NATO Communications and Information Agency

Acquisition Office

Boulevard Léopold III
B-1110 Brussels, Belgium

NCIA/ACQ/2023/07106
14 July 2023

To: Dynamic Sourcing - Sprint 3 Successful Participants

Subject: **Request for Solution (RFS) Amendment 2, RFS-CO-115699-ACPV Asset, Configuration, Patching and Vulnerability Management (ACPV) Enterprise Service**

Reference:

A. NCIA/ACQ/2022/07363, Request for Solution RFS-CO-115699-ACPV Asset, Configuration, Patching and Vulnerability Management (ACPV) Enterprise Service, dated 13 December 2022

B. RFS-CO-115699-ACPV Clarification Requests (CR) questions and answers (Q&As), published 23 January 2023

C. NCIA/ACQ/2023/06717, RFS-CO-115699-ACPV Amendment 1, dated 24 March 2023

D. RFS-CO-115699-ACPV Sprint 2 Q&As (Rev.), dated 14 July 2023

Dear Sir/Madam,

1. The purpose of this Amendment 2 is to:
   a. Confirm that Sprint 1 and Sprint 2 have been completed and shift focus to Sprint 3 activities.
   b. Issue revised Request for Solution (RFS) documents as follows:
      - Book I – RFS Instructions
      - Book II Part I – Schedule of Supplies and Services (SSS)
      - Book II Part II – Terms and Conditions
      - Book II Part IV – Statement of Objectives (SOO)
      - Book II Part IV Annex A – Performance Work Statement (PWS)
2. This Amendment makes the following revisions, made with red font for ease of review:
   a. **Book I - RFS Instructions**
      - Minor administrative corrections through the document.
      - Paragraph 1.3 revised security provision with guidance on release of NR documents
      - Paragraph 2.3 revised to include the new delivery and RFS closing date for Sprint 3
      - Annex A-1 revised to include CLIN Summary sheet, and detailed pricing sheets
      - Annex B-15 added to include guidance for the structure and content of Project Security
      - Annex B-16 added compliance certificate for Safeguarding NATO Information Controls
   b. **Book II, Part I – Schedule of Supplies and Services (SSS)**
      - Revised document header for releasability to Sweden.
   c. **Book II, Part II – Terms and Conditions**
      - Article 4 revised to add the required time for implementation of the full service
      - Article 7 revised to include Finland

- Article 28 revised to remove inapplicable language.
- Article 39 added for guidance on handling of Purchaser Furnished Information (PFI)
- Article 40 added for guidance on handling of Purchaser Furnished Property
- Article 41 added for guidance on REACH Capability
- Article 42 added for guidance on cyber incident reporting
- Annex B added to include SLA for the provision of REACH devices

d. **Book II, Part IV – Statement of Objectives (SOO)**

- Paragraph 7.2, removed duplicative sentence.

e. **Book II, Part IV Annex A – Performance Work Statement (PWS)**

- Minor administrative corrections throughout the document recorded with track changes
- Editable final draft prepared for release to Industry.

3. Sprint 2 Questions & Answers (Rev) document resulting from Sprint 2 workshops is hereby incorporated into the RFS.

4. With the exception of the revisions mentioned above, all other RFS documents remain unchanged from their original version as issued on 13 December 2022 and later amended on 24 March 2023.

5. The award will be issued in accordance with the Dynamic Sourcing process using a Best Value (BV) trade-off methodology, as described in Book I - RFS Instructions.

6. With Sprints 1 and 2 closed, two out of three down selection activities are complete. There will be one (1) additional down selection activity remaining in the Dynamic Souring process, at the end of Sprint 3. Firms responding to this RFS Amendment 2 for Sprint 3 will be evaluated in accordance with Sprint 3 specific requirements described in Book I – RFS Instructions.

7. The overall Dynamic Sourcing Sprints are projected to follow the following schedule:

a) Sprint 1: Completed on 09 March 2023
b) Sprint 2: Completed on 30 June 2023
c) Sprint 3: July – August 2023
d) Sprint 4: September 2023

8. THE REQUEST FOR SOLUTION (RFS) SPRINT 3 CLOSING TIME IS SEVEN (7) CALENDAR DAYS OF WHEN THE LAST WORKSHOP WAS HELD.

a) Company A: 08 August 2023 + 7 calendar days = **15 August 2023**
b) Company B: 09 August 2023 + 7 calendar days = **16 August 2023**

NOTE: OFFERS WILL NO BE OPENED UNTIL AFTER ALL OFFERS ARE RECEIVED.

9. Requests for Extensions to RFS closing date are not anticipated at this time.

10. The security classification of this RFS and subsequent Amendments is “NATO UNCLASSIFIED”. This RFS remains the property of the NCI Agency and shall be protected in accordance with the applicable national security regulations.

11. The reference for this RFS is RFS-CO-115699-ACPV, and all correspondence concerning the RFS should include this reference.

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

13. Your point of contact for all information concerning this RFS is the undersigned, who may be reached at RFS-CO-115699-ACPV@ncia.nato.int

For the Chief of Acquisition:

Edel Esparza

Digitally signed by Edel Esparza
Date: 2023.07.14 21:49:02 +02'00'

Edel Esparza
Senior Contracting Officer

Attachment(s): RFS Amendment 2

1. Revised RFS Document(s):
    a. Revised RFS Document(s):
    b. Book I – RFS Instructions
    c. Book II – Part I Schedule for Supplies and Services (SSS)
    d. Book II – Part II Terms and Conditions
    e. Book II – Part IV Statement of Objectives (SOO)
    f. Book II – Part IV Annex A Performance Work Statement (PWS)

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

NATO Communications and Information Academy

NCI AGENCY

BOOK I

RFS INSTRUCTIONS

TABLE OF CONTENTS

SECTION 1. **INTRODUCTION**

1.1 PURPOSES

1.1.1 The purpose of this Request for Solution (RFS) is to award a Contract for the provision of an Asset, Configuration, Patching and Vulnerability (ACPV) Management solution using the best value trade-off source selection process. This process allows for a trade-off between non-cost/price factors (i.e., technical, pre-qualification questionnaire) and price and allows the NCI Agency to accept other than the lowest priced offer or other than the highest technically rated offer to achieve a best-value contract award. Offerors submitting proposals in response to the NCI Agency Request for Solutions (RFS) CO-115699-ACPV will be evaluated as outlined in this document.

1.1.2 ACPV will be procured through a Dynamic Sourcing which is an agile competitive procedure with negotiations. Dynamic Sourcing is used when a project is not able to define detailed technical requirements upfront, but instead collaborates with industry to determine them. Dynamic Sourcing also provides a faster time-to-solution and a more effective mechanism for collaboration with industry.

1.1.3 Dynamic Sourcing uses competitive collaboration approach based on five (5) steps referred to as “Sprints” and three (3) down selection activities.

1.1.3.1 Preparation Sprint. The Preparation Sprint allows the NCI Agency to identify resources, mobilize, and begin the preparation of the Request for Solutions (RFS) artefacts.

1.1.3.2 Sprint 1. In Sprint 1 the NCI Agency notifies Allied Nations of the NCI Agency’s intent to solicit for a solution, the Offerors list is established and the RFS is released at the end of Sprint 1. The RFS includes a Pre-Qualification Questionnaire, which will be the basis for the initial down selection. Only five (5) firms will be selected for participation in collaborative workshops consisting of five (5) workstreams; (i) Commercial Workstream, (ii) Service Workstream, (iii) Performance Workstream, (iv) Technical Solution Workstream, and (iv) Implementation / Transition Workstream. Successful and unsuccessful Offerors will be notified of the evaluation outcome.

1.1.3.3 Sprint 2. In Sprint 2 high level collaboration workshops are conducted with all five (5) successful Offerors. The workshops will consist of five (5) workstreams identified in paragraph 1.1.3.2 above. The non-cost/price and price evaluations will be conducted at the end of the workshops. The Offerors will be given a week to provide a proposal and a second down selection will be made at the end of Sprint 2. Upon evaluation completion, a recommendation to select two (2) firms for further collaboration will be made in writing to the Contracts Award Committee (CAC) at the end of Sprint 2. Successful and unsuccessful Offerors will be notified of the evaluation outcome.

1.1.3.4 Sprint 3. In Sprint 3, detailed collaboration workshops are conducted with both successful Offerors. The same five (5) workstreams described in paragraph 1.1.3.2. above will be held. The non-cost/price and price evaluations will be conducted during the workshops. Upon completion of the workshops, both firms will be invited to submit their Best and Final Offer (BAFO) and final down selection will be made

at the end of Sprint 3. Concurrently, a recommendation to select a solution provider for award will be made in writing to the Contracts Award Committee (CAC) at the

end of Sprint 3. Successful and unsuccessful Offerors will be notified of the evaluation outcome.

1.1.3.5 Sprint 4. In Sprint 4, the contract will be formed and presented to the selected Offeror for review and signature. Meaningful discussion may be held but negotiations will not be permitted at this stage. The contract will be signed at the end of Sprint 4.

1.1.4 The high level collaboration workshops in Sprint 2 and detailed collaboration workshops in Sprint 3 are hereinafter jointly referred to as the "Collaboration Workshops".

1.1.5 Instead of a complete compendium of technical requirements being issued to Industry upfront via a Statement of Work (SOW), Dynamic Sourcing issues a Statement of Objectives (SOO), found in Book II Part IV herein.

1.1.5.1 The SOO is an outcome-based, solution-focused document which establishes the outcome sought by the procuring organization.

1.1.6 Dynamic Sourcing constitutes a competitive collaboration process with Industry that, through a series of managed, themed workshops (both high-level and detailed). Each workshop allows industry SMEs to propose solutions and engage with NATO directly, in order to demonstrate their professional and technical abilities to fulfil the RFS. The procuring organization is then able to transform the Request for Solution (RFS) into a binding bi-lateral contract

1.1.7 No contractual liability with Offerors will be incurred during the Dynamic Sourcing procurement process. Hence, the process is non-committal on both parties.

1.2 PROJECT SCOPE

1.2.1 The scope of this contract covers the services to be delivered by the contractor in order to support the execution of the ACPV Dynamic Sourcing acquisition process by the NCI Agency.

1.2.2 The NCI Agency aims to contract an ACPV solution for the NATO Enterprise ACPV Service through Dynamic Sourcing, which is a competitive procedure with negotiations.

1.2.3 This procurement is a contributor to the full ACPV ambition. Its primary scope is to provide a service to which cybersecurity functions across the Enterprise will interface, to access and dynamically query the asset, configuration, and patch information of the NATO Enterprise.

1.2.4 This service will provide the required visibility of ACP data to the cybersecurity functions at NATO Enterprise, with a special focus on vulnerability management (ACP for V). It will draw this ACP data from management systems and tools in the local entities, and will allow cybersecurity functions across the Enterprise to interface with, access and dynamically query the asset and configuration data of the NATO Enterprise. This new service will be built on top of existing asset, configuration and patching capabilities across NATO.

1.2.5 This new service will be built on top of existing Asset, Configuration and Patching solutions across NATO, this service can be referred to as the "Enterprise ACPV Service."

1.2.6 The secondary scope of the ACPV Dynamic Sourcing exercise is to create a NATO Enterprise framework that will eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on asset, configuration and patch management information through a federated approach.

1.2.7 The desired project outcomes are described in Book II, Part IV Statement of Objectives (SOO).

1.3 SECURITY

1.3.1 The overall security classification of this solicitation document (RFS) is ~~This RFS has been classified as~~ NATO UNCLASSIFIED when separated from the NATO Restricted Annexes. ~~There is a limited number of references pointing to NATO RESTRICTED documents.~~

1.3.1.1 The NATO Restricted Annexes to this solicitation are:

1.3.1.1.1 AC/322-D/0030-REV6 Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS), 06 July 2023 – Approved draft – Official Publication under AC/322-D(2023)0042 (INV) is to be published in the incoming weeks.

1.3.1.1.2 AC/322-D/0047-REV2 (INV) InfoSec Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009

1.3.1.1.3 AC/322-N(2014)0158-ADD3 SECAN Doctrine and Information Publication (SDIP) 29, Selection and Installation of Equipment for the Processing of Classified Information (SDIP-29/2), March 2015

1.3.1.1.4 AC/322-D/0049-REV1 CIS Security Technical & Implementation Directive for Transmission Security (TRANSEC), 29 November 2018

1.3.1.1.5 AC/322-D(2004)0030 INFOSEC Technical & Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools, 17 May 2004

1.3.1.1.6 AC/322-D(2019)0021 Technical and Implementation Directive on Emission Security, 25 April 2019

1.3.1.1.7 AC/322-D(2012)0011 INFOSEC Technical & Implementation Directive on Downgrading, Declassification and Destruction of System Equipment and Storage Media - Corrigendum 1, 10 Jul 2012

1.3.1.1.8 AC/322-D(2012)0012 INFOSEC Technical & Implementation Guidance on Downgrading, Declassification and Destruction of System Equipment and Storage Media, 07 June 2012

1.3.1.1.9 AC/322-D(2015)0029 CIS Security Technical and Implementation Guidance on Protecting Authentication Credentials, 27 November 2015

1.3.1.1.10 AC/322-D(2005)0044 INFOSEC Technical & Implementation Guidance on Identification and Authentication, 26 October 2005

1.3.1.1.11 AC/322-D/0049-REV1 CIS Security Technical and Implementation Directive for Transmission Security (TRANSEC), 29 November 2018

1.3.1.1.12 AC/322-D(2007)0047 INFOSEC Technical and Implementation Supporting Document on the Use of Shared Peripheral Switches, 12 September 2007

1.3.1.1.13 AC/35-D/1039 Guidelines on Business Continuity Planning for Communications and Information Systems (CIS), 8 October 2008

1.3.1.1.14 AC/322-D(2018)0016 NATO Secure Voice Strategy, 14 March 2018

1.3.1.1.15 AD70-005ACO Communication and Information Systems (CIS) Security, 18 May 2021

1.3.1.1.16 AC/35-D1015-REV4 Guidelines for the Development of Security Requirement Statements (SRSs), 05 July 2023

1.3.1.1.17 SDIP-28/1 NATO Zoning Procedures, December 2009

1.3.1.1.18 SDIP-293/1 Instructions for the Control and Safeguarding of NATO Cryptomaterial, March 2011

1.3.2 ~~Contractor will be required to handle and store classified material to the level of "NATO RESTRICTED".~~

1.3.3 ~~The discussions during the dynamic sourcing sprints may lead to the requirement for the Contractor to have the appropriate facility and personnel clearances of "NATO SECRET" in order to deliver the Enterprise ACPV Service.~~

1.3.4 ~~Contractor personnel working at NATO sites are required to possess a security clearance of "NATO SECRET". Contractor personnel who need System Administrator or Operator privileges when working on NATO SECRET systems shall be required to hold NATO CTS (Cosmic Top Secret) clearances.~~

1.3.5 ~~All documentation, including the RFS itself, all applicable documents and any reference documents provided by the Purchaser are solely to be used for the purpose of preparing a response to this RFS. They are to be safeguarded at the appropriate level according to their classification and reference documents are provided "as is, without any warranty" as to quality or accuracy.~~

1.3.2 Offerors wishing to receive the NATO RESTRICTED documents shall request the documents from the Purchaser's Point of Contact listed in Book I, Section 2.5. The request must include the following information:

1.3.2.1 the name of the authorized Point of Contact

1.3.2.2 the postal address where the NATO RESTRICTED documents may be mailed

1.3.2.3 a signed copy of the Comprehension and Acceptance of the Security Aspect Letter and Program Security Instructions (provided as Annex B-14 and B-15)."

1.3.3 The unsuccessful Offeror having been provided NATO classified information in connection with this RFS shall be required to return the classified information to the Contracting Authority within 15 working days of receipt of notification of their unsuccessful otcome.

SECTION 2. **GENERAL RFS INSTRUCTIONS**

2.1 DEFINITIONS

2.1.1 The following terms and acronyms, as used in this RFS, shall have the meanings specified below:

2.1.1.1 "Compliance": strict conformity to the requirements and standards specified in this RFS and its attachments.

2.1.1.2 "Contractor": the awardee of this RFS, which shall be responsible for the fulfilment of the requirements established in the prospective Contract.

2.1.1.3 "Firm": an organization legally constituted or chartered under the laws of, and geographically located in, or falling under the jurisdiction of a Participating Country.

2.1.1.4 "Offeror": a firm, consortium, or joint venture which submits an offer in response to this solicitation. Offerors 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 "Principal Contractor", shall represent all members of the consortium with the NCI Agency and/or NATO. The "Principal 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 or equivalent issued to the "Principal Contractor" by all members associated with the consortium. Evidence of authority to act on behalf of the consortium by the "Principal Contractor" shall be enclosed and sent with the proposed solution. Failure to furnish proof of authority shall be a reason for the proposed solution being declared non-compliant.

2.1.1.5 "Participating Country": any of the NATO nations contributing to the project, namely, (in alphabetical order):

ALBANIA, BELGIUM, BULGARIA, CANADA, CROATIA, CZECH REPUBLIC, DENMARK, ESTONIA, FINLAND, FRANCE, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, MONTENEGRO, NETHERLANDS, NORTH MACEDONIA, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TÜRKIYE, THE UNITED KINGDOM and THE UNITED STATES.

2.1.1.6 ''Purchaser'': The Purchaser is defined as the current NCI Agency or its legal successor.

2.1.1.7 "RFS": Request for Solution.

2.1.1.8 "Solution" or "Offer": a binding offer to perform the work specified in the attached prospective Contract (Book II).

2.1.1.9 "SOO": Statement of Objectives.

2.2 ELIGIBILITY AND ORIGIN OF EQUIPMENT AND SERVICES

2.2.1 As stated in paragraph 2.1.1.5 above only firms from a Participating Country are eligible to engage in this competitive process. In addition, all Contractors, sub-Contractors and manufacturers, at any tier, must be from Participating Countries.

2.3 OFFER DELIVERY AND RFS CLOSING

2.3.1 This section only applies to Sprint ~~2~~ 3 as Sprint 1 and Sprint 2 ~~is~~ are now complete. ~~The due date for Sprint 3 will be established upon completion of Sprint 2.~~ Note: An Administrative Package is not required for Sprint ~~2~~ 3 therefore, paragraph 2.3.5.1 below does not apply. However, should any of the certificates require updates based on the refinement and tailoring of your solutions, companies are given the opportunity to propose revised Administrative Certificates.

2.3.2 Responses to the RFS shall be in the possession of the Purchaser at the e-mail address given below in paragraph 2.3.3 **SEVEN (7) CALENDAR DAYS OF WHEN THE LAST WORKSHOP WAS HELD.**

a) Company A: 08 August 2023 + 7 calendar days = **15 August 2023**

b) Company B: 09 August 2023 + 7 calendar days = **16 August 2023**

NOTE: OFFERS WILL NO BE OPENNED UNTIL AFTER ALL OFFERS ARE RECEIVED.

2.3.3 Offers shall be delivered in electronic format only to the following email address:

RFS-CO-115699-ACPV@ncia.nato.int

2.3.4 As described in paragraph 1.1.2, this procurement will adhere to the Dynamic Sourcing process which will consist of three (3) down selection activities at the end of Sprints 1, 2, and 3. As such, all interested firms will respond to this RFS and only successful firms participating in high level and detailed collaboration workshops will have the opportunity to supplement its initial offer with a revised technical solution proposal as well as a price proposal.

2.3.5 Full offers consists of three packages; an Administrative package, a Technical package, a Price package. However, only successful Offerors will be required to submit a Price offer at the end of Sprint 2 and 3. All three packages shall be submitted separately:

2.3.5.1 For the first e-mail the subject line shall read: “RFS-CO-115699-ACPV – Official Solution for [company name] – Part I - Administrative Offer”. The e-mail content shall be as described in Paragraph 3.2.2, Part I: Administrative Offer Package below, with no password protection to the file and shall be not larger than 20MB total.

