreed period as per the SoW