2.3.5.2 For the second e-mail the subject line shall read: “RFS-CO-115699-ACPV – Official Offer for [company name] – Part II – Technical Solution”. The e-mail content shall

be as described in Paragraph 3.2.2, Part II: Technical Solution below, with no password protection to the file, and shall be no larger than 20MB total per e-mail. For large Technical Solutions, multiple e-mails may be required to submit the entire package. In such case, Offerors shall clearly indicate the correct order in the e-mail subject line.

NOTE: Firms shall provide Pre-Qualification Questionnaires as well as Volumes described in Section 3.2.2. below. Only successful firms participating in high level and detailed collaboration workshops will have the opportunity to supplement their proposed technical solution.

2.3.5.3 For the third e-mail the subject line shall read: "RFS-CO-115699-ACPV - Official Offer for [company name] – Part III - Price Offer". The e-mail content shall be as described in Paragraph 3.2.2, Part III: Price Offer below, with no password protection to the file, and shall be not larger than 20MB total.

NOTE: Price will not be evaluated during the initial down selection activity. Therefore, submission of price proposals are not required for purposes of responding to this RFS. Only successful firms participating in high level and detailed collaboration workshops will have the opportunity to submit their proposed price accompanying their proposed technical solutions as described in paragraph 2.3.5.2.

2.3.6 Late Offers

2.3.6.1 It is the responsibility of the Offeror to ensure that the offer submission is duly completed by the specified RFS closing time and date.

2.3.6.2 Offers which are delivered to the Purchaser after the specified time and date set forth above for RFS Closing are "Late Offers". Acceptance of late offers will be at the discretion of the Contracting Officer.

2.4 REQUESTS FOR EXTENSION OF RFS CLOSING DATE

2.4.1 Offerors are informed that due to agility and the collaborative nature of this procurement, requests for extension to the closing date for the RFS are not anticipated at this time. Therefore, the NCI Agency kindly requests all interested Offerors carefully review the RFS package upon its receipt and raise any and all clarification requests during the Offerors Conference as described in paragraph 2.13.

2.5 PURCHASER'S POINT OF CONTACT

2.5.1 The Purchaser Point of Contact (POC) for all information concerning this solicitation is Mr. Edel Esparza, Senior Contracting Officer who may be reached at:

RFS-CO-115699-ACPV@ncia.nato.int

2.6 REQUEST FOR RFS CLARIFICATIONS

2.6.1 The ACPV Enterprise Service is being procured through Dynamic Sourcing which requires increased levels of agility. In order to remain consistent with Dynamic Sourcing, Clarification Requests (CRs) will be handled in accordance with its principles and only Administrative CRs will be allowed. Additionally, CRs shall be raised after careful review of the RFS in its entirety and within two (2) weeks from the release of the RFS.

2.6.2 All questions and requests for clarification shall be forwarded to the Purchaser via email to the Contract Authority at email address listed in paragraph 2.5.1 using the

Clarification Request Form provided at ANNEX D. An editable version of the form will be provided separately and its format shall remain unchanged.

2.6.3 CRs shall be forwarded to the POC specified in paragraph 2.5.1 above and the NCI Agency intends to address all CRs during an Offerors Conference as described in paragraph 2.13. Requests for clarification must address the totality of the concerns of the Offeror.

2.6.4 Additional CRs will be allowed and addressed at the end of the Offerors Conference.

2.6.5 The Purchaser reserves the right to provide answers orally or in writing. Regardless of the delivery method, all answers will be provided simultaneously to all prospective Offerors.

2.6.6 Answers issued by the Purchaser shall be regarded as the authoritative interpretation of the RFS.

2.7 REQUESTS FOR WAIVERS AND DEVIATIONS

2.7.1 Requests for alteration to, waivers, or deviations from the terms and conditions of this RFS and attached Prospective Contract (Book II) will be reviewed and considered. Specifically, Offerors will have an opportunity to address concerns or suggest waivers and deviations to the Purchaser during the High Level and/or Detailed workshops in Sprints 2 and 3. The Purchaser will assess such request and determine feasibility and communicate the outcome to the Offerors.

2.8 AMENDMENT OF THE RFS

2.8.1 The Purchaser may revise, amend or correct the terms, conditions and/or specifications and provisions of the RFS at the earliest stage possible during the solicitation period. Any and all modifications will be communicated to all participating Offerors at any given Dynamic Sourcing Sprint.

2.9 MODIFICATION AND WITHDRAWAL OF OFFERS

2.9.1 Sprint 1 offers, once submitted, may be modified by Offerors, but only to the extent that the modifications are in writing, conform to the requirements of the RFS, and are received by the Purchaser prior to the exact time and date established for RFS Closing Date. Such modifications shall be considered as an integral part of the

submitted Offer.

2.9.2 Modifications to Offers which arrive after the Offer Closing Date will be considered as "Late Modifications" and will be processed in accordance with the procedure set forth in paragraph 2.3.6 above. However, modification to Offers submitted by Offerors participating in High Level or Detailed collaboration workshops (Dynamic Sourcing Sprints 2-4),will be permissible at the end of Sprints 2 and 3.

2.9.3 An Offeror may withdraw its Offer at any time without penalty. In order to do so, an authorised agent or employee of the Offeror must provide an original statement of the firm's decision to withdraw the offer.

2.10 OFFER VALIDITY

2.10.1 Offerors shall be bound by the term of their Offers for a period of twelve (12) months after submission of their offer.

2.11 CANCELLATION OF RFS

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

2.12 ELECTRONIC TRANSMISSION OF INFORMATION AND DATA

2.12.1 The Purchaser will endeavour to communicate answers to clarification requests (CRs) to this RFS to the prospective Offerors during the Offerors Conference.

2.12.2 Offerors are cautioned that unless communication is provided to all potential Offerors through a public forum, the Purchaser will rely exclusively on electronic mail communication to manage all correspondence related to this RFS, including RFS Amendments and clarifications.

2.12.3 Offerors are cautioned that electronic transmission of documentation which contains classified information is not permissible.

2.13 OFFERORS CONFERENCE

2.13.1 A Pre-Award Offerors Conference may be held between two to four weeks after RFS release. The Purchaser anticipates the Offerors Conference to be held on Thursday,19 January 2023. However, a date and time will be confirmed by Friday, 13 January 2023. Registration instructions will be provided at the time of notification.

2.13.2 The purpose of the Conference will be to address previously submitted CRs and allow the Prospective Offerors to clarify aspects of the RFS for which they may have additional questions at that time.

2.13.3 A detailed agenda for the Conference will be sent to the participating companies in due course.

2.13.4 The potential Offerors may submit CRs not later than 7 days prior to the date of the Conference to the POC, at the address mentioned under paragraph 2.5.1. The Purchaser will endeavour to respond to the previously submitted questions at the Conference. If any additional questions are asked by the potential Offerors at the Conference, the Purchaser will attempt to answer them at that time.

2.13.5 Any unanswered questions will be addressed by the Purchaser at a later time, orally or in writing as per instructions provided in paragraph 2.6.5.

2.14 NOTICE TO OFFERORS 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 by Resource Committees”; and (ii) to the customer holding a Service Level Agreement with the Agency related to this requirement, upon request from that customer.

2.15 USE OF NON-NATO PERSONNEL IN EVALUATIONS

2.15.1 The NCI Agency intends to use one or more non-NATO personnel as advisor(s) in evaluating proposed solutions. These advisors will not have voting rights in the actual evaluation assessments. These contractor-advisor(s) are required by the terms of their NATO contract to maintain the confidentiality of any materials to which they are given access. Submission of your proposal to the NCI Agency constitutes implied consent to allow review of your proposal by the contractor-advisor(s).

2.15.2 An offeror shall require the contractor-advisor to execute a supplemental non-disclosure agreement (NDA) by including a copy of the NDA with their proposal. The NDAs are not considered part of the proposal and communications (if any) between the contractor-advisor(s) and the offerors regarding the terms of the NDA are neither discussions nor clarifications.

2.15.3 In the unlikely event the offeror and the contractor-advisor(s) are unable to agree on the terms and conditions to be set forth in the NDA, offerors are advised that the inability of the NCI Agency to obtain the contractor-advisor's expertise in reviewing the offer may adversely impact the NCI Agency's evaluation of the proposal.

2.16 DYNAMIC SOURCING PROTEST AND DISPUTE RESOLUTION PROCEDURE

2.16.1 The NCI Interested Parties may present a protest to the NCI Agency Procurement Authority, of any decision made as a result of Dynamic Sourcing that allegedly violated applicable solicitation provisions and, thus, prejudiced the Offeror.

2.16.2 Regardless of the timeframe of the submission of the protest as indicated in Article 26.4 below, the grounds for protests are limited to:

a) The non-observance of applicable procurement procedures, if it can be demonstrated that this has led to discrimination against one or more Offerors;

b) The non-admission of an Offeror to submit a proposal; if not in compliance with the applicable internal procedures;

c) The wording of the solicitation documents/specifications in such a way as to restrict competition unduly;

2.16.3 Protests shall be submitted in English and in writing. Protests shall be clear and concise. Failure to submit a coherent protest may be grounds for dismissal.

2.16.4 The Offeror must file its protest within 5 calendar days of when the protester knew or should have known of the basis for the protest in writing or by requesting a debriefing.

2.16.5 The NCI Agency Procurement Authority will review the protest or hold a defraying and notify the Offeror of its decision within 5 calendar days of when the protest arrived or 5 calendar days of when the debriefing was held. The decision will be provided verbally or in writing.

2.16.6 Thereafter, if the Offeror is not satisfied with the decision made by the NCI Agency Procurement Authority, a dispute is deemed to exist and it must follow the periods specified below:

a) The Offeror may raise the dispute to their National Delegation within 5 calendar days of when the protest dismissal notification was obtained. Extension requests of up to 5 additional calendar days must be submitted in writing by the National Delegation.

b) Upon review of Oferrors dispute, the National Delegation shall submit a formal notification to the NCI Agency within 5 calendar days.

c) The NCI Agency shall review the notification and make an immediate determination.

d) If an amicable settlement is not possible, the protest/dispute will be sent to an independent board and a decision shall be made within 10 calendar days. Timeline depicted below.

e) Protests/Disputes shall be addressed to the NCI Agency Procurement Authority at: RFS-CO-115699-ACPV@ncia.nato.int

SECTION 3. **OFFER PREPARATION INSTRUCTIONS**

3.1 GENERAL

Offerors shall prepare and submit their Offer in accordance with the requirements and format set forth in this RFS. Compliance with all Offer submission requirements is mandatory. Failure to submit an Offer in conformance with the stated requirements may result in a determination of non-compliance by the Purchaser and the elimination of the Offer from further consideration. Partial bidding is not authorized and will not be considered. Bids, which are not complete, may be declared non-compliant.

Offerors shall prepare their Offer in accordance with Sprint requirement as all Sprint (1, 2, and 3) offer requirements are different.

3.1.1 The specific format for each Offer per Sprint is stated in paragraph 3.2.2.

3.1.2 Offerors shall not simply restate the RFS objectives or requirements. An Offer shall demonstrate that the Offeror understands the terms, conditions and requirements of the RFS and shall demonstrate the Offeror's ability to provide all the services and deliverables listed in Book II Part IV, Statement of Objectives (SOO).

3.1.3 Offerors are informed that the quality, thoroughness and clarity of the Offer will affect the overall scoring of the Offer. Although the Purchaser may request clarification of the Offer, it is not required to do so and may make its assessment on the content of the Offer as written. Therefore, Offerors shall assume that inconsistencies, omissions, errors, lack of detail and other qualitative deficiencies in the submitted Offer will have a negative impact on the final Best Value score.

3.1.4 Offers and all related documentation shall be submitted in the English language.

3.1.5 All documentation submitted as part of the Offer shall be classified no higher than "NATO UNCLASSIFIED".

3.2 PACKAGING AND MARKING OF OFFERS

3.2.1 A complete Offer shall consist of three distinct and separated parts each of which will be send as an individual electronic submission as described in paragraph 3.1.2 as well as in the following subparagraphs.

3.2.2 All e-mails submitted shall be less than 20MB and shall not be password-protected.

Part	Format and Quantity Details
I: SPRINT 1	<u>Administrative Offer Package:</u> <u>1 .zip File Submitted by Email, which includes:</u> • 1 Scanned PDF copies of the certificates with physical (non-digital) signatures of the prescribed certifications ✓ All of the required contents are outlined in Section 3.3.2 <u>Technical Solution:</u>

	1 .zip File Submitted by Email, which includes: • Completed Pre-Qualification Questionnaire found in Book I ANNEX C-1 and ANNEX C-2: 1 Excel file and 1 PDF file • Executive Summary: text doc and 1 PDF file If necessary, the technical volume may be separated into more than one email. Maximum email size per each email is 20MB. The file should address the evaluation criteria in section 4.4.3 and be in accordance with the requirements of section 3.3.3
II: SRINT 2	Technical Report: 1 .zip File Submitted by Email, which includes the Technical Report: • Table of Contents, text doc and 1 PDF file • Volume 1, Executive Summary: text doc and 1 PDF file • Volume 2, Service Objectives Compliance: text doc and 1 PDF file Volume 3, Service Implementation approach: text doc and 1 PDF file • Volume 4, Risk management approach: text doc and 1 PDF file • ANNEX E-1: Cross Reference Table: 1 Excel file and 1 PDF file If necessary, the technical volume may be separated into more than one email. Maximum email size per each email is 20MB. The file should address the evaluation criteria in section 4.5.2 and be in accordance with the requirements of section 3.4.2. 1 .zip File Submitted by Email, which includes: Price Offer: • Sprint 2 Pricing Sheets template provided with the RFS: 1 Excel file and 1 PDF file • **NOTE:** As stated above, only successful firms selected in Sprint 1 to participate in Sprint 2 will submit price proposals accompanying supplemental technical solutions during High Level or Detailed collaboration workshops. ✓ All of the required contents are outlined in Section 3.4.3
III: SPRINT 3	Technical Report.: 1 .zip File Submitted by Email, which includes: • Table of Contents, text doc and 1 PDF file • Volume 1, Executive Summary : text doc and 1 PDF file • Volume 2, Service Objectives Compliance : text doc and 1 PDF file • Volume 3, Service Implementation Plan : text doc and 1 PDF file • Volume 4, Risk Management Plan : text doc.and 1 PDF file

	• Volume 5, Performance Work Statement : text.doc and 1 PDF file • ANNEX E-2: Cross Reference Table: 1 Excel file and 1 PDF file If necessary, the technical volume may be separated into more than one email. Maximum email size per each email is 20MB. The file should address the evaluation criteria in section 4.6.2 and be in accordance with the requirements of section 3.5.2 <u>Price Offer:</u> • Sprint 3 Pricing Sheets template (detailed), which will be provided to the successful Offeror(s) passing Sprint 2 and competing in Sprint 3: 1 Excel file and 1 PDF file o Derived Schedule of Supplies and Services (SSS): 1 Excel file and 1 PDF file • **NOTE:** As stated above, only successful firms selected in Sprint 2 to participate in Sprint 3 will submit price proposals accompanying supplemental technical solutions during High Level or Detailed collaboration workshops. ✓ All of the required contents are outlined in section 3.5.3

3.2.3 The proposal shall be sent via separate e-mails to the Offer Delivery e-mail address as specified in Paragraph 2.3 and in accordance with Paragraph 3.2.1 and 3.2.2 above.

3.3 SPRINT 1

3.3.1 This procurement will have three (3) separate down selection activities conducted at the end of Sprints 1, 2 and 3. Sprint 1 will be based on the assessment of all Administrative certificates as well as the evaluation of Pre-Qualification Questionnaires submitted in response of this Request for Solution (RFS). At the end of Sprint 1, and as a result of its pre-qualification based evaluation, only five (5) Offerors will be selected and invited to participate in Sprint 2 high level collaboration workshops. The remaining Offerors will be notified of the results in due time. Offerors shall refer to section 3.2 for packaging and marking requirements. Additionally, Offerors shall refer to Section 3.3.2 and 3.3.3 for details on Administrative and Technical solution package requirements.

3.3.2 Administrative Offer Package

3.3.2.1 Prior to evaluating Pre-Qualification Questionnaires or technical aspects of firms' proposed solutions, the NCI Agency will evaluate Administrative Compliance. Offers will be reviewed for compliance with the formal requirements for Offer submission as stated in this RFS and the content of the Administrative Offer Package. The evaluation of the Administrative Offer Package will be made on its completeness, conformity and compliance to the requested information. The Package shall include the Certificates set forth in ANNEX B to these RFS Instructions, signed in the original by an authorised representative of the Offeror. The text of the certificates must not be altered in any way. Within the Package the Offeror shall also include the signed electronic copies of the certifications – with physical, not electronic signatures - set forth in Annex B hereto, specifically:

a) ANNEX B-1: Certificate of Legal Name of Firm

b) ANNEX B-2: Certificate of Exclusion of Taxes, Duties and Charges

c) ANNEX B-3: Comprehension and Acceptance of Terms and Conditions

d) ANNEX B-4: Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements

e) ANNEX B-5: Certificate of Compliance AQAP 2110 or ISO 9001:2015 or Equivalent

f) ANNEX B-6: List of Prospective Subcontractors/Consortium Members

g) ANNEX B-7: Offeror Background IPR

h) ANNEX B-8: List of Subcontractors IPR

i) ANNEX B-9: Certificate of Origin of Equipment, Services, and Intellectual Property

j) ANNEX B-10: List of Proposed Key Personnel and Security Clearance

k) ANNEX B-11: Disclosure of Involvement of Former NCI Agency Employment

l) ANNEX B-12: Comprehension And Intention To Comply With Exclusion Clause And Conflict Of Interest

m) ANNEX B-13: Certificate of Compliance ISO 27001:2022

n) ANNEX B-14: Security Aspects Letter (SAL)

o) ANNEX B-15: Project Security Instructions (PSIs) – Structure and Content

p) ANNEX B-16: Self-Attestation Certificate-Compliance With Safeguarding NATO Information Controls

3.3.2.2 Concerning ANNEX B-4, Offerors shall disclose any prospective Supplemental Agreements that are required by national governments to be executed by NATO/NCI Agency or successor organisations as a condition of Contract performance. Supplemental Agreements are typically associated with, but not necessarily limited to, national export control regulations, technology transfer restrictions and end user agreements or undertakings. If supplemental agreements, such as End-User Certificates or Technical Assistance Agreements, are required by national regulations, these must be submitted with the firm's offer. The terms of supplemental agreements, if necessary, are the Offerors/ Contractors responsibility and shall be totally consistent with the terms of the RFS, and shall not duplicate, negate, or further interpret any provisions of this RFS. The terms of the RFS shall take precedence over the Supplemental Agreement.

3.3.2.3 Concerning ANNEX B-5, Offerors are requested to note that, in accordance with the Certificate at ANNEX B-6 hereto, Offerors shall provide documentary evidence that the Offeror possesses a current certification that is compliant with the requirements of Allied Quality Assurance Publication (AQAP) 2110, ISO 9001:2015, or an equivalent QA/QC regime. Offerors shall further demonstrate that such regime is applied within the Offeror's internal organisation, as well as extended to its relationships with Subcontractors. If the Offeror is offering a QA/QC regime that is claimed to be equivalent to AQAP 2110 or ISO 9001:2015, the burden of proof of such equivalency shall be on the Offeror and such evidence of equivalency shall be submitted with ANNEX B-6 in the Administrative Offer Package.

3.3.2.4 Concerning ANNEX B-6, the Offeror shall identify by name, project role, and country of origin, all sub-contractors whose sub-contract value is expected to equal or exceed EUR 125,000, if any. A list of consortium members shall also be completed and included. If there are no sub- contractors/consortium members involved, the Offeror shall state this separately. The subcontractors listed in this certificate shall be traceable in the Pricing Sheets.

3.3.2.5 Concerning ANNEX B-7 and ANNEX B-8, Offerors are instructed to review Clauses 10 and 11 of the Terms and Conditions set forth in Book II Part II herein. These Clauses sets forth the definitions, terms and conditions regarding the rights of the Parties concerning Intellectual Property developed and/or delivered under this Contract or used as a basis of development under this Contract. Offerors are required to disclose, in accordance with ANNEX B-8 and ANNEX B-9, the Intellectual Property proposed to be used by the Offeror that will be delivered with either Background Intellectual Property Rights or Third Party Intellectual Property Rights. Offerors are required to identify such Intellectual Property and the basis on which the claim of Background or Third Party Intellectual Property is made. Offerors are further required to identify any restrictions on Purchaser use of the Intellectual Property that is not in accordance with the definitions and rights set forth in the Contract concerning use or dissemination of such Intellectual Property.

3.3.2.6 ANNEX B-13: Offerors shall provide documentary evidence that the Offeror possesses and maintains a current certification that is compliant with the requirements of ISO 27001:2022, or an equivalent industry or national certification for Security Management Systems Requirements.

If the Offeror is presenting an Information Security Management Requirements

Certificate, or similar industry or national certificate, that is claimed to be equivalent to ISO/IEC 27001- Security Management Systems Requirements, the burden of proof of such equivalency shall be on the Offeror and such evidence of equivalency shall be submitted with the ANNEX B-13 in the Administrative Package.

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

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

If the Offeror provides a certification that is scheduled to expire, during the solicitation phase or during the contract performance period, the Offeror will be required to provide evidence that a renewal process has begun and that a renewed certification will be obtained. In such circumstance, the Offeror shall provide a written statement of their intention to renew such certificate in their Administrative Package.

3.3.2.7 Documentation Disclosure of Conflict of Interest

3.3.2.7.1 Offerors are instructed to review Clause 38 of the Terms and Conditions set forth in Book II Part II herein. In compliance with paragraph 4.4.2.6, Offerors and proposed subcontractors detailed at ANNEX B-6 shall identify all business relationships or personal relationships of staff with the Cyber Evaluation and Adaptation contractor, Dynamic Sourcing Process Augmentation Support Contractor, or Programmatic and Technical Augmentation Support Contractor including but not limited to those resulting from current or previous (over the last five (5) years) ownership, personal relationships of staff, share of assets, strategic business agreements regardless of their nature or financial magnitude of which the Offerors or subcontractors are knowledgeable at the time of offer submission. If any of such relationships could constitute a real or apparent conflict of interest, or could otherwise, in any manner or form, influence or appear to influence the capacity of the Offeror to render unbiased service, Offerors shall, as part of the Offer, submit a statement that clearly defines the nature of the apparent or real conflict of interests including a complete description of the relationship, and the individuals subject to the real or apparent conflict, and a plan for the mitigation of the conflict detailing the measures the Offeror has or proposes to put in place for the purpose of preventing unfair advantage in relation to the performance associated with the prospective contract.

3.3.3 Technical Solution Package

3.3.3.1 Only those Offerors in full compliance with Administrative Offer package requirements will be subject to an evaluation of their Technical Solution through their Pre-Qualification Questionnaires.

3.3.3.2 The Offeror shall submit their Technical Solution as one (1) email. This email shall contain one (1) zip file which addresses each criterion as described in section 4.4.3 and in accordance with the requirements of sections 3.2, and 3.3.3.

NOTE 1: The Pre-Qualification Questionnaire will consist in two sections, each of them with distinctive approach. The first part of the Pre-Qualification Questionnaire, found in ANNEX C-1, includes open ended questions while the second part of the questionnaire, found in ANNEX C-2, includes a self-declared compliance criteria of 'YES', 'PARTIALLY', and 'NO'.

3.3.3.3 The Technical Proposal package shall include the following:

3.3.3.4 Completed Pre-Qualification Questionnaire found in ANNEX C-1 and ANNEX C-2.

3.3.3.5 Offerors shall provide answers to each of the pre-qualification questionnaire requirements, providing sufficient evidence of Offerors' capabilities to deliver a solution for the Enterprise ACPV Service.

3.3.3.6 Pass/Fail Criteria.

3.3.3.6.1 Offerors will provide a brief narrative addressing each of the questions using the below criteria. Each question will have a weighting factor based on relevancy to ACPV and responses shall be provided in accordance with below response criteria.

3.3.3.6.2 For requirements with weighting factor “High” the answer will not exceed 500 words.

3.3.3.6.3 For requirements with weighting factor “Medium” the answer will not exceed 300 words.

3.3.3.6.4 For requirements with weighting factor “Low” the answer will not exceed 200 words

3.3.3.7 Yes/No/Partially Criteria.

3.3.3.7.1 Offerors shall respond if their proposal can deliver each of the individual service objectives by answering Yes/No/Partially to each of the objectives in the table in accordance with response criterial shown below.

3.3.3.7.2 Yes - The Offeror shall reply ‘YES’ if their proposal is able to deliver the individual service objective.

3.3.3.7.3 Partially - The Offeror shall reply ‘PARTIALLY’ if their proposal is able to deliver the individual service objective only partially.

3.3.3.7.4 No - The Offeror shall reply ‘NO’ if their proposal is not able to deliver the individual service objective.

3.3.3.8 Executive Summary of Offeror's proposal

3.3.3.8.1 Offerors shall provide an overview of the salient features of their technical proposal in the form of an Executive Summary.

3.3.3.8.2 The Executive Summary shall provide a general description of how the offer will deliver the goal and expected outcome of the Enterprise ACPV Service as described in section 5 of Book II Part IV Statement of Objectives and its ANNEX A - Performance Work Statement (PWS) Template. It shall demonstrate the depth of the Offeror's understanding of: (i) the service objectives, the service implementation environment, (ii) the problems and risks of the service implementation and delivery foreseen by the Offeror, (iii) as well as the Offeror's ability to communicate high level concepts in an appropriate and succinct manner. The Offeror shall highlight the strengths which it and its team bring to the project in terms of minimising the problems and reducing the risks, while meeting the overall schedule, and the key points of the technical approach.

NOTE 1: A Performance Work Statement (PWS) template is provided as ANNEX A to Book II Part IV Statement of Objectives (SOO). The purpose of the PWS is to provide Offerors with a consistent structure in which their proposed requirements package must be submitted. PWS content is subject to adaptation and refinement as a result of the collaborative discussions taking place during dynamic sourcing

Sprints 2 and 3.

NOTE 2: The Statement of Objectives (SOO) is referenced as Book II Part IV and the Performance Work Statement (PWS) is referenced as an attachment to the SOO throughout this document. However, Offerors shall note that during contract formation (Sprint 4), the PWS will become Book II Part IV, replacing the SOO in its entirety and capturing all contractual service requirements.

3.3.3.8.3 The Executive Summary shall include three sections; Service Objectives Compliance, Service Implementation, and Risk. All three (3) section are described below.

3.3.3.8.4 Service Objectives Compliance.

3.3.3.8.4.1 This section shall summarize, in accordance with Book II Part IV- Statement of Objectives:

3.3.3.8.4.2 How the offer will deliver the goal and expected outcome of the Enterprise ACPV Service as described in sections 5 of Book II Part IV Statement of Objectives.

3.3.3.8.4.3 The technical solution proposed to deliver the service objectives.

3.3.3.8.4.4 The service delivery and service management approach.

3.3.3.8.4.5 If the proposed solution will support all the asset types described in the Statement of Objectives and how it will do it.

3.3.3.8.4.6 If the proposed solution will support integration with all the Tier 2 systems described in the reference scenario of the Statement of Objectives and how it will do it.

3.3.3.8.4.7 The Service Objectives Compliance section of the Executive summary shall not exceed seven (7) A4 sized pages and use Arial font, size 12.

3.3.3.8.5 Service Implementation.

3.3.3.8.5.1 This section shall summarize, in accordance with Book II Part IV Statement of Objectives, at least:

3.3.3.8.5.2 How the Offeror intends to organize and manage the service implementation project from contract signature through to Final Service Acceptance

3.3.3.8.5.3 An overview of the Implementation Project Master Schedule (PMS). The PMS shall clearly identify the date of the operational launch of the service.

3.3.3.8.5.4 The testing, verification and validation approach.

3.3.3.8.5.5 The Service Implementation section of the Executive summary shall not exceed four (4) A4 sized pages and use Arial font, size 12.

3.3.3.8.6 Risk.

3.3.3.8.6.1 This section shall summarize:

3.3.3.8.6.2 The key risks identified in the service implementation and service delivery and their proposed responses.

3.3.3.8.6.3 The corporate experience of the Offeror in providing similar services (as a prime or subcontractor) in a similar environment in the last five (5) years

3.3.3.8.6.4 If applicable, the subcontracting approach and how subcontractors will contribute and add value to the service implementation or delivery.

3.3.3.8.6.5 Which parts of the proposed service solution are based on already existing solutions and which parts will require new ad-hoc developments.

3.3.3.8.6.6 The Risk section of the Executive summary shall not exceed four (4) A4 sized pages using size and use Arial font, size 12.

3.4 SPRINT 2

3.4.1 This procurement will have three (3) separate down selection activities conducted at the end of Sprints 1, 2 and 3. Sprint 2 will be based on the evaluation of Offerors Technical Solution package and its corresponding Price Offer package. Both Technical and Price packages will be based on information discussed during Sprint 2 high-level collaboration workshops held with all five (5) Offerors selected in the prior Sprint 1. At the end of Sprint 2, and as a result of its best value evaluation, two (2) out of five (5) Offerors will be selected and invited to participate in Sprint 3 detailed collaboration workshops. The remaining three (3) Offerors will be notified of the results in due time. Offerors will refer to section 3.2 for packaging and marking requirements. Additionally, Offerors will refer to Section 3.4.2 and 3.4.3 for details on Technical Solution and Price Offer package requirements.

3.4.2 Technical Solution Package

3.4.2.1 After the high level collaboration workshops in Sprint 2, the Offeror shall submit their Technical Proposal (hereinafter referred to as the Technical Report) as one (1) email containing the Technical Report. This email shall contain one (1) zip file which addresses each criterion as described in section 4.5.2 and in accordance with the requirements of section 3.2 and 3.4.2.5.

3.4.2.2 Offerors shall respond to the service objectives and technical requirements of the Book II Part IV Statement of Objectives with not only an affirmation of compliance but also with an explanation of how the objective and requirement will be met.

3.4.2.3 To facilitate submission and the subsequent evaluation of the Offeror's response to the various sections of the Statement of Objectives, the Technical Report shall be organised and submitted in four (4) volumes as follows.

- Volume 1 – Executive Summary.
- Volume 2 – Service Objectives Compliance.
- Volume 3 – Service Implementation.
- Volume 4 – Risk.

3.4.2.4 RFS instructions related to each of the four (4) volumes are provided in Sections 3.4.2.8 through 3.4.2.11.

3.4.2.5 Technical Report Contents (also refer to section 3.2)

3.4.2.6 Cross-Reference Table. The Offeror shall include the completed Cross-Reference Table at ANNEX E-1 accompanying their offers in Sprint 2 and capturing all 4 Volumes included therein. The Offeror shall complete the Column marked "OFFER REFERENCE" of the Table, citing the appropriate section of the Technical Report that corresponds to each paragraph of these Instructions for the Preparation of the Technical Solution. The completed table serves as an index for the Purchaser's Technical Evaluation Panel and also as an aide memoire to the Offeror to ensure that all the required information has been provided in the Technical Report.

3.4.2.7 Table of Contents for the whole Technical Report. Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic

headings required in these Instructions or implicit in the organisation of the Technical Report.

3.4.2.8 Volume 1 – Executive Summary

3.4.2.8.1 Executive Summary

3.4.2.8.1.1 Offerors shall provide an overview of the salient features of their Technical Report in the form of an Executive Summary.

3.4.2.8.1.1.1 The Executive Summary in Volume 1 shall not exceed fifteen (15) A4 sized pages and use Arial font, size 12.

3.4.2.8.1.2 The Executive Summary shall provide a general description of how the offer will deliver the objectives in Book II Part IV Statement of Objectives. It shall demonstrate the depth of the Offeror's understanding of: the service objectives, the service implementation environment, the problems and risks of the service implementation and delivery foreseen by the Offeror, as well as the Offeror's ability to communicate high level concepts in an appropriate and succinct manner. The Offeror shall highlight the strengths which it and its team bring to the project in terms of minimising the problems and reducing the risks, while meeting the overall schedule, and the key points of the technical approach.

3.4.2.8.1.3 The Executive Summary shall include the following three (3) sections:

3.4.2.8.1.3.1 Service Objectives Compliance.

3.4.2.8.1.3.1.1 This section shall summarize, in accordance with Book II Part IV Statement of Objectives:

a) How the offer will deliver the goal and expected outcome of the Enterprise ACPV Service as described in Book II Part IV Statement of Objectives, Section 5.

b) The proposed technical solution design and integration approach

c) The service delivery and service management approach.

d) If the proposed solution will support all the asset types described in the Statement of Objectives and how it will do it.

e) If the proposed solution will support integration with all the Tier 2 systems described in the reference scenario of the Statement of Objectives and how it will do it.

3.4.2.8.1.3.1.2 The Service Objectives Compliance section of the Executive summary shall not exceed seven (7) A4 sized pages and use Arial font, size 12.

3.4.2.8.1.3.2 Service Implementation.

3.4.2.8.1.3.2.1 This section shall summarize, in accordance with Book II Part IV Statement of Objectives, at least:

a) How the Offeror intends to organize and manage the service implementation project from contract signature through to Final Service Acceptance

b) An overview of the Implementation Project Master Schedule (PMS). The PMS shall clearly identify the date of the operational launch of the service.

c) The testing, verification and validation approach.

3.4.2.8.1.3.2.2 The Service Implementation section of the Executive summary shall not exceed four (4) A4 sized pages and use Arial font, size 12.

3.4.2.8.1.3.3 Risk.

3.4.2.8.1.3.3.1 This section shall summarize, in accordance with Book II-Part IV- Statement of Objectives:

a) The key risks identified in the service implementation and service delivery and their proposed responses.

b) The corporate experience of the Offeror in providing similar services (as a prime or subcontractor) in a similar environment in the last five (5) years

c) The key personnel and their relevant skills for the implementation and delivery of the service.

d) If applicable, the subcontracting approach and how subcontractors will contribute and add value to the service implementation or delivery.

e) Which parts of the proposed service solution are based on already existing solutions and which parts will require new ad-hoc developments.

3.4.2.8.1.3.3.2 The Risk management section of the Executive summary shall not exceed four (4) A4 sized pages and use Arial font, size 12.

3.4.2.9 Volume 2 – Service Objectives Compliance

3.4.2.9.1 This volume covers the service delivery component of the Technical Report and will be used to assess the Offeror's ability to deliver a service that meets the goal and expected outcome of the service.

3.4.2.9.1.1 The Volume 2-Service Objectives Compliance shall not exceed twenty-five (25) A4 sized pages and use Arial font, size 12.

3.4.2.9.2 The volume shall include the following elements:

(a) Table of Contents for Volume 2.

(b) Technical Solution Design and Integration approach

(c) Service delivery approach

(d) Draft Performance Requirements Summary and PWS compliance statement

(e) Service Objectives Compliance Table in ANNEX F

3.4.2.9.3 Table of Contents for Volume 2. Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report.

3.4.2.9.4 Technical Solution Design and Integration approach: Offerors shall explain their proposed technical solution, including an overview of their technical solution design and system integration requirements in order to meet in the objectives in Book II-Part IV- Statement of Objectives.

3.4.2.9.5 Service delivery approach: Offerors shall explain their service delivery and service management approach in order to meet the objectives in Book II Part IV Statement of Objectives.

3.4.2.9.6 Draft Performance Requirements Summary and PWS compliance statement:

Offerors shall propose a draft Performance Requirements Summary in accordance with the PWS template found in Book II Part IV Statement of Objectives-ANNEX A

3.4.2.9.6.1 Offerors shall explicitly state in this section that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and service(s) shall be specified in accordance with the PWS template found in Book II Part IV Statement of Objectives-ANNEX A and shall comply (if applicable to the service in question) with the requirements in the PWS (including all annexes/exhibits).

3.4.2.9.7 Completed Service Objectives Compliance Table found in Book I ANNEX F.

3.4.2.9.7.1 Offerors shall respond if their proposal can deliver each of the individual service objectives by answering Yes/No/Partially to each of the objectives in the table.

3.4.2.9.7.2 Yes/No/Partially Criteria

3.4.2.9.7.2.1 Yes - The Offeror shall reply 'YES' if their proposal is able to deliver the individual service objective.

3.4.2.9.7.2.2 Partially - The Offeror shall reply 'PARTIALLY' if their proposal is able to deliver the individual service objective only partially.

3.4.2.9.7.2.3 No - The Offeror shall reply 'NO' if their proposal is not able to deliver the individual service objective.

3.4.2.10 Volume 3 - Service Implementation

3.4.2.10.1 This volume covers the service implementation component of the Technical Report and will be used to assess the Offeror's ability to implement the service according to the proposed project milestones.

3.4.2.10.1.1 The Volume 3-Service Implementation shall not exceed ten (10) A4 sized pages and use Arial font, size 12.

3.4.2.10.2 The volume shall include the following elements:

(a) Table of Contents for Volume 3

(b) Service implementation approach

(c) Project Master Schedule (PMS)

(d) Testing, verification and validation approach

3.4.2.10.3 Table of Contents for Volume 3. Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report.

3.4.2.10.4 Service Implementation approach; The Offeror shall indicate in broad detail the service implementation approach and how the implementation project will be executed and managed from contract signature through to Final Service Acceptance in order to meet the objectives in Book II Part IV Statement of Objectives.

3.4.2.10.5 Project Master Schedule (PMS): Offerors shall provide a draft PMS with the key contract events and milestones for the service implementation project. The PMS shall provide milestone and Gantt views and identify the critical path for the overall project. The draft PMS shall clearly identify the operational launch of the service

(OLS) milestone, where OLS is the period, measured in days, between the Effective Date of the Contract (EDC) and the date of the operational launch of the service, according to the following formula:

OLS = Date of Operational Launch of the Service – EDC

3.4.2.10.6 Testing, verification and validation: Offerors shall describe their proposed testing, verification and validation approach in order to meet the objectives in Book II Part IV Statement of Objectives. They shall also propose a use case to validate their solution during Sprint 3 should they be shortlisted.

3.4.2.11 Volume 4 - Risk

3.4.2.11.1 This volume covers the service implementation component of the Technical Report and will be used to assess the Offeror's ability to implement the service according to the proposed project milestones.

3.4.2.11.1.1 The Volume 4-Risk shall not exceed ten (10) A4 sized pages and use Arial font, size 12.

3.4.2.11.2 The volume shall include the following elements:

(a) Table of Contents for Volume 4

(b) Risk Management approach

(c) Corporate experience and individual skills

(d) Availability of the proposed service solution

3.4.2.11.3 Table of Contents for Volume 4. Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report.

3.4.2.11.4 Risk management: Offerors shall identify the key risks in their project and their proposed response actions.

3.4.2.11.5 Corporate experience and individual skills: Offerors shall provide a description of the corporate capabilities of the Offeror, including corporate experience, and individual skills and experience, both in service implementation and service delivery. The Offeror shall identify its major proposed sub-contractors and describe their contribution and added value to the implementation and delivery of the service The Offeror shall provide at least one (1) executive summary of the successful delivery of a similar service in a similar environment during the last five (5) years.

3.4.2.11.6 Availability of the proposed service solution: Offerors shall describe which parts of the proposed service solution are based on already existing and working services and which parts will require new ad-hoc integrations or developments.

3.4.3 Price Offer Package

3.4.3.1 Interested firms will be required to submit price offer packages twice throughout the Dynamic Sourcing solicitation process; once at the end of Sprint 2 (which will be evaluated during sprint 2) and a second time at the end of Sprint 3 (which will be evaluated during sprint 3).

NOTE 1: Only successful firms participating in the high level and detailed

collaboration workshops (Sprints 2 and 3) will be required to submit a price proposal.

NOTE 2: Pricing sheets evaluated in Sprint 2 will only consist of an Offer and a CLIN Summary (high level), while Sprint 3 pricing sheets require details per CLIN about: labour, material, Other Direct Costs (ODC) and travel, if applicable. Sprint 3 pricing sheets therefore shall have more granularity.

3.4.3.2 Price Offer Package Contents (also refer to section 3.2)

3.4.3.2.1 Firms will submit one ZIP file by email, containing the completed Sprint 2 Pricing Sheets (Excel) provided in ANNEX A-1 to these RFS Instructions and 1 PDF of the Pricing Sheets "Offer Summary" tab. All documentation stated in Section 3.2 shall be submitted.

3.4.3.3 General Rules

3.4.3.3.1 Offerors shall prepare their Price Offer by completing the Pricing Sheets referred in Section 3.4.3.2.1 above, in accordance with the instructions specified in ANNEX A-2.

3.4.3.3.2 The structure of the Pricing Sheets shall not be changed, other than as indicated elsewhere, nor should any quantity or item description in the Pricing Sheets. The currency(ies) of each Contract Line Item and sub-item shall be shown. Offerors may use one pricing sheet per currency if quoting in multiple currencies. The prices provided shall be intended as the comprehensive total price offered for the fulfilment of all requirements as expressed in the RFS documentation and as discussed during the collaboration workshops.

3.4.3.3.3 When completing the Pricing Sheets the Offeror shall insert information in all yellow cells of the Pricing Sheets and complete the Offer Summary as instructed. A price for each specified element needs to be supplied on each CLIN. Prices should not be grouped. The prices entered on the document shall reflect the total items required to meet the contractual requirements. The total price shall be indicated in the appropriate columns and in the currency quoted. If the price of a line item is expressed in different currencies, these shall be identified, and there shall be as many totals on that line item as there are currencies; unless Offerors choose to use one pricing sheet per currency. Sprint 2 pricing sheets are high level and no quantity is required, only a price per CLIN item. However, in Sprint 3, price and quantity against each CLIN and sub-CLINs will be required.

3.4.3.3.4 Offerors shall furnish Firm Fixed Prices for all required items in accordance with the format set forth in the Instructions for preparation of the Pricing Sheets.

3.4.3.3.5 Offerors shall furnish Firm Fixed Prices for all CLINs as defined in the Schedule of Supplies and Services (SSS). Purchaser evaluation of the submitted Offers will be on the basis of the complete submission including administrative, price and technical components for all CLINs. The Contract will be awarded for all CLINs, with CLINs 1 through 10 being the basic contract and the services defined for CLINs 11 and 12 being Firm Fixed Evaluated Price options to the Contract. These options may be exercised by the Purchaser, at the sole discretion of the Purchaser. The Purchaser's decision to exercise any Options will take into consideration the Contractor's successful performance on the basic contract, as well as the availability of the required funding.

3.4.3.3.6 Offered prices shall not be "conditional" in nature. Any comments supplied in the

Pricing Sheets or in any part of the Offer package which are conditional in nature, relative to the offered prices may result in a determination that the Offer is non-compliant.

3.4.3.4 Offerors are responsible for the accuracy of their Price Offers. Price Offers that have apparent computational errors may have such errors resolved in the Purchaser's favour or, in the case of gross omissions, inconsistencies or errors, may be determined to be non-compliant. In the case of inconsistencies between the electronic version of the Pricing Sheets and the PDF of the Pricing Sheets, the "hard copy, PDF version" will be considered by the Purchaser to have precedence over the electronic version.

3.4.3.4.1 Offerors shall quote in their own national currency or in EURO. Offerors may also submit Offers in multiple currencies including other NATO member states' currencies under the following conditions:

3.4.3.4.1.1 the currency is of a "participating country" in the project, and

3.4.3.4.1.2 the Offeror can demonstrate, either through sub-contract arrangements or in its proposed work methodology, that it will have equivalent expenses in that currency. All major subcontracts and their approximate anticipated value should be listed on a separate sheet and included with the Price Offer.

3.4.3.4.2 The Purchaser, by virtue of its status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct and indirect taxes (incl. VAT) and all customs duties on merchandise imported or exported.

3.4.3.4.3 Offerors shall therefore exclude from their Price Offer all taxes, duties and customs charges from which the Purchaser is exempted by international agreement and are required to certify that they have done so through execution of the Certificate at ANNEX B-2.

3.4.3.4.4 The Offerors' attention is directed to the fact that Price Offer shall contain no document and/or information other than the priced copies of the Pricing Sheets. However, the NCI Agency reserves the right to use any information obtained through collaboration workshops during the evaluation.

3.4.3.4.5 All prices offered shall be clearly traceable in the detailed pricing sheets.

3.4.3.4.6 Any adjustment or discount to prices should be clearly traceable to the lowest level of breakdown in the pricing sheets and should not be aggregated or summed. Any lack of clarity or traceability may render the offer non-compliant.

3.4.3.4.7 The Offeror understands that there is no obligation under this contract for the Purchaser to exercise any of the optional line items and that the Purchaser bears no liability should it decide not to exercise the options (totally or partially). Further, the Purchaser reserves the right to order another Contractor (or the same), to perform the tasks described in the optional line items of the current contract through a new contract with other conditions.

3.5 SPRINT 3

3.5.1 This procurement will have three (3) separate down selection activities conducted at the end of Sprints 1, 2 and 3. Sprint 2 will be based on the evaluation of Offerors Technical Solution package and its corresponding Price Offer package. Both Technical and Price packages will be based on information discussed during Sprint 2 high-level collaboration workshops held with all five (5) Offerors selected in the prior Sprint 1. At the end of Sprint 2, and as a result of its best value evaluation, two (2) out of five (5) Offerors will be selected and invited to participate in Sprint 3 detailed collaboration workshops. The remaining three (3) Offerors will be notified of the results in due time. Offerors will refer to section 3.2 for packaging and marking requirements. Additionally, Offerors will refer to Section 3.5.2 and 3.5.3 for details on Technical Solution and Price Offer package requirements.

3.5.2 Technical Solution Package

3.5.2.1 After the detailed collaboration workshops in Sprint 3 the Offeror shall submit their Technical Proposal (hereinafter referred to as the Technical Package) as one (1) email. This email shall contain one (1) zip file which addresses each criterion as described in section 4.6.2 and in accordance with the requirements of section 3.2 and 3.5.2.6.

3.5.2.2 It is of the utmost importance that Offerors respond to all of the service objectives and technical requirements of the Purchaser Statement of Objectives, not only with an affirmation of compliance but also with an explanation of how each objective and requirement will be met.

3.5.2.3 To facilitate Offerors' submission and the subsequent evaluation of the Offeror's response to the various sections of the Statement of Objectives, offers shall be organised and submitted in five (5) volumes as follows:

- Volume 1 – Executive Summary.
- Volume 2 – Service Objectives Compliance.
- Volume 3 – Service Implementation.
- Volume 4 – Risk.
- Volume 5 – Performance Work Statement

3.5.2.3.1 The proposed Technical Solution shall not be "conditional" in nature. Any comments supplied in the Technical Package which are conditional in nature, relative to the proposed Technical Solution, may result in a determination that the offer is non-compliant.

3.5.2.4 Offeror's responses shall be clearly readable and use Arial font size 12.

3.5.2.5 RFS instructions related to each of the five (5) volumes are provided in Sections 3.5.2.9 through 3.5.2.13

3.5.2.6 Technical Package Contents (also refer to section 3.2)

3.5.2.7 Cross-Reference Table. The Offeror shall include the completed Technical Package Cross-Reference Table at ANNEX E-2 accompanying their offers and capturing all Volumes included therein. The Offeror shall complete the Column marked "OFFER

REFERENCE" of the Table, citing the appropriate section of the Technical Package that corresponds to each paragraph of these Instructions for the Preparation of the Technical Solution. The completed table serves as an index for the Purchaser's Technical Evaluation Panel and also as an aide memoire to the Offeror to ensure that all the required information has been provided in the Technical Package.

3.5.2.8 Table of Contents for the whole Technical Package. Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Package.

3.5.2.9 Volume 1 – Executive Summary

3.5.2.9.1 The volume shall include the following elements

(a) Executive Summary

(b) Applicable documents

3.5.2.9.2 Executive Summary

3.5.2.9.2.1 The Executive Summary shall provide a general description of how the offer will deliver the objectives in Book II Part IV Statement of Objectives. It shall demonstrate the depth of the Offeror's understanding of: the service objectives, the service implementation environment, the problems and risks of the service implementation and delivery foreseen by the Offeror, as well as the Offeror's ability to communicate high level concepts in an appropriate and succinct manner. The Offeror shall highlight the strengths which it and its team bring to the project in terms of minimising the problems and reducing the risks, while meeting the overall schedule, and the key points of the technical approach.

3.5.2.9.2.2 The Executive Summary shall not exceed fifteen (15) A4 sized pages and Arial font size 12.

3.5.2.9.1 Applicable documents: listing all documents or standards referenced by the other sections of the Technical Package.

3.5.2.10 Volume 2 – Service Objectives Compliance

3.5.2.10.1 This volume covers the service delivery component of the Technical Package and will be used to assess the Offeror's ability to deliver a service that meets the goal, expected outcome and service objectives of the service.

3.5.2.10.2 The volume shall include the following elements:

(a) Table of Contents for Volume 2.

(b) Technical Solution Design and Integration Plan

(c) Service Delivery Plan

(d) Completed Service Objectives Compliance Table found in ANNEX F.

3.5.2.10.3 Table of Contents for Volume 2. Offeror shall compile a detailed Table of Contents which lists not only section headings but also major sub-sections, and topic headings required set forth in these Instructions or implicit in the organisation of the Technical Package.

3.5.2.10.4 Technical Solution Design and Integration: The Offeror shall describe how the

Enterprise ACPV service will be implemented with sufficient technical detail for the Purchaser to determine compliance with the Statement of Objectives. For this purpose the Offeror shall provide in its Offer a draft Technical Solution Design and Integration Plan which shall demonstrate compliance with the objectives and sub-objectives in Book II Part IV Statement of Objectives.

3.5.2.10.5 Service delivery: The Offeror shall explain and provide enough evidence of how the proposed PWS will deliver the objectives in Book II Part IV Statement of Objectives. The Offeror shall provide sufficient detail for the Purchaser to determine compliance with the Statement of Objectives. The Offeror shall describe how the Information Technology Infrastructure Library (ITIL) service management framework will be applied to the delivery of the service.

3.5.2.10.6 Completed Service Objectives Compliance Table: The Offeror shall complete the service objectives compliance table found in ANNEX F.

3.5.2.10.6.1 Offerors shall respond if their proposal can deliver each of the individual service objectives by answering Yes/No/Partially to each of the objectives in the table.

3.5.2.10.6.2 Yes/No/Partially Criteria

3.5.2.10.6.2.1 Yes - The Offeror shall reply ‘YES’ if their proposal is able to deliver the individual service objective.

3.5.2.10.6.2.2 Partially - The Offeror shall reply ‘PARTIALLY’ if their proposal is able to deliver the individual service objective only partially.

3.5.2.10.6.3 No - The Offeror shall reply ‘NO’ if their proposal is not able to deliver the individual service objective.

3.5.2.11 Volume 3 - Service Implementation

3.5.2.11.1 This volume covers the service implementation component of the Technical Package and will be used to assess the Offeror’s ability to implement the service according to the proposed project milestones.

3.5.2.11.2 The volume shall include the following sections:

(a) Table of Contents for Volume 3

(b) Service implementation Project Overview

(c) Service implementation Project Management Plan

(d) Project Master Schedule (PMS)

(e) Testing and acceptance

(f) Security Accreditation

(g) Quality Assurance and Quality Control

(h) Documentation

(i) Training

3.5.2.11.3 Table of Contents. Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Package.

3.5.2.11.4 Service implementation Project Overview: The Offeror shall provide the Project Overview which shall provide an executive summary overview of the service

implementation project. The Project Overview shall also summarise the main features of each of the sections of Volume 3 and shall indicate in broad detail how the Project will be executed during the full lifetime of the Project in order to meet the objectives in Book II Part IV Statement of Objectives.

3.5.2.11.5 Service implementation Project Management Plan (PMP): defining how the Offeror intends to manage the service implementation project from contract signature through to Final Service Acceptance in order to meet the objectives in Book II Part IV Statement of Objectives.

3.5.2.11.5.1 The PMP shall consider all aspects of project management and control detailed in the PWS in Book II Part IV Statement of Objectives and demonstrate how all the critical dates defined in the contract will be met.

3.5.2.11.5.2 The PMP shall include a Work Breakdown Structure (WBS) that shall contain the critical work elements (tasks) of the project and illustrate their relationships to each other and to the project as a whole.

3.5.2.11.6 Project Master Schedule (PMS): that shall contain all contract events and milestones for the service implementation project. As described in the PWS in Book II Part IV Statement of Objectives ANNEX A, the PMS shall show all contractual deliverables, their delivery dates, and the tasks associated with them, including the Purchaser's review stages. The PMS shall, for each task, identify the start and finish dates, duration, predecessors, constraints, and resources. The PMS shall provide network, milestone, and Gantt views, and identify the critical path for the overall project. The PMS shall clearly identify the operational launch of the service (OLS) milestone, where OLS is the period, measured in days, between the Effective Date of the Contract (EDC) and the date of the operational launch of the service, according to the following formula:

OLS = Date of Operational Launch of the Service – EDC

3.5.2.11.7 Testing, verification and validation: The Offeror shall describe their proposed testing, verification and validation plan explaining how it can meet the testing requirements and its methodology for conducting all related activities in accordance with the PWS in Book II Part IV Statement of Objectives ANNEX A. This includes the development of all test documentation required under this Contract, the conduct of all testing and the evaluation and documentation of the tests results by an Independent Verification and Validation (IV&V).

3.5.2.11.8 Security Accreditation: The Offeror shall describe their input to the security accreditation documentation in support of the accreditation process in accordance with the PWS in Book II Part IV Statement of Objectives ANNEX A. The Offeror shall explain how it will implement and follow the security accreditation process described in the PWS in Book II Part IV Statement of Objectives ANNEX A. The Offeror shall provide a draft Security Accreditation Plan (SAP), initial High Level Design (HLD) for the initial CIS Description and an initial compliance check against required NATO Security directives, which describes how its proposed technical solution will implement requirements of the NATO security policies and demonstrates its understanding of the requirements in the PWS.

3.5.2.11.9 Quality Assurance and Control: The Offeror shall cover the Quality Assurance and Quality Control aspects of the Project in accordance with the PWS in Book II Part IV Statement of Objectives ANNEX A. This Section shall include the QA Plan (QAP), with details of how the Offeror shall establish, execute, document and

maintain an effective Quality Assurance (QA) program, throughout the Contract lifetime.

3.5.2.11.10 Documentation: The Offeror shall describe their Documentation Pack and proposed Project Portal in accordance with the PWS in Book II Part IV Statement of Objectives ANNEX A. The Contractor shall provide details on when and how the documents will be delivered

3.5.2.11.11 Training: The Offeror shall describe their training plan in accordance with the PWS in Book II Part IV Statement of Objectives ANNEX A.

3.5.2.12 Volume 4 - Risk

3.5.2.12.1 This volume covers the service implementation component of the Technical Package and will be used to assess the Offeror's ability to implement the service according to the proposed project milestones.

3.5.2.12.2 The volume shall include the following elements:

(a) Table of Contents for Volume 4

(b) Risk Management Plan (RMP)

(c) Corporate experience and individual skills

(d) Availability of the proposed service solution

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

3.5.2.12.4 Risk Management Plan (RMP): The Offeror shall describe in the initial RMP how it will implement the Risk Management process in accordance with the PWS in Book II Part IV Statement of Objectives ANNEX A. The Offeror shall describe how risks will be managed throughout the execution of the contract. The initial RMP shall include a Risk Log which shall at minimum follow the outline recommended in the PWS in Book II Part IV Statement of Objectives ANNEX A.

3.5.2.12.5 Corporate experience and individual skills: The Offeror shall describe how the experience and expertise of the prime Contractor and all nominated sub-Contractors will contribute to the successful execution of the Contract. The Technical Package shall provide a description of the corporate capabilities of the Offeror, including corporate experience, and individual skills in the fields of asset, configuration, patching and vulnerability management and of business intelligence/data analytics. The experience and skills shall be demonstrated for both the service implementation and service delivery. The Offeror shall provide at least one (1) summary describing the successful delivery of a similar service in a similar environment during the last five (5) years.

3.5.2.12.5.1 For each example of a similar service, the Contractor shall describe:

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

3.5.2.12.5.1.2 The scope of work, demonstrating its capability to implement and deliver an Enterprise ACPV service similar to the objectives defined in the Statement of Objectives.

3.5.2.12.5.2 The Offeror shall identify its major proposed sub-Contractors. Major proposed sub-Contractors, for purposes of this section, refer to the criteria set forth in Clause 12 “Sub-Contracts” of Book II Part II Terms and Conditions.

3.5.2.12.5.3 The Offeror shall identify the firm and the nation of origin and describe the contribution which the sub - Contractor is expected to make to the execution of the project.

3.5.2.12.5.4 The Offeror shall provide rationale for the selection of the sub-Contractor and describe the added value the sub-Contractor will bring to the execution of the project.

3.5.2.12.5.5 The Offeror shall describe their management structure put in place to manage the subcontractors.

3.5.2.12.5.6 The Offeror shall provide a description of individual skills and experience in relation to the project of all project team members and Subject Matter Experts (SMEs) foreseen to support the project team. The description shall include how each individual expertise and experience will add value to the team.

3.5.2.12.5.7 The Offeror shall provide the resumes / Curricula Vitae (CV) and supporting certification documentation (e.g. Prince 2 certificates) of each proposed Key Personnel. The CVs shall provide details about qualifications and evidence of the experience according to the requirements in the PWS in Book II Part IV Statement of Objectives ANNEX A.

3.5.2.12.5.8 In particular, the Offeror shall provide the CV of the proposed Project Manager, Technical Lead, Quality Assurance Representative (QAR) and Service Delivery Manager.

3.5.2.12.6 Availability of the proposed service solution: Offerors shall describe which parts of the proposed service solution are based on already existing and working services and which parts will require new ad-hoc integrations or developments.

3.5.2.13 Volume 5 – Performance Work Statement (PWS)

3.5.2.13.1 The Offeror shall provide the proposed Performance Work Statement (PWS) for the delivered product(s) and service(s) which shall be specified in accordance with the PWS template in Book II Part IV Statement of Objectives-ANNEX A, (including all annexes/exhibits). The PWS must, to the maximum extent practicable:

(a) Describe work in terms of required results and “how” the work is to be accomplished

(b) Enable assessment of work performance against measurable performance standards

NOTE: A Performance Work Statement (PWS) template is provided as an ANNEX A to Book II Part IV Statement of Objectives (SOO). The purpose of the PWS is to provide Offerors with a consistent structure in which their proposed requirements package must be submitted. PWS content is subject to adaptation and refinement as a result of the collaborative discussions taking place during dynamic sourcing Sprints 2 and 3.

3.5.2.13.2 The Offeror shall explicitly state that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and service(s) shall comply with the requirements in the PWS (including all annexes).

3.5.3 Price Offer Package

3.5.3.1 Interested firms will be required to submit price offers twice throughout the Solicitation process; once at the end of Sprint 2 (which will be evaluated during sprint 2) and a second time at the end of Sprint 3 (which will be evaluated during sprint 3).

NOTE 1: Only successful firms participating in the high level and detailed collaboration workshops (Sprints 2 and 3) will be required to submit a price proposal.

NOTE 2: Pricing sheets evaluated in Sprint 2 will only consist of an Offer and a CLIN Summary (high level), while Sprint 3 pricing sheets require details per CLIN about: labour, material, Other Direct Costs (ODC) and travel, if applicable. Sprint 3 pricing sheets therefore shall have more granularity.

3.5.3.2 Price Offer Package Contents (also refer to section 3.2)

3.5.3.2.1 Firms will submit one ZIP file by email, containing the completed Sprint 3 Pricing Sheets (Excel) and 1 PDF of the Pricing Sheets “Offer Summary” tab. All documentation stated in Section 3.2 shall be submitted.

3.5.3.3 General Rules

3.5.3.3.1 Offerors shall prepare their Price Offer by completing the Pricing Sheets referred in Section 3.5.3.2.1 above, in accordance with the instructions specified in ANNEX A-2.

3.5.3.3.2 The structure of the Pricing Sheets shall not be changed, other than as indicated elsewhere, nor should any quantity or item description in the Pricing Sheets. The currency(ies) of each Contract Line Item and sub-item shall be shown. Offerors may use one pricing sheet per currency if quoting in multiple currencies. The prices provided shall be intended as the comprehensive total price offered for the fulfilment of all requirements as expressed in the RFS documentation and as discussed during the collaboration workshops.

3.5.3.3.3 When completing the Pricing Sheets the Offeror shall insert information in all yellow cells of the Pricing Sheets and complete the Offer Summary as instructed. A price for each specified element needs to be supplied on each CLIN. Prices should not be grouped. Prices and quantities entered on the document shall reflect the total items required to meet the contractual requirements. The total price shall be indicated in the appropriate columns and in the currency quoted. If the price of a line item is expressed in different currencies, these shall be identified, and there shall be as many totals on that line item as there are currencies; unless Offerors choose to use one pricing sheet per currency. In preparing the Price Offer, Offerors shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part. In Sprint 3, price and quantity against each CLIN and sub-CLINs will be required.

3.5.3.3.4 Offerors shall furnish Firm Fixed Prices for all required items in accordance with the format set forth in the Instructions for preparation of the Pricing Sheets for Sprint 3 (different sets of instructions than in Sprint 2).

3.5.3.3.5 Offerors shall furnish Firm Fixed Prices for all CLINs as defined in the Schedule of Supplies and Services (SSS). Purchaser evaluation of the submitted Offers will be on the basis of the complete submission including administrative, price and technical components for all CLINs. The Contract will be awarded for all CLINs, with CLINs 1 through 10 being the basic contract and the services defined for

CLINs 11 and 12 being Firm Fixed Evaluated Price options to the Contract. These options may be exercised by the Purchaser, at the sole discretion of the Purchaser. The Purchaser's decision to exercise any Options will take into consideration the Contractor's successful performance on the basic contract, as well as the availability of the required funding.

3.5.3.3.6 Offered prices shall not be "conditional" in nature. Any comments supplied in the Pricing Sheets or in any part of the Offer package which are conditional in nature, relative to the offered prices may result in a determination that the Offer is non-compliant.

3.5.3.3.7 Offerors are responsible for the accuracy of their Price Offers. Price Offers that have apparent computational errors may have such errors resolved in the Purchaser's favour or, in the case of gross omissions, inconsistencies or errors, may be determined to be non-compliant. In the case of inconsistencies between the electronic version of the Pricing Sheets and the PDF of the Pricing Sheets, the "hard copy, PDF version" will be considered by the Purchaser to have precedence over the electronic version.

3.5.3.3.8 Offerors shall quote in their own national currency or in EURO. Offerors may also submit Offers in multiple currencies including other NATO member states' currencies under the following conditions:

3.5.3.3.8.1 the currency is of a "participating country" in the project, and

3.5.3.3.8.2 the Offeror can demonstrate, either through sub-contract arrangements or in its proposed work methodology, that it will have equivalent expenses in that currency. All major subcontracts and their approximate anticipated value should be listed on a separate sheet and included with the Price Offer.

3.5.3.3.9 The Purchaser, by virtue of its status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct and indirect taxes (incl. VAT) and all customs duties on merchandise imported or exported.

3.5.3.3.10 Offerors shall therefore exclude from their Price Offer all taxes, duties and customs charges from which the Purchaser is exempted by international agreement and are required to certify that they have done so through execution of the Certificate at ANNEX B-2.

3.5.3.3.11 The Offerors' attention is directed to the fact that Price Offer shall contain no document and/or information other than the priced copies of the Pricing Sheets. However, the NCI Agency reserves the right to use any information obtained through collaboration workshops during the evaluation.

3.5.3.3.12 All prices offered shall be clearly traceable in the detailed pricing sheets.

3.5.3.3.13 Any adjustment or discount to prices should be clearly traceable to the lowest level of breakdown in the pricing sheets and should not be aggregated or summed. Any lack of clarity or traceability may render the offer non-compliant.

3.5.3.3.14 The Offeror understands that there is no obligation under this contract for the Purchaser to exercise any of the optional line items and that the Purchaser bears no liability should it decide not to exercise the options (totally or partially). Further, the Purchaser reserves the right to order another Contractor (or the same), to perform the tasks described in the optional line items of the current contract through a new contract with other conditions.

SECTION 4. **OFFER EVALUATION**

4.1 BASIS FOR AWARD

4.1.1 The evaluation of Offers will be made by the Purchaser solely on the basis of the requirements specified in this RFS.

4.1.2 This procurement will conduct three separate down selection activities throughout the procurement process consisting of Administrative, Technical and Price evaluations. The initial down selection will be conducted at the end of Sprint 1 and based on an Administrative evaluation followed by a Technical evaluation comprising a Pre-Qualification Questionnaire and Executive Summary. Offers not meeting all of the mandatory administrative requirements may be determined to be non-compliant and not further considered in the evaluation or for award After the Administrative Compliance is complete, Pre-Qualification Questionnaires will be evaluated to select no more than five (5) Offerors who will be invited to participate in Sprint 2 high level collaboration workshops. The Executive Summary will only be evaluated if the NCI Agency is unable to select five (5) Offerors through the assessment of Pre-Qualification Questionnaires. The second and third down selection activities will be conducted using the Best Value trade-off methodology. The second and third down selection activities will based conducted during Sprints 2 and 3 and will be based on a best value methodology using Technical Report/Package and Price Offers.

4.1.3 The NCI Agency reserves the right to eliminate from consideration for award any or all offers at any time prior to award of the contract; to negotiate with offerors; and to award the contract to the offeror submitting the offer determined to represent the best value-the offer most advantageous to NATO, price and other factors considered.

4.1.4 As stated in the RFS, the NCI Agency intends to evaluate offers and award a contract after conducting discussions through the Dynamic Sourcing workshop plan during Sprints 2 and 3. If the Contracting Officer determines that the number of offers that would otherwise be moved from one Sprint to the next exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the range to the greatest number that will permit an efficient competition among the most highly rated offers. The NCI Agency's goal is to down select from all eligible firms identified in the Sprint 1 to five (5) firms in Sprint 2, then down select to two (2) firms in Sprint 3, and select the Best Valued solution at the end of Sprint 3.

4.1.5 The Best Value trade-off process is selected as appropriate for this procurement. The NCI Agency considers it to be in its best interest to allow consideration of award to other than the lowest priced offeror or other than the highest technically rated offeror.

4.1.6 As stated in the RFS, all technical factors when combined are of equal importance to the performance confidence assessment (Pre-Qualification Questionnaire) rating; and all technical factors and the performance confidence assessment (Pre-Qualification Questionnaire) rating, when combined are significantly more important than price as detailed in paragraph 4.1.9.2 below.

4.1.7 Any proposal found to have a deficiency in meeting the stated RFS requirements or performance objectives will be considered ineligible for award, unless the deficiency is corrected through discussions. Offers may be found to have either a significant weakness or multiple weaknesses that impact either the individual factor rating or the

overall rating for the proposal. The evaluation report must document the evaluation board's assessment of the identified weakness(s) and the associated risk to successful contract performance resulting from the weakness(s). This assessment must provide the rationale for proceeding to award without discussions.

4.1.8 The maximum possible Best Value Final Score is one-hundred (100); the minimum possible is zero (0). The Offer with the highest Best Value Final Score will be recommended to be potential successful Offeror.

4.1.9 The Offer evaluation criteria, and associated weightings, are as follow:

4.1.9.1 Administrative Compliance - Compliant/non-compliant; no scoring or weighting (not evaluated using a best value methodology)

4.1.9.2 Technical Evaluation

4.1.9.2.1 Sprint 1: The Pre-qualification Questionnaire is a tool used in Sprint 1 to ensure high level and detailed collaboration workshops are held with Offerors with capabilities to deliver a solution for the Enterprise ACPV Service. Therefore, responses to the RFS (Pre-Qualification Questionnaire) will be evaluated using a distinctive methodology.

4.1.9.2.2 Sprints 2 and 3: (%T=70%) comprising Service Objectives Compliance (C) (60%), Service Implementation (S) (20%), Risk (R) (20%). Technical evaluations will be conducted using Adjectival Ratings; Unsatisfactory, Marginal, Satisfactory, Very Good, Excellent. Weighted Technical Score will be realized using the formula in paragraph 4.1.10.

4.1.9.3 Price Evaluation (%P=30%) comprising the Offerors' stated price for the sum of all evaluated CLINs, assessed as realistic and fulfilling the requirements of the Pricing Sheets in the RFS, with the Weighted Price Score using the formula in paragraph 4.1.11.

4.1.10 The technical weight will be applied to the raw Technical Score (TS) to produce the weighted technical score.

TS = a%*TS1 + b%*TS2 + c%*TS3

Where: TS1, TS2, TS3 ≤ 100 are the Technical Scores of each second-level or published third-level technical sub-criteria; and a% b% c% are the related weighting factors for each of the second-level or third-level technical sub-criteria adding up to 100%.

4.1.11 The Price Score (PS) shall be determined according to the following formula:

PS = 100 * [1 - (Offer Price / (2 * Average Offer Price))]

4.1.12 The Best Value Final Score (FS) will be the sum of the weighted Technical Score (TS) plus the Price Score (PS) according to the following formula:

FS = TS*70% + PS*30% ≤ 100

4.2 TECHNICAL EVALUATION RATINGS/DESCRIPTIONS

4.2.1 **Sprint 1**

4.2.1.1 The technical rating reflects the degree to which the Offerors will be capable of delivering a solution for the Enterprise ACPV Service, based on their responses.

4.2.1.1.1 Offerors shall respond to the Pre-Qualification Questionnaire requirements, providing sufficient evidence of Offeror's capabilities to deliver a solution for the Enterprise ACPV Service.

4.2.1.1.2 The Pre-Qualification Questionnaire will consist in two sections, each of them with distinctive approach. The first part of the Pre-Qualification Questionnaire, found in ANNEX C-1, includes open ended questions while the second part of the questionnaire, found in ANNEX C-2, includes a self-declared compliance criteria of 'YES', 'PARTIALLY', and 'NO'.

4.2.1.2 Pass/Fail Criteria.

4.2.1.2.1 Offerors will provide a brief narrative addressing each of the questions using the below criteria. Each question will have a weighting factor based on relevancy to ACPV and responses shall be provided in accordance with below response criteria.

4.2.1.2.1.1 Each requirement evaluated with a "Pass" will receive a score of 8 for "High" weighting factor requirements, 5 for "Medium" weighting factor requirements and 3 for "Low" weighting factor requirements.

4.2.1.2.1.2 Requirements evaluated with a "Fail" will receive a score of 0.

4.2.1.2.1.3 Failure to comply with one requirement marked as "High" weighting factor, two "Medium" ones or three "Low" ones may be a basis for disqualification.

Table 1. Pre-Qualification Questionnaire / PASS-FAIL Rating Method

Weighting Factor	Description
High (**H**)	A narrative addressing each question marked as "High" and not exceeding 500 words shall be provided. (8 points)
Medium (**M**)	A narrative addressing each question marked as "Medium" and not exceeding 300 words shall be provided. (5 points)
Low (**L**)	A narrative addressing each question marked as "Low" and not exceeding 200 words shall be provided. (3 points)

4.2.1.3 Yes/No/Partially Criteria.

4.2.1.3.1 Offerors shall respond if their proposal can deliver each of the individual service objectives by answering Yes/No/Partially to each of the objectives in the table in accordance with response criterial shown below.

4.2.1.3.1.1 Proposals will receive a score of 1 for each service objective with an answer “YES” and of 0.5 for each service objective with an answer of “Partially”.

4.2.1.3.1.2 The scores resulting from the evaluation of the prequalification questionnaire as described in ANNEX C-1 and ANNEX C-2 and evaluated according to sections 4.2.1.2 and 4.2.1.3 will be added and a total prequalification questionnaire score will be determined.

Table 2. Pre-Qualification Questionnaire / Self-Assessment Rating Method	
Weighting Criteria	**Description**
Yes (**Y**)	The Offeror shall reply ‘YES’ if their proposal is able to deliver the individual service objective. (1 point)
Partially (**P**)	The Offeror shall reply ‘PARTIALLY’ if their proposal is able to deliver the individual service objective only partially. (0.5 point)
No (**N**)	The Offeror shall reply ‘NO’ if their proposal is not able to deliver the individual service objective. (0 points)

4.2.1.4 Proposals will be ranked according to the prequalification questionnaire score and the five proposals with the highest score will be selected to move to Sprint 2.

4.2.1.5 Should there be a number of proposals after the evaluation of Pre-Qualification Questionnaires with the same score, precluding from choosing the best five, the proposals with equal score will be evaluated against the Executive Summary using the ratings as described in section 4.2.2.1.1.

4.2.2 **Sprints 2 and 3**

4.2.2.1 The technical rating reflects the degree to which the proposed approach meets or does not meet the minimum performance or capability requirements through an assessment of the strengths, weaknesses, significant weaknesses, deficiencies, and risks of an offer.

4.2.2.1.1 A combined technical/risk evaluation considering risk in conjunction with the strengths, weaknesses, significant weaknesses, and deficiencies in determining technical ratings shall be used. The technical risk evaluation shall utilize the combined technical/risk ratings listed in the following table. Adjectival ratings and rating descriptions will be used to assign an overall rating to each technical proposal and to assign a rating for each technical factor. Use upper case letter ratings for major technical factors as well as the overall rating. The addition of plus (+) or minus (-) to an adjective rating is not allowed.

Table 3. Combined Technical/Risk Rating Method	
Adjectival Rating	**Description**
Excellent (**E**)	A comprehensive and thorough offer of exceptional merit with multiple significant strengths. No deficiency or significant weakness exists. Risk of unsuccessful performance is low. (10 points)
Very Good (**G**)	Offer having no deficiency and which demonstrates over-all competence. One or more significant strengths have been found, and strengths outbalance any weaknesses that exist. Risk of unsuccessful performance is low to moderate. (8 points)
Satisfactory (**S**)	Offer having no deficiency and which shows a reasonably sound response. There may be strengths or weaknesses, or both. As a whole, weaknesses not off-set by strengths do not significantly detract from the Offeror's response. Risk of unsuccessful performance is no worse than moderate. (5 points)
Marginal (**M**)	Offer having no deficiency and which has one or more weaknesses. Offer marginally meets criterion but has numerous and significant weaknesses and/or omissions. Weaknesses outbalance any strengths. Risk of unsuccessful performance is high. (3 points)
Unsatisfactory (**U**)	Offer has one or more deficiencies or significant weaknesses that demonstrate a lack of overall competence or would require a major offer revision to correct. Risk of unsuccessful performance is unacceptable. Offer is unawardable. (0 points)

4.2.2.2 Definitions: The following definitions are provided to assist evaluators in the evaluation of each non-cost/price factor.

4.2.2.2.1 Strength: An aspect of an offer that has merit or exceeds specified performance or capability requirements in a way that will be advantageous to NATO during contract performance.

4.2.2.2.2 Weakness: A flaw in the offer that increases the risk of unsuccessful contract performance.

4.2.2.2.3 Significant Weakness: A flaw that appreciably increases the risk of unsuccessful contract performance.

4.2.2.2.4 Deficiency: A material failure of an offer to meet a NATO requirement or a combination of significant weaknesses in an offer that increases the risk of unsuccessful contract performance to an unacceptable level.

4.3 EVALUATION PROCEDURE

4.3.1 This procurement will have three (3) separate down selection activities throughout the procurement process consisting of Administrative, Technical and Price evaluations. The initial down selection will be conducted at the end of Sprint 1 and based on an Administrative evaluation followed by a Technical evaluation comprising a Pre-Qualification Questionnaire and Executive Summary. Offers not meeting all of the mandatory administrative requirements may be determined to be non-compliant and not further considered in the evaluation or for award After the Administrative Compliance is complete, Pre-Qualification Questionnaires will be evaluated to select no more than five (5) Offerors who will be invited to participate in Sprint 2 high level collaboration workshops. The Executive Summary will only be evaluated if the NCI Agency is unable to select five (5) Offerors through the assessment of Pre-Qualification Questionnaires. The second and third down selection activities will be conducted during Sprints 2 and 3 and will be based on a best value methodology using Technical Report/Package and Price Offers.

4.3.2 All three (3) evaluations will be conducted at the end of Sprints 1, 2 and 3, as described below:

4.3.2.1 **Sprint 1**

4.3.2.1.1 Administrative Compliance

4.3.2.1.1.1 Offers received will be reviewed for compliance with the mandatory Administrative requirements specified in Section 4.4.2. Offers not meeting all of the mandatory requirements may be determined to be non-compliant and not further considered in the evaluation or for award.

4.3.2.1.2 Technical Solution Evaluation

4.3.2.1.2.1 Responses to the Pre-qualification Questionnaire and corresponding Executive Summary will be evaluated to ensure high level and detailed collaboration workshops are held with Offerors possessing the capabilities to deliver a solution for the Enterprise ACPV Service.

4.3.2.2 **Sprint 2**

4.3.2.2.1 Technical Report Evaluation

4.3.2.2.1.1 Offers will have their Technical Offer Packages evaluated against predetermined top-level criteria and identified sub-criteria, and scored accordingly. This evaluation will result in “raw” or not weighted technical scores against the criteria.

4.3.2.2.1.2 Offerors are advised that any Technical Offer receives a score of less than 20% of the not weighted raw score possible in any of the sub-criteria listed in Section 4.5.2 of this document may be determined by the Purchaser to be non-compliant and not further considered for award.

4.3.2.2.2 Price Offer Evaluation

4.3.2.2.2.1 The high level Price Offers will be evaluated and scored in accordance with Section 4.5.3.

4.3.2.3 **Sprint 3**

4.3.2.3.1 Technical Package Evaluation

4.3.2.3.1.1 Offers will have their Technical Offer Packages evaluated against predetermined top-level criteria and identified sub-criteria, and scored accordingly. This evaluation will result in “raw” or not weighted technical scores against the criteria.

4.3.2.3.1.2 Offerors are advised that any Technical Offer receives a score of less than 20% of the not weighted raw score possible in any of the sub-criteria listed in Section 4.6.2 of this document may be determined by the Purchaser to be non-compliant and not further considered for award.

4.3.2.3.2 Price Offer Evaluation

4.3.2.3.2.1 The high level Price Offers will be evaluated and scored in accordance with Section 4.6.3.

4.3.3 **Upon completion of the Sprint 3 Evaluation, the Successful Offer will be determined in accordance with Section 4.7 hereafter.**

4.4 SPRINT 1

4.4.1 This procurement will have three (3) separate down selection activities conducted at the end of Sprints 1, 2 and 3. Sprint 1 will be based on the assessment of all Administrative certificates as well as the evaluation of Pre-Qualification Questionnaires submitted in response of this Request for Solution (RFS). At the end of Sprint 1, and as a result of its pre-qualification based evaluation, only five (5) Offerors will be selected and invited to participate in Sprint 2 high level collaboration workshops. The remaining Offerors will be notified of the results in due time. Offerors shall refer to section 3.2 for packaging and marking requirements. Additionally, Offerors shall refer to Section 3.3.2 and 3.3.3 for details on Administrative and Technical solution package requirements.

4.4.2 Administrative Offer Package

4.4.2.1 Prior to evaluating Pre-Qualification Questionnaires or technical aspects of firms' proposed solutions, the NCI Agency will evaluate Administrative Compliance. Offers will be reviewed for compliance with the formal requirements for Offer submission as stated in this RFS and the content of the Administrative Offer Package. The evaluation of the Administrative Offer Package will be made on its completeness, conformity and compliance to the requested information. This evaluation will not be scored in accordance with Best Value procedures but is made to determine if an Offer complies with the requirements of the RFS Instructions and Prospective Contract. Specifically, the following requirements shall be verified:

4.4.2.2 The Offer was received by the RFS Closing Date and Time;

4.4.2.3 The Offer is packaged and marked properly;

4.4.2.4 The Administrative Offer Package contains the documentation listed in Section 3.2 above and complies with the formal requirements established in Section 3.3.2 above;

4.4.2.5 The Offeror **has not taken exception** to the Terms and Conditions of the Prospective Contract or has not qualified or otherwise conditioned its offer on a modification or alteration of the Terms and Conditions or the language of the SOO (including all its Annexes); and

4.4.2.6 Evaluation of Conflict of Interest Documentation

4.4.2.7 The Purchaser will evaluate the Offeror's submission in accordance with Book II Part II Terms and Conditions Clause 38 and as detailed in Section 3.3.2.7.1 and resort to the disqualification of the Offer in those cases in which it is deemed that the Offeror's relationships with the Cyber Evaluation and Adaptation Contractor, Dynamic Sourcing Process Augumentation Support Contractor, or Programmatic and Technical Augmentation Support Contractor could constitute a real or apparent conflict of interest, could in any manner or form influence or appear to influence the capacity of the Offeror to render unbiased service or otherwise result in an advantage during the course of the performance under the prospective Contract and any proposed conflict of interest mitigation plan proposed by the Offeror does not satisfactorily resolve the conflict of interest in place.

4.4.2.8 Conversely, should the Purchaser deem that the Offeror's Conflict of Interest Mitigation Plan adequately addresses the concerns relevant to any conflict of interest, it will

make such plan part of any awarded Contract and subject to the stipulation of Clause 38 of the Terms and Conditions. Equally in those cases where the Offeror declares that no apparent or real conflict of interest exists such condition shall be reflected in any resulting Contract and made subject to the prescription of Clause 38 of the Terms and Conditions.

4.4.2.9 In the event that, during the evaluation of the Offers, the Purchaser would determine or suspect that the Offeror has not disclosed a real or apparent conflict of interest of which it was knowledgeable at the time of Offer submission, in breach of Sections 4.4.2.7 and 4.4.2.8, Purchaser reserves the right to declare the Offer non-compliant.

4.4.2.10 Subject to the stipulation of Section 4.4.2.2 through 4.4.2.5 Offers failing to conform to the above requirements may be declared non-compliant and may not undergo through further evaluation. Offers that are determined to be administratively compliant will proceed to the Technical Evaluation.

4.4.2.11 Notwithstanding paragraph 4.4.2.10, if it is later discovered in the evaluation of the Technical Offer or the Price Offer that the Offeror has taken exception to the Terms and Conditions of the Prospective Contract, or has qualified and/or otherwise conditioned their offer on a modification or alteration of the Terms and Conditions or the language of the SOO (including all its Annexes), the Offeror may be determined to have submitted a non-compliant Offer at the point in time of discovery.

4.4.3 Technical Solution Package

4.4.4 The Technical evaluation comprises a Pre-Qualification Questionnaire and Executive Summary. Offers not meeting all of the mandatory administrative requirements may be determined to be non-compliant and not further considered in the evaluation or for award After the Administrative Compliance is complete, Pre-Qualification Questionnaires will be evaluated to select no more than five (5) Offerors who will be invited to participate in Sprint 2 high level collaboration workshops. The Executive Summary will only be evaluated if the NCI Agency is unable to select five (5) Offerors through the assessment of Pre-Qualification Questionnaires.

4.4.4.1 The Technical Evaluation will be based on:

a) Assessment of the Pre-Qualification Questionnaire

b) Executive Summary (tie breaker)

4.4.4.2 Assessment of the Pre-Qualification Questionnaire found in ANNEX C-1 and ANNEX C-2, and described in section 3.3.3. The assessment shall be done according to PASS/FAIL requirements criteria for the questions in ANNEX C-1 and against YES/NO/PARTIALLY service objectives compliance criteria for the questions in ANNEX C-2. The proposals shall be evaluated to confirm compliance with the sub criteria in sections 4.4.4.2.1 and 4.4.4.2.3 :

4.4.4.2.1 PASS/FAIL Criteria – ANNEX C-1:

4.4.4.2.1.1 The tenderer must have been in operation for at least 5 years by the deadline for submission of offers

4.4.4.2.1.2 The tenderer must have over 5 years of business experience in the type of services and domains which are the subject of this procurement.

4.4.4.2.1.3 The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractual work for Asset and configuration

management services"

4.4.4.2.1.4 The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractual work for Vulnerability management services

4.4.4.2.1.5 The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractual work for Business Intelligence/data analytics services

4.4.4.2.1.6 The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractual work for Patch Management services.

4.4.4.2.1.7 The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of at least 2 relevant experiences in a multi-national and/or multi-national military environment.

4.4.4.2.1.8 The tenderer must demonstrate inclusion on the team of technical asset, configuration, patching and vulnerability management experts, meeting the minimum experience required of 5 years

4.4.4.2.1.9 The tenderer must be proficient in an English language environment. French language proficiency is desirable, but not mandatory.

4.4.4.2.1.10 The tenderer must have the financial capacity to provide the required services. Specifically, the tenderer must have had an average annual revenue, after expenses, of at least 30MEUR

4.4.4.2.1.11 The tenderer must be able to contract from a NATO Nation

4.4.4.2.1.12 The tender must not have had a contract Terminated for Default (T4D) in the past 5 years

4.4.4.2.1.13 The tenderer must be able to demonstrate their ability to staff the opportunity with NATO security cleared personnel to deliver the required services.

4.4.4.2.1.14 The tender must have current security accreditations required to work with NATO (valid Designation of Eligibility received)

4.4.4.2.1.15 Data Residency – the tenderer must certify data will only be shared/stored to NATO Nation.

4.4.4.2.1.16 The tenderer must demonstrate a teamed arrangement, if necessary. That is that NATO has a direct and only contract with the prime Service Providers. Sub relationships, through sub-contracting is however authorized as long as the industry teaming arrangement members are part of NATO Nations.

4.4.4.2.1.17 The tenderer must comply with the request to deliver Enterprise ACPV Service as a managed service

4.4.4.2.1.18 The tenderer must have resource capacity in NATO Nations to deliver the required services.

4.4.4.2.1.19 The tenderer must have sufficient geographic coverage to provide service resiliency across NATO nations.

4.4.4.2.2 Pass/Fail Evaluation

4.4.4.2.2.1 Pass – The Offeror has provided sufficient evidence in their response that their proposal meets the requirement.

4.4.4.2.2.2 Fail – The Offeror has not provided enough evidence in their response that their proposal meets the requirement.

4.4.4.2.2.3 Each of the requirements in section 4.4.4.2.1 is given a weighting factor of “High”, “Medium” or “Low” as described in ANNEX C-1.

4.4.4.2.2.4 Each requirement evaluated with a “Pass” will receive a score of 8 for “High” weighting factor requirements, 5 for “Medium” weighting factor requirements and 3 for “Low” weighting factor requirements.

4.4.4.2.2.5 Requirements evaluated with a “Fail” will receive a score of 0.

4.4.4.2.2.6 Failure to comply with one requirement marked as “High” weighting factor, two “Medium” ones or three “Low” ones may be a basis for disqualification.

4.4.4.2.3 Service Objectives Compliance – ANNEX C-2

4.4.4.2.3.1 Proposals will receive a score of 1 for each service objective with an answer “YES” and of 0.5 for each service objective with an answer of “Partially”.

4.4.4.2.4 The scores resulting from the evaluation of the prequalification questionnaire as described in ANNEX C-1 and ANNEX C-2 and evaluated according to sections 4.4.4.2.1 and 4.4.4.2.3 will be added and a total prequalification questionnaire score will be determined.

4.4.4.2.5 Proposals will be ranked according to the prequalification questionnaire score and the five proposals with the highest score will be selected to move to Sprint 2.

4.4.4.3 Should there be a number of proposals after the evaluation of Pre-Qualification Questionnaires with the same score, precluding from choosing the best five, the proposals with equal score will be evaluated against the Executive Summary.

4.4.4.3.1.1 The Executive Summary will be evaluated against the following sub criteria:

4.4.4.3.1.1.1 Service Objectives compliance (60%)

a) Overall understanding of the goal and expected outcome of the Enterprise ACPV project

b) Demonstration of the suitability of the proposed technical solution to meet the goal and expected outcome of the Enterprise ACPV project

c) Support of NATO asset types as described in Book II Part IV Statement of Objectives

d) Integration with NATO Tier 2 systems as described in Book II Part IV Statement of Objectives

e) Suitability of the service delivery and service management approach to meet the service goal and service outcome

f) Use of ITIL or an equivalent service management framework.

4.4.4.3.1.1.2 Implementation schedule (20%)

a) Suitability of the service implementation approach to guarantee the execution of the project according to the PMS

b) Quality of the PMS

c) Date of the operational launch of the service. The PMS shall clearly identify the operational launch of the service (OLS) milestone, where OLS is the period, measured in days, between the Effective Date of the Contract (EDC) and the date of the operational launch of the service, according to the following formula:

OLS = Date of Operational Launch of the Service – EDC

The Date Score (DS) for the evaluation of the operational launch of the service milestone shall be determined according to the following formula:

DS = 100 * [1 – (OLS / (2* Average OLS))]

d) Suitability of the testing, verification and validation approach to ensure the service will meet the goal and expected outcome

4.4.4.3.1.1.3 Risk (20%)

a) Assessment of the project risk level.

b) Credibility of the PMS

c) Suitability of the corporate experience and individual skills to meet the goal and expected outcome of the service.

d) Suitability of the subcontracting approach

e) Availability of the proposed service solution

f) Assessment of the individual service objectives compliance risk

4.4.4.3.2 The offers tied during the evaluation of Pre-Qualification Questionnaires and will be ranked based on the evaluation of Executives Summaries and the highest scored offers will be selected to complete the shortlisting activity under Sprint 1.

4.4.4.3.3 A total of five (5) Offerors representing the top five (5) scores using the Pre-Qualification Questionnaires and Executive Summary (if necessary) will be selected to complete the shortlist of five Offerors.

4.5 SPRINT 2

4.5.1 This procurement will have three (3) separate down selection activities conducted at the end of Sprints 1, 2 and 3. Sprint 2 will be based on the evaluation of Offerors Technical Solution package and its corresponding Price Offer package. Both Technical and Price packages will be based on information discussed during Sprint 2 high-level collaboration workshops held with all five (5) Offerors selected in the prior Sprint 1. At the end of Sprint 2, and as a result of its best value evaluation, two (2) out of five (5) Offerors will be selected and invited to participate in Sprint 3 detailed collaboration workshops. The remaining three (3) Offerors will be notified of the results in due time. Offerors will refer to section 3.2 for packaging and marking requirements. Additionally, Offerors will refer to Section 3.4.2 and 3.4.3 for details on Technical Solution and Price Offer package requirements.

4.5.2 Technical Report Evaluation

4.5.2.1 The Technical Offer will be evaluated against the criteria and sub criteria set forth in this section. For some sub-criteria, there may be additional supporting factors at the next lower level. These lower level factors are not published here but are predetermined and included in the Technical Evaluation Weighting Scheme. This evaluation will be conducted throughout the Technical Report which consists of four (4) volumes: Executive Summary, Service Objectives Compliance, Service Implementation and Risk. Within each of the four (4) volumes of the Technical Proposal the criteria and their sub criteria are identified as follows:

4.5.2.1.1 Criteria - The Offeror shall provide a completed Cross-Reference Table in accordance with section 3.4.2.6. Failure to submit the completed Cross-Reference Table will be deemed non-compliant.

4.5.2.2 **Volume 1 – Executive Summary**

4.5.2.2.1 Criteria - The Offeror shall provide an executive summary. Failure to submit an executive summary will be deemed non-compliant.

4.5.2.3 **Volume 2 – Service Objectives Compliance**

4.5.2.3.1 Criteria - The Offeror shall provide a PWS compliance statement in accordance with paragraph 3.4.2.9.6.1. Failure to submit the PWS compliance statement will be deemed non-compliant.

4.5.2.3.2 Criteria - The Offeror shall provide a completed Service Objectives Compliance Table in accordance with section 3.4.2.9.7. Failure to submit the completed Service Objectives Compliance Table will be deemed non-compliant.

4.5.2.3.3 In addition to the criteria in paragraphs 4.5.2.3.1 and 4.5.2.3.2, the offer will be evaluated against the criteria in section 4.5.2.3.4.

4.5.2.3.4 Criteria – Service Objectives Compliance (60% of the Technical Proposal, to assess the initial technical solution design and integration proposal, the service delivery approach, the draft performance requirements summary and the objectives compliance)

4.5.2.3.4.1 Third-level sub criteria in the following order of importance:

a) Initial Technical Solution Design and Integration proposal in the following order of importance:

1. Demonstration of the suitability of the proposed technical solution to meet the goal, expected outcome and service objectives of the Enterprise ACPV project.
2. Compliance of the proposed technical solution and integration proposal with the service objectives
3. Overall quality of the Initial Technical Solution Design and Integration proposal

b) Service Delivery approach in the following order of importance:

1. Demonstration of the suitability of the proposed service delivery approach to meet the service goal, expected outcome and objectives
2. Compliance of the proposed service delivery approach with the service objectives
3. Overall quality of the service delivery approach

c) Draft Performance Requirements Summary in the following order of importance:

1. Suitability of the draft performance requirements summary to meet the goal, expected outcome and objectives of the service
2. Compliance of the Draft Performance Requirements Summary with the service objectives
3. Quality of the proposed Draft Performance Requirements Summary

4.5.2.4 Volume 3 – Service Implementation

4.5.2.4.1 Criteria – Service Implementation Schedule (20% of the Technical Proposal, to assess the service implementation approach, the implementation schedule and the testing, verification and validation approach)

4.5.2.4.1.1 Third-level sub criteria in the following order of importance:

a) Project Master Schedule (PMS) in the following order of importance:

1. Operational launch of the service milestone. The Date Score (DS) for the evaluation of the operational launch of the service milestone shall be determined according to the following formula:

DS = 100 * [1 – (OLS / (2* Average OLS))]

where OLS is the period, measured in days, between the Effective Date of the Contract (EDC) and the date of the operational launch of the service, according to the following formula:

OLS = Date of Operational Launch of the Service – EDC.

2. Demonstration of the suitability of the draft PMS to meet the goal, expected outcome and service objectives of the Enterprise ACPV service according to the agreed schedule, cost and scope.

3. Compliance of the proposed draft PMS with the PWS requirements
4. Overall quality of the draft PMS

b) Service Implementation approach in the following order of importance:

1. Demonstration of the suitability of the service implementation approach to meet the goal, expected outcome and service objectives of the Enterprise ACPV project according to the agreed schedule, cost and scope.
2. Compliance of the proposed service implementation approach with the PWS requirements.
3. Overall quality of the service implementation approach

c) Testing, verification and validation approach in the following order of importance:

1. Sprint 3 use case
2. Demonstration of the suitability of proposed testing verification and validation approach to meet the goal, expected outcome and service objectives of the Enterprise ACPV project in the shortest possible time.
3. Compliance of the proposed testing verification and validation approach with the PWS requirements
4. Overall quality of the proposed testing verification and validation approach

4.5.2.5 Volume 4 – Risk

4.5.2.5.1 Criteria – Risk (20% of the Technical Proposal, to assess project risk, service compliance risks, corporate experience and availability of the proposed service solution)

4.5.2.5.1.1 Third-level sub criteria in the following order of importance:

a) Initial project risk management analysis in the following order of importance:

1. Assessment of the project risk level from the initial project risk management analysis.
2. Compliance of the proposed risk management analysis with the PWS requirements
3. Overall quality of the initial risk management analysis.

b) Credibility of the PMS

c) Corporate experience and individual skills in the following order of importance:

1. Demonstration of the suitability of the corporate experience and individual skills description to meet the goal, expected outcome and service objectives of the Enterprise ACPV service according to the agreed schedule, cost, scope and performance targets.
2. Compliance of the corporate experience and individual skills description with the instructions in 3.4.2.11.5.

3. Suitability of the subcontracting approach
4. Overall quality of the Corporate experience and individual skills description

d) Availability of the proposed service solution

e) Assessment of the individual service objectives compliance risk

f) Suitability of the proposed solution for NATO

4.5.3 Price Offer Evaluation

4.5.3.1 Price will not be evaluated during the initial down selection activity, Sprint 1.

4.5.3.2 Price evaluation will take place twice throughout the dynamic sourcing process:

- During Sprint 2, the high-level pricing sheets submitted in the RFS package will be evaluated against the price criteria listed hereinafter.

- During Sprint 3, the detailed pricing sheets submitted to the shortlisted Offerors will be evaluated against the same price criteria, listed hereinafter.

NOTE 1: The granularity level of the two pricing sheets will vary.

NOTE 2: Specific criteria will only be applicable for Sprints 2 and 3 pricing sheets assessment (identified in the list below).

4.5.3.3 The Offeror's Price Offer will be first assessed for compliance against the following criteria:

4.5.3.3.1 The Price Offer meets the requirements set forth in the Offer Preparation Section and the Instructions for Preparation of the Pricing Sheets in ANNEX A-2.

4.5.3.3.2 Adequacy, accuracy, traceability and completeness of detailed pricing information.

4.5.3.3.2.1 The Offeror has furnished Firm Fixed Prices for all items listed.

4.5.3.3.2.2 Offer prices include all costs for items supplied, delivered, and supported.

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

4.5.3.3.2.4 The grand total is accurate.

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

4.5.3.3.2.6 The Offeror has quoted in its own national currency or in the Host Nation currency, Euros. Where multiple currencies including other NATO member states' currencies are quoted, the conditions of Section III, are met.

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

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

4.5.3.3.2.9 The Price Offer meets requirements for price realism and balance as described below in Section 4.5.3.6.

4.5.3.4 An Offer 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.

4.5.3.5 Basis of Price Comparison

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

4.5.3.5.2 The Evaluated Price Offer to be inserted into the formula specified at Section 4.5.3.8 will be derived from the Grand Total of the Schedule of Supplies and Services (SSS) calculated as follows:

- The Sum of the Firm - Fixed Prices offered for CLINS 1 through ~~10~~ 12, as detailed below:

CLIN	Description
1	Project Management
2	Design
3	Equipment
4	Software / Licenses
5	Installation, integration and testing
6	Training
7	Warranty
8	Base Year 1
9	Base Year 2
10	Base Year 3
11	Option Year 1
12	Option Year 2

4.5.3.6 Price Balance and Realism

4.5.3.6.1 In the event that the successful Offeror has submitted a price Offer that is less than two thirds of the average of the remaining compliant Offers, the Purchaser must ensure that the successful Offeror has not artificially reduced the offered price to assure contract award. As such, the Purchaser will request the firm to provide clarification of the Offer and will inform the national delegation of the firm. In this regard, the Offeror shall provide an explanation to both Purchaser and their national delegation on the basis of one of the following reasons:

4.5.3.6.1.1 An error was made in the preparation of the price Offer. The Offeror must document the nature of the error and show background documentation regarding the preparation of the price Offer that convincingly demonstrates that an error was made by the Offeror. In such a case the Offeror may request to remain in the competition and accept the contract at the offered price, or to withdraw from the competition;

4.5.3.6.1.2 The Offeror has a competitive advantage due to prior experience or internal business/technological processes that demonstrably reduce cost to the Offeror

resulting in an offered price that is realistic. The Offeror's explanation must support the Technical Offer and convincingly and objectively describe the competitive advantage of and savings achieved by the advantage over the standard marked costs, practices and technology;

4.5.3.6.1.3 The Offeror understands that the submitted Price Offer is unrealistically low in comparison with the level of effort required. In this case, the Offeror is required to estimate the potential loss and show that the financial resources of the Offeror are adequate to withstand such a reduction in revenue.

4.5.3.6.1.4 If an Offeror fails to submit a comprehensive and convincing explanation for one of the based above, the Purchaser shall declare the Offer non-compliant and the Offeror will be notified accordingly.

4.5.3.6.1.5 If the Purchaser accepts the Offerors explanation of a mistake and allows the Offeror to accept the contract at the offered price or the explanation regarding competitive advantage in convincing, the Offeror shall agree that the supporting pricing data submitted with this Offer will be the basis to determine fair and reasonable pricing for all subsequent negotiations for modifications or additions to the contract and that no revisions of proposed prices will be made.

4.5.3.7 In the case of incrementally funded projects, the cost and pricing methodology used by the winning Offeror on the contract will be used as the basis for all follow-on contracts or amendments to the contract.

4.5.3.8 Determination of the Price Score. Once the administrative report has been approved by the Contract Awards Committee and all issues of compliance completed, the Price Offers will be opened and evaluated. The Price Score shall be determined according to the following formula:

PS = 100*(1-(Offer Evaluated Price / (2 x Average Offer Evaluated Price))

where: Offer Evaluated Price and Average Offer Evaluated Price will be the investment cost (CLINs 1 – 12) or the Present Value of the system life-cycle cost.

4.6 SPRINT 3

4.6.1 This procurement will have three (3) separate down selection activities conducted at the end of Sprints 1, 2 and 3. Sprint 3 will be based on the evaluation of Offerors Technical Solution package and its corresponding Price Offer package. Both Technical and Price packages will be based on information discussed during Sprint 3 detailed collaboration workshops held with all two (2) Offerors selected in the prior Sprint 2. At the end of Sprint 3, and as a result of its best value evaluation, a service provided will be selected. The unsuccessful Offeror will be notified of the results in due time. Offerors will refer to section 3.2 for packaging and marking requirements. Additionally, Offerors will refer to Section 3.5.2 and 3.5.3 for details on Technical Solution and Price Offer package requirements.

4.6.2 Technical Package Evaluation

4.6.2.1 The Technical Offer will be evaluated against the criteria and sub criteria set forth in this section. For some sub-criteria, there may be additional supporting factors at the next lower level. These lower level factors are not published here but are predetermined and included in the Technical Evaluation Weighting Scheme. This evaluation will be conducted throughout the Technical Report which consists of five (5) volumes: Executive Summary, Service Objectives Compliance, Service Implementation, Risk, and Performance Work Statement. Within each of the five (5) volumes of the Technical Proposal the criteria and their sub criteria are identified as follows:

4.6.2.1.1 Criteria - The Offeror shall provide a completed Cross-Reference Table in accordance with section 3.5.2.7. Failure to submit the completed Cross-Reference Table will be deemed non-compliant.

4.6.2.2 Volume 1 – Executive Summary

4.6.2.2.1 Criteria - The Offeror shall provide an executive summary. Failure to submit an executive summary will be deemed non-compliant.

4.6.2.3 Volume 2 and Volume 5 – Service Objectives Compliance

4.6.2.3.1 Criteria - The Offeror shall provide the proposed PWS in accordance with paragraph 3.5.2.13.1. Failure to submit the proposed PWS will be deemed non-compliant.

4.6.2.3.2 Criteria - The Offeror shall provide a PWS compliance statement in accordance with paragraph 3.5.2.13.2 Failure to submit the PWS compliance statement will be deemed non-compliant.

4.6.2.3.3 Criteria - The Offeror shall provide a completed Service Objectives Compliance Table in accordance with section 3.5.2.10.6. Failure to submit the completed Service Objectives Compliance Table will be deemed non-compliant.

4.6.2.3.4 In addition to the criteria in paragraphs 4.6.2.3.1 and 4.6.2.3.2 and 4.6.2.3.3, the offer will be evaluated against the criteria in section 4.6.2.3.5.

4.6.2.3.5 Criteria – Service Objectives Compliance (60% of the Technical Proposal, to assess the initial technical solution design and integration proposal, the service

delivery approach, the draft performance requirements summary and the objectives compliance)

4.6.2.3.5.1 Third-level sub criteria in the following order of importance:

a) Service Delivery in the following order of importance:

1. Demonstration of the suitability of the proposed PWS to meet the service goal, expected outcome and objectives
2. Compliance of the proposed PWS with the PWS template
3. Overall quality of the PWS

b) Technical Solution Design and Integration in the following order of importance:

1. Demonstration of the suitability of the Technical Solution Design and Integration description to meet the goal, expected outcome and service objectives of the Enterprise ACPV project.
2. Overall quality of the System Design and Integration description

4.6.2.4 Volume 3 – Service Implementation

4.6.2.4.1 Criteria – Service Implementation Schedule (20% of the Technical Proposal, to assess the service implementation approach, the implementation schedule and the testing, verification and validation approach)

4.6.2.4.1.1 Third-level sub criteria in the following order of importance:

a) Project Master Schedule (PMS) in the following order of importance:

1. Operational launch of the service milestone. The Date Score (DS) for the evaluation of the operational launch of the service milestone shall be determined according to the following formula:

DS = 100 * [1 – (OLS / (2* Average OLS))]

where OLS is the period, measured in days, between the Effective Date of the Contract (EDC) and the date of the operational launch of the service, according to the following formula:

OLS = Date of Operational Launch of the Service – EDC.

2. Demonstration of the suitability of the draft PMS to meet the goal, expected outcome and service objectives of the Enterprise ACPV service according to the agreed schedule, cost and scope.
3. Compliance of the proposed draft PMS with the PWS requirements
4. Overall quality of the draft PMS

b) Testing, verification and validation plan in the following order of importance:

1. Demonstration of the suitability of the initial testing verification and validation plan to meet the goal, expected outcome and service objectives of the Enterprise ACPV project in the shortest possible time.
2. Compliance of the initial testing verification and validation plan with the PWS requirements

3. Overall quality of the initial testing verification and validation plan

c) Service Implementation Project Management Plan (PMP) in the following order of importance:

1. Demonstration of the suitability of the initial service implementation plan to meet the goal, expected outcome and service objectives of the Enterprise ACPV project according to the agreed schedule, cost and scope.
2. Compliance of the initial service implementation plan with the PWS requirements.
3. Overall quality of the initial service implementation PMP

d) Security Accreditation Plan in the following order of importance:

1. Demonstration of the suitability of the initial Security Accreditation plan to meet the goal, expected outcome and service objectives of the Enterprise ACPV project according to the agreed schedule, cost and scope.
2. Compliance of the initial Security Accreditation plan with the PWS requirements.
3. Overall quality of the initial Security Accreditation plan

e) Quality Assurance and Quality Control Plan in the following order of importance:

1. Demonstration of the suitability of the initial Quality Assurance and Quality Control Plan to meet the goal, expected outcome and service objectives of the Enterprise ACPV project according to the agreed schedule, cost and scope.
2. Compliance of the initial Quality Assurance and Quality Control Plan with the PWS requirements.
3. Overall quality of the initial Quality Assurance and Quality Control Plan

f) Documentation Pack in the following order of importance:

1. Demonstration of the suitability of the Documentation Pack to meet the goal, expected outcome and service objectives of the Enterprise ACPV project according to the agreed schedule, cost and scope.
2. Compliance of the Documentation Pack with the PWS requirements.
3. Overall quality of the Documentation Pack description

g) Training plan in the following order of importance:

1. Demonstration of the suitability of the initial Training Plan to meet the goal, expected outcome and service objectives of the Enterprise ACPV project according to the agreed schedule, cost and scope.
2. Compliance of the initial Training Plan with the PWS requirements.
3. Overall quality of the initial Training Plan

4.6.2.5 Volume 4 – Risk

4.6.2.5.1 Criteria – Risk (20% of the Technical Proposal, to assess project risk, service

compliance risks, corporate experience and availability of the proposed service solution)

4.6.2.5.1.1 Third-level sub criteria in the following order of importance:

a) Initial project risk management analysis in the following order of importance:

1. Assessment of the risk level in the initial project risk management analysis.
2. Compliance of the proposed risk management analysis with the PWS requirements
3. Overall quality of the initial risk management analysis.

b) PMS credibility

c) Corporate experience and individual skills in the following order of importance:

1. Demonstration of the suitability of the corporate experience and individual skills description to meet the goal, expected outcome and service objectives of the Enterprise ACPV service according to the agreed schedule, cost, scope and performance targets.
2. Compliance of the corporate experience and individual skills description with the instructions in 3.4.2.11.5.
3. Suitability of the subcontracting approach
4. Overall quality of the Corporate experience and individual skills description

d) Availability of the proposed service solution

e) Assessment of service compliance risk

f) Suitability of the proposed solution for NATO

4.6.3 Price Offer Evaluation

4.6.3.1 Price will not be evaluated during the initial down selection activity, Sprint 1.

4.6.3.2 Price evaluation will take place twice throughout the dynamic sourcing process:

- During Sprint 2, the high-level pricing sheets submitted in the RFS package will be evaluated against the price criteria listed hereinafter.

- During Sprint 3, the detailed pricing sheets submitted to the shortlisted Offerors will be evaluated against the same price criteria, listed hereinafter.

NOTE 1: The granularity level of the two pricing sheets will vary.

NOTE 2: Specific criteria will only be applicable for Sprints 2 and 3 pricing sheets assessment (identified in the list below).

4.6.3.3 The Offeror's Price Offer will be first assessed for compliance against the following criteria:

4.6.3.3.1 The Price Offer meets the requirements set forth in the Offer Preparation Section and the Instructions for Preparation of the Pricing Sheets in ANNEX A-2.

4.6.3.3.2 Adequacy, accuracy, traceability and completeness of detailed pricing information.

4.6.3.3.2.1 The Offeror has furnished Firm Fixed Prices for all items listed.

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

4.6.3.3.2.3 Offer prices include all costs for items supplied, delivered, and supported.

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

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

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

4.6.3.3.2.7 The grand total is accurate.

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

4.6.3.3.2.9 The Offeror has quoted in its own national currency or in the Host Nation currency, Euros. Where multiple currencies including other NATO member states' currencies are quoted, the conditions of Section III, are met.

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

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

4.6.3.3.2.12 Detailed pricing information has been provided and is adequate, accurate, traceable, and complete; and

4.6.3.3.2.13 The Price Offer meets requirements for price realism and balance as described below in Section 4.6.3.6.

4.6.3.4 An Offer 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.

4.6.3.5 Basis of Price Comparison

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

4.6.3.5.2 The Evaluated Price Offer to be inserted into the formula specified at Section 4.6.3.8 will be derived from the Grand Total of the Schedule of Supplies and Services (SSS) calculated as follows:

- The Sum of the Firm - Fixed Prices offered for CLINS 1 through ~~10~~ 12, as detailed below:

CLIN	Description
1	Project Management
2	Design
3	Equipment
4	Software / Licenses
5	Installation, integration and testing
6	Training
7	Warranty
8	Base Year 1
9	Base Year 2
10	Base Year 3
11	Option Year 1
12	Option Year 2

4.6.3.6 Price Balance and Realism

4.6.3.6.1 In the event that the successful Offeror has submitted a price Offer that is less than two thirds of the average of the remaining compliant Offers, the Purchaser must ensure that the successful Offeror has not artificially reduced the offered price to assure contract award. As such, the Purchaser will request the firm to provide clarification of the Offer and will inform the national delegation of the firm. In this regard, the Offeror shall provide an explanation to both Purchaser and their national delegation on the basis of one of the following reasons:

4.6.3.6.1.1 An error was made in the preparation of the price Offer. The Offeror must document the nature of the error and show background documentation regarding the preparation of the price Offer that convincingly demonstrates that an error was made by the Offeror. In such a case the Offeror may request to remain in the competition and accept the contract at the offered price, or to withdraw from the competition;

4.6.3.6.1.2 The Offeror has a competitive advantage due to prior experience or internal business/technological processes that demonstrably reduce cost to the Offeror resulting in an offered price that is realistic. The Offeror's explanation must support the Technical Offer and convincingly and objectively describe the competitive advantage of and savings achieved by the advantage over the standard marked costs, practices and technology;

4.6.3.6.1.3 The Offeror understands that the submitted Price Offer is unrealistically low in comparison with the level of effort required. In this case, the Offeror is required to estimate the potential loss and show that the financial resources of the Offeror are adequate to withstand such a reduction in revenue.

4.6.3.6.1.4 If an Offeror fails to submit a comprehensive and convincing explanation for one of the based above, the Purchaser shall declare the Offer non-compliant and the Offeror will be notified accordingly.

4.6.3.6.1.5 If the Purchaser accepts the Offerors explanation of a mistake and allows the Offeror to accept the contract at the offered price or the explanation regarding competitive advantage in convincing, the Offeror shall agree that the supporting pricing data submitted with this Offer will be the basis to determine fair and

reasonable pricing for all subsequent negotiations for modifications or additions to the contract and that no revisions of proposed prices will be made.

4.6.3.7 In the case of incrementally funded projects, the cost and pricing methodology used by the winning Offeror on the contract will be used as the basis for all follow-on contracts or amendments to the contract.

4.6.3.8 Determination of the Price Score. Once the administrative report has been approved by the Contract Awards Committee and all issues of compliance completed, the Price Offers will be opened and evaluated. The Price Score shall be determined according to the following formula:

PS = 100*(1-(Offer Evaluated Price / (2 x Average Offer Evaluated Price))

where: Offer Evaluated Price and Average Offer Evaluated Price will be the investment cost (CLINs 1 – 12) or the Present Value of the system life-cycle cost.

4.7 CALCULATION OF BEST VALUE SCORES (SPRINTS 2 & 3)

4.7.1 Upon conclusion and approval of the Price Evaluation results at the end of both Sprints 2 and 3, the Offers will be calculated in order to obtain the Best Value Score of each Offer.

4.7.2 The highest scored Offer will be recommended as the Successful Offer.

4.7.3 A statistical tie is deemed to exist when the final scores of the highest scoring Offers are within one point of each other. The Purchaser will then resolve the statistical tie by awarding the contract to the Offer with the highest weighed technical score.

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

NATO Communications and Information Academy

NCI AGENCY

BOOK I – ANNEX A

PRICING SHEETS

ANNEX A-1

Pricing Sheets

See separate Excel Workbook attached
"RFS-CO-115699-ACPV_Book1_Annex_A_PricingSheets"

Pricing Sheets

On behalf of the firm stated below I hereby offer the Purchaser the services and deliverables (collectively referred as "ITEMS") set forth in the attached schedules[1], at the specified prices, and subject to the terms and conditions stated in RFS-CO-115699-ACPV.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Offer Reference _____

[1] Offerors shall submit in electronic form the cover page and an electronic copy of the worksheets contained in the file "2-RFS-CO-115699- ACPV_Book1_AnnexA_PricingSheets.xls" that was submitted to them as part of the RFS package.

ANNEX A-2

Instructions for the Preparation of Pricing Sheets

1. INTRODUCTION

Offer pricing requirements as addressed in this Annex are mandatory. Failure to abide to the prescriptions of offer submission referred in this section may lead to the offer being declared non-compliant and not being taken into consideration for award.

No alteration of the pricing sheets including but not limited to quantity indications, descriptions or titles are allowed with the sole exception of those explicitly indicated as allowed in this document. Additional price columns may be added if multiple currencies are offer, including extra provisions for all totals. Offerors may use one pricing sheet per currency if quoting in multiple currencies.

2. GENERAL REQUIREMENTS (SPRINTS 2 & 3)

Offerors shall follow the specific instructions provided in each worksheet. Instructions will be specific to the Sprint (Sprint 2 pricing sheets are high level whereas Sprint 3 pricing sheets include CLIN Summary and detailed tabs).

Offerors shall insert information in all yellow cells.

The prices and quantities entered on the document shall reflect the total items required to meet the Contractual requirements. The total price shall be indicated in the appropriate columns.

In preparing the Pricing Sheets, Offerors shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part.

Offerors are advised that formulae designed to ease evaluation of the offer have been inserted in the electronic copies of the Pricing Sheets. Notwithstanding this, the Offeror remains responsible for ensuring that their figures are correctly calculated and should not rely on the accuracy of the formulae in the electronic copies of the Pricing Sheets.

If the Offeror identifies an error in the spreadsheet, it should notify the Purchaser who will make a correction and notify all the Offerors of the update.

Any discounted or reduced prices offered by the Offeror must be traceable to a CLIN or CLINs at the lowest level.

During price evaluation, prices and detail of the traceability of application of the discount shall be clearly identified in the supporting detail sheets and applied at the unit price level.

3. STRUCTURE OF PRICING SHEETS

The Pricing Sheets provided in MS Office Excel format are organised according to the following structure and depending on the Sprint:

Sprint 2 pricing sheets:

- **Section 1. Offer Summary Sheets**

Sprint 3 pricing sheets:

- **Section 1. Offer Summary Sheets**
- **Section 2. CLIN Summary sheet**
- **Section 3. Detailed Pricing sheets for**
    - **Labour, Material, Travel, ODC and Rates**

4. COMPLETING PRICING SHEETS (Offer Summary Sheets)

Instructions are maintained throughout the pricing sheets to support the completion. Please refer to the green instruction boxes in the specific pricing sheets tab.

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK I – ANNEX B

Prescribed Administrative Forms and Certificates

ANNEX B-1

CERTIFICATE OF LEGAL NAME OF OFFEROR

This Offer 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 OFFER:

NAME: _____
POSITION: _____
TELEPHONE: _____

ALTERNATIVE POINT OF CONTACT:

NAME: _____
POSITION: _____
TELEPHONE: _____

Signature of authorised Representative: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-2

CERTIFICATE OF EXCLUSION OF TAXES, DUTIES AND CHARGES

I hereby certify that the prices offered for Request for Solution CO-115699-ACPV exclude all taxes, duties and customs charges from which the Purchaser has been exempted by international agreement.

Signature of authorised Representative:_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-3

COMPREHENSION AND ACCEPTANCE OF CONTRACT SPECIAL AND GENERAL PROVISIONS

The Offeror hereby certifies that he has reviewed the Term and Conditions set forth in the Prospective Contract, Book II of this Request for Solution. The Offeror hereby provides its confirmation that he fully comprehends the rights, obligations and responsibilities of the Contractor as set forth in the Articles and Clauses of the Prospective Contract. The Offeror additionally certifies that the offer submitted by the Offeror is without prejudice, qualification or exception to any of the Terms and Conditions and he will accept and abide by the stated Articles if awarded the Contract as a result of this Request for Solution.

The Offeror also agrees that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and service(s) shall be specified in accordance with the Performance Work Statement (PWS) and shall comply with all references and annexes.

Signature of authorised Representative: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-4

DISCLOSURE OF REQUIREMENTS FOR NCI AGENCY EXECUTION OF SUPPLEMENTAL AGREEMENTS

I, the undersigned, as an authorised representative of _____, certify the following statement:

All supplemental agreements, defined as agreements, documents and/or permissions outside the body of the Contract but are expected to be required by my Government, and the governments of my subContractors, to be executed by the NCI Agency, or its legal successors, as a condition of my firm's performance of the Contract, have been identified, as part of the Offer.

These supplemental agreements are listed as follows:

Examples of the terms and conditions of these agreements have been provided in our Offer. 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. 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.

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).

We recognise that additional supplemental agreements, documents and permissions presented as a condition of Contract performance or MOU signature after our firm would be selected as the successful Offeror may be cause for the NCI Agency, or its legal successors, to determine the submitted Offer to be non-compliant with the requirements of the RFS;

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.

Signature of authorised Representative: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-5

CERTIFICATE OF COMPLIANCE AQAP 2110 OR ISO 9001:2015 OR EQUIVALENT

I hereby certify that _____ (name of Company) possesses and applies Quality Assurance Procedures/Plans that are equivalent to the AQAP 2110 or ISO 9001:2015 as evidenced through the attached documentation[2].

Signature of authorised Representative: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

[2] Offerors must attach copies of any relevant quality certification.

ANNEX B-6

LIST OF PROSPECTIVE SUBCONTRACTORS/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

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-7

OFFEROR BACKGROUND IPR

I, the undersigned, as an authorised representative of Offeror _____, warrant, represent, and undertake that:

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

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

ITEM	DESCRIPTION

C. The Background IPR stated above complies with the terms specified in Clause 10 of the Prospective Contract and shall be licensed to the Purchaser according to the terms and conditions specified in the prospective Contract, and more particularly, in accordance with Clause 10 of the Terms and Conditions.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Offer Reference _____

ANNEX B-8

LIST OF SUBCONTRACTORS IPR

I, the undersigned, as an authorised representative of Offeror _____, warrant, represent, and undertake that:

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

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

ITEM	DESCRIPTION

C. The SubContractor IPR stated above complies with the terms specified in Clause 10 of the Prospective Contract and shall be licensed to the Purchaser according to the terms and conditions specified in the prospective Contract, and more particularly, in accordance with Clause 10 of the Terms and Conditions.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Offer Reference _____

ANNEX B-9

CERTIFICATE OF ORIGIN OF EQUIPMENT, SERVICES, AND INTELLECTUAL PROPERTY

The Offeror hereby certifies that, if awarded the Contract pursuant to this solicitation, he 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 provisioned 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 Offeror to firms, individuals or Governments other than within the NATO member countries.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Offer Reference _____

ANNEX B-10

LIST OF PROPOSED KEY PERSONNEL

POSITION	NAME	DESIGNATION PERIOD
Project Manager		EDC thru Contract expiration date
System Engineer (Technical Lead)		EDC thru Contract expiration date
Test Director / Test Engineer		EDC thru Contract expiration date
Quality Assurance Manager		EDC thru Contract expiration date
Service Delivery Manager		EDC thru Contract expiration date
Contract Manager		EDC thru Contract expiration date
Other (tbd by Offeror):		EDC thru Contract expiration date

The Offeror hereby certifies that all personnel meet or exceed the security requirements indicated in Book I, Section 1.3 and Book II Part II Terms and Conditions, Article 8 of this solicitation.

Signature of authorised Representative:_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-11

DISCLOSURE OF INVOLVEMENT OF FORMER NCI AGENCY EMPLOYMENT

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

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

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

☐ 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 Annex B of the prospective Contract Provisions):

Employee Name	Former NCI Agency Position	Current Company Position

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

Date : .....

Signature : .....

Name & Title : .....

Company : .....

Offer Reference : .....

ANNEX B-12

COMPREHENSION AND INTENTION TO COMPLY WITH EXCLUSION CLAUSE AND CONFLICT OF INTEREST

A. I, the undersigned, as an authorised representative of the firm submitting this Offer, do hereby certify that the _____ (FIRM NAME) and its sub Contractors have not participated in support of RFTOP MAS 2020-01 Cyber Evaluation and Adaptation, CO-115695-DYNS Dynamic Sourcing Process Augmentation Support, CO-115696-PROG Programmatic and Technical Augmentation Support and are eligible for Contract award.

B. The NCI Agency shall not consider mitigation plans regarding this exclusion.

C. This exclusion clause does not apply to parent companies of the Contractor and their wholly owned subsidiaries provided that the parent company or its subsidiaries provides proof to the satisfaction of the Purchaser that they operate as a separate legal entity in a completely distinguishable and different business domain. Proof as mentioned above may consist of:

   i. company's structure
   ii. roles and responsibilities within structure
   iii. business domain
   iv. ownership and control
   v. and any other proof that will fulfil the purpose of the exclusion clause

D. The Contractor shall insert the substance of this clause in all subContracts for work performed under this Contract. It is the responsibility of the Contractor to ensure that their subContractor(s) are made aware of this exclusion clause prior to the subContractor(s) commencing performance under this Contract.

E. The Contractor agrees that compliance with this exclusion clause is of the essence and that failure to abide to these terms shall constitute sufficient grounds for the Termination for Default of the Contract in accordance with Clause 37 of the Terms and Conditions.

Signature of authorised Representative: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

ANNEX B-13

CERTIFICATE OF ISO 27001:2022 COMPLIANCE

I hereby certify that …… *(Company Name)* is fully compliant with the ISO 27001:2022 Information Security Management and is currently so certified.

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

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

ANNEX B-14

SECURITY ASPECTS LETTER (SAL)

1. In the performance of this contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the work is performed or in the contracts involving NR information only as established in the contract's Statement of Objectives (SOO) section labelled, "Safeguarding of NATO Restricted Information".
2. All classified information and material shall be protected in accordance with the requirements established by the NSA/DSA of the nation in which the work is performed or in the case of NR information as may also be established in the Safeguarding of NATO Restricted Information Clause.
3. In particular, the Contractor shall:
    a. appoint an officer to be responsible for supervising and directing security measures in relation to the Request for Solution (RFS), contract or sub-contract;
    b. submit in due time to the NSA/DSA the personal particulars of the person the contractor wishes to employ on the project with a view to obtaining PSCs at the required level where NC and above is involved;
    c. maintain, preferably through this officer responsible for security measures, a continuing relationship with the NSA/DSA and / or the Contracting Authority in order to ensure that all NATO classified information involved in the offer, contract or sub-contract is properly safeguarded;
    d. limit the copying of any classified materiel (including documents) to the absolute minimum to perform the contract;
    e. supply the NSA/DSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information;
    f. maintain a record of his employees taking part in the project and who have been cleared for access to NATO classified information. This record must show the period of validity and the level of the clearances;
    g. deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DSA or in the case of NR information as determined by the need-to-know;
    h. limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub-contract;
    i. comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information, and that they recognise that they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

j. report to the Security Officer and to his NSA/DSA any breaches or suspected breaches of security, suspected sabotage or subversive activity, any breach giving rise to doubts as to the trustworthiness of an employee, any changes in the ownership, supervisory or managerial staff of the facility or any changes that affect the security arrangements and security status of the facility, and any other information which may be required by the NSA/DSA, such as reports on holdings of NATO classified information or materiel;

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

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

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

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

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

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

q. No CIS may be used for processing classified information without prior accreditation by the responsible authorities. At the level of NR, such accreditation can be under delegated authority of the responsible accreditation authority or the contracting authority in accordance with contract's Statement of Objectives (SOO) section labelled, "Safeguarding of NATO Restricted Information".

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

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

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

u. The Contractor shall be required to acknowledge receipt of an accompanying SAL or Program Security Instruction (PSI) that is made part of the applicable contract and confirm that it understands the security aspects defined. With respect to contracts involving only NR information the Contractor shall also be required to confirm that it will comply with the provisions of the Safeguarding of NATO Restricted Information clause provided in Book II, Special Provisions and specifically that any company CIS used to handle or process NR classified information has been appropriately security accredited.

Comprehension and Acceptance of the Security Aspect Letter (SAL)

The Offeror hereby acknowledges receipt of the SAL letter in relation to the NATO Restricted Information provided under solicitation reference number RFS-CO-115699-ACPV and certifies:

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

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

…….. ……..

Date Signature of Authorised Representative

……..

Printed Name and Title

……..

Company

ANNEX B-15

Project Security Instructions (PSIs) – Structure and Content

The following is provided as guidance for the structure and content of Project Security

Section	Content
1 Document Control	• The issue number; • the date of issue; • the reference and details of the latest Change Proposal; • any related Contract Amendment; • index of amendments; • PSIs index of contents.
2 Introduction / Definitions	• The purpose of the PSIs; • the authority of the PSIs (for example, Project Security Group); • definitions of frequently used terms in NATO contracts involving classified information.
3 National/NATO/ Industry Officials	• The contact details (name, address, telephone / fax number, e-mail address) for the national / NATO officials involved in the project/programme, who are responsible for the following: - administration and policy; - technical security; - CIS Security. Note: This may be included as an Annex to the PSIs.
4 Security Instructions	• General aspects relating to the exchange of NATO classified information and the responsibilities of the NSAs/DSAs; • definition of the security classifications and markings appropriate to the project/programme; • explanation of terms - classified information, material and documents. • storage and transmission of NATO classified information; • disposal / destruction of NATO classified information; • breaches of security; instructions relating to the loss, compromise or possible compromise of NATO classified information; • instructions relating to the unauthorised release of NATO information.
5 Release of Information	Definitions of terms, for example, public release, marketing release, sales release, project information, participants, authorities, and approval; • a release statement, for example, “the release of project information (classified or non-classified) to authorities or persons outside of the project (non-participants) without prior approval is strictly prohibited”. • release of project information:

	- general information - NATO/National policies, required Facility Security Clearances, contractual requirements, security agreements for marketing activities; - release of project information to non-participating bodies; - release in connection with sub-contracting; - public release - general instructions, management of public releases; - sales releases - general instructions, management of sales releases; - marketing releases - general instructions, management of marketing releases; • formats for request for release of project information to nonparticipants, for use at symposia, seminars, etc., and for public release.
6 Change Procedures	• Procedures for changes to security instructions, including the PSIs; • procedures for changes to the Security Classification Guide; • the use of interim procedures.
7 International Hand Carriage of NATO Classified Documents	• Classification of documents for hand carriage; • conditions when hand carriage of documents is permitted; • courier certificate; • responsibilities of Security Offices in the NPA/NPO, Government bodies and industry - administrative procedures, packaging; • responsibilities of the courier; • instructions in the event of loss of documents; • format for “document transmission notification”; • format for “instructions to persons who are authorised to hand-carry NATO classified documents”; • format for “instructions to prevent customs examination”.
8 International Visit Control Procedures	• General instructions for international visits; • procedures for one-time and recurring visits, including use of the standard “Request for Visit” format, and lead times; • procedures for emergency visits; • instructions for the use and completion of the standard “Request for Visit” format; • list of authorities concerned with International Visit Control Procedures (Note: This may be included as an Annex to the PSIs).
9 Sub-Contracting	• Definitions of terms, for example, negotiations, Contractor, Sub-contractor, classified contract, and facility security clearance; • security instructions relating to the negotiation of a NATO classified contract; • permission to negotiate contracts; • security classification of contracts.

10 International Transportation	• Security procedures relating to the international transportation of NATO classified material. • Transportation Plan to be established if required.
11 Communication and Information Systems (CIS)	• Security procedures for the accreditation and use of CIS (or reference to a specific document dealing with projectrelated CIS).
12 Security Classification Guide	A document which outlines classifications applicable to the programme/project as allocated and approved by the participants (background and/or foreground information, procedures for downgrading and declassification, caveats).

Comprehension and Acceptance of the Program Security Instructions (PSIs)

The Offeror hereby acknowledges receipt of the PSIs in relation to the NATO Restricted Information provided under solicitation reference number RFS-CO-115699-ACPV and certifies:

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

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

…….

Date

…….

Signature of Authorised Representative

…….

Printed Name and Title

…….

Company

ANNEX B-16

Company Compliance with Safeguarding NATO Information Controls Self-Attestation Statement

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

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

I can supply supporting evidence, upon request by the Contracting Officer, by means of a completed System Security Plan[3] (or extract thereof) and any associated plans of actions developed to describe the Contractor's CIS where NATO Information associated with the execution and performance of this contract is processed, stored, developed, or transmitted.

……. ……

Date Signature of Authorised Representative

……

Printed Name and Title

……

Company

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

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK I – ANNEX C

PRE-QUALIFICATION QUESTIONNAIRE (PQQ)

ANNEX C-1

See separate Excel Workbook attached
"RFS-CO-115699-ACPV_Book1_Annex_C_Pre-Qualification_Questionnaire"

Evaluation Criteria	Weighting Factor	Objective	Response
The tenderer must have been in operation for at least 5 years by the deadline for submission of offers	Medium	To meet this minimum (mandatory) requirement, the tender must provide a brief history of the company, including length of time in business, overall size and geographic locations (can be primary locations only)	
The tenderer must have over 5 years of business experience in the type of services and domains which are the subject of this procurement.	Medium	To meet this minimum (mandatory) requirements, the tenderer must demonstrate through a capability statement relevant experience in the following services/capabiltites: Asset Management lifecycle Configuration Management lifecycle Patching Management lifecycle Vulnerability Management lifecycle Business Intelligence and Data Analytics	
The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractal work for: - **Asset and configuration management services**	High	To meet this minimum (mandatory) requirements, the tenderer must demonstrate through a capability statement relevant experience in the following services/capabiltites: Asset Management lifecycle Configuration Management lifecycle Patching Management lifecycle Vulnerability Management lifecycle Business Intelligence and Data Analytics	
The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractal work for: **- Patch management services**	Medium	To meet this minimum (mandatory) requirements, the tenderer must demonstrate through a capability statement relevant experience in the following services/capabiltites: Asset Management lifecycle Configuration Management lifecycle Patching Management lifecycle Vulnerability Management lifecycle Business Intelligence and Data Analytics	
The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractal work for: **- Vulnerability management services**	High	To meet this minimum (mandatory) requirements, the tenderer must demonstrate through a capability statement relevant experience in the following services/capabiltites: Asset Management lifecycle Configuration Management lifecycle Patching Management lifecycle Vulnerability Management lifecycle Business Intelligence and Data Analytics	

Evaluation Criteria	Weighting Factor	Objective	Response
The tenderer must demonstrate relevant experience in the sourcing of services required under this procurement, by providing a minimum of one summary of successfully delivered past contractal work for: **- Business Intelligence/data analytics services**	High	To meet this minimum (mandatory) requirements, the tenderer must demonstrate through a capability statement relevant experience in the following services/capabiltites: Asset Management lifecycle Configuration Management lifecycle Patching Management lifecycle Vulnerability Management lifecycle Business Intelligence and Data Analytics	
At least 2 relevant experiences should be in a multi-national and/or multi-national military environment	Low	The tenderer must show at least two experiences in international or multi-national organizations or military organizations (NATO Nations only)	
The tenderer must demonstrate inclusion on the team of technical A, C P and V experts, meeting the minimum experience required of 5 years	High	The tenderer must note key personnel proposed for this opportunity in the areas of ACPV and BI/Data Analytics in the capability statement and their background, technical experience and level of expertise.	
The tendered shall specify proficient in an English language environment. French language proficiency is desirable, but not obligatory.	High	Delivery of work and communication with past clients was in English	
The tenderer must have the financial capacity to provide the required services. Specifically, the tenderer must have had an average annual revenue, after expenses, of at least 30MEUR	Medium	To meet this minimum requirement (mandatory), copies of the balance sheets and economic outturn (profit & loss) statements covering at least the last three years for which accounts have been closed where publication of them is required under the company law of the country in which the economic operator is established must be provided	
Legal Status – the tenderer must be able to contract from a NATO Nation	High		
The tender must not have had an active legal or contractal dispute proceedings with NATO or its Agencies in the past 5 years	Medium	To meet this minimum requirement (mandatory), a certificate of registration in the relevant trade or professional registers in the country of establishment/incorporation must be provided	
Security clearances – the tenderer must be able to demonstrate their ability to staff the opportunity with NATO security cleared personnel (demonstration of an appropriate pipeline) to deliver the required services.	Medium		
Security Accreditations – the tender must have current accreditations required to work with NATO (valid Designation of Eligibility received)	High		
Data Residency – the tenderer must certify data will only be shared/stored to NATO Nation.	Medium	To meet this minimum requirement (mandatory), the tenderer must provide proof of valid facility clearance and provide the number of security cleared personnel	

Evaluation Criteria	Weighting Factor	Objective	Response
The tenderer must demonstrate a teamed arrangement, if necessary. That is that NATO has a direct and only contract with the prime Service Providers. Subrelationships, through sub-contracting is however authorized as long as the industry teaming arrangement members are part of NATO Nations.	Medium	To meet this minimum requirement (mandatory), the tenderer must detail their approach for providing the service, which service providers will be part of the teaming arrangement (if any), and which parts of the service will be sub-contracted (if any)	
The tenderer must comply with the request to deliver Enterprise ACPV Service as a managed service	High	Failure to comply/commit to this requirement will lead the tenderers from being excluded of the subsequent phases	
The tenderer must have resource capacity in NATO Nations to deliver the required services.	Medium	To meet this minimum (mandatory) requirements, the tenderer must demonstrate pool of resources available in NATO nations	
The tenderer must have sufficient geographic coverage to provide service resiliency across NATO nations.	Low	To meet this minimum (mandatory) requirements, the tenderer will be assessed on the availability of skilled and cleared resources and their proximity to relevant NATO locations.	

ANNEX C-2

See separate Excel Workbook attached
"RFS-CO-115699-ACPV_Book1_Annex_C_Pre-Qualification_Questionnaire"

Number		YES / NO / PARTIALLY
1	Provide users with visibility of technical asset details and configuration from technology management systems	
2	Provide users with visibility of data and information about (privileged) identity and access management of technology assets	
3	Provide users with visibility of technical log data from technology assets	
4	Provide users with visibility of information about who manages the technology asset	
5	Provide users with information about who the risk owner(s) are for the asset	
6	Provide users with information about who the business owner(s) is for the asset	
7	Provide users with information about the function and importance of the technology asset	
8	Provide users with information about the security accreditation status of technology assets	
9	Provide users with information about the relationships between technology assets (logical and technical)	
10	Provide users with information about the network context of assets (e.g. exposure to internet, security classification, etc.)	
11	Provide users with vulnerability information about technology assets	
12	Provide users with data and information about vulnerability mitigating actions	
13	Provide users with data and information about anti-malware protection of assets	
14	Provide users with security exception information for technology assets	
15	Provide users with security incident information for technology assets	
16	Provide users with cyber threat information related to technology assets	
17	Document when the last security audit occurred	
18	Allow alarms or alerts to be created to remind of the need for a security audit	
19	Provide users with information on physical servers and virtual machines	
20	Provide users with information on OT / IoT / facility devices	
21	Provide users with information on network components (e.g. router, switches, firewalls, etc.)	
22	Provide users with information on IT services	
23	Provide users with information on (web) applications and middleware	
24	Provide users with information on software supply chain (e.g. software bill of materials)	
25	Provide users with information on databases	
26	Provide users with information on mobile and end user devices	
27	Provide users with information on cloud based services	
28	Integrate with the Tier 2 data sources (management systems) as described in the reference scenario in Book II-Part IV-Statement of Objectives and display their data through a centralized interface	
29	Handle and store classified information in accordance with NATO security policies	
30	Retain historical data for the duration that stakeholders require to meet their use cases	
31	Be able to actively perform asset discovery on networks to identify online technology assets	

32	Perform advanced data engineering and analytics in order to meet the use cases and requirements of stakeholders	
33	Join, aggregate and transform data from multiple data sources to create enriched datasets	
34	Provide support from data analysts that can develop data, analysis, transformation and visualizations based on the requirements from the end user.	
35	Produce advanced reports, dashboards, alerting or self-service portals to meet the use cases and requirements of stakeholders	
36	Other cyber capabilities are able to easily consult and access the information and produce advanced reports or dashboards themselves	
37	Keep the data and information on technology assets up-to-date and accurate	
38	Make use, where possible, of automation to keep the data and information up-to-date	
39	Perform data governance for the technology asset data in scope for the service	
40	Maintain a common data model and data dictionary based on the information requirements from stakeholders	
41	Assess and report on data quality and trustworthiness of the information it provides to other capabilities	
42	Users have access to the requested information in less than 1 hour from the time it is requested. The data covers at least 95% of the known assets, is no more than 24 hours old and is at least 95% correct.	
43	Support all the technology asset types described in the reference scenario in Book II-Part IV-Statement of Objectives	
44	The service shall be resilient and ensure business continuity and disaster recovery	
45	Technology solutions part of the service have geographic redundancy and off-site backups	
46	The service shall adhere to the NATO cyber security policies and requirements in accordance with the references provided in Book II-Part IV-Statement of Objectives	
47	The least privilege and need to know principles shall be adhered to by the service in order to protect sensitive information and data	
48	The service shall be delivered as a managed service in accordance with the ITIL service management framework.	
49	The contractor shall manage the software	
50	The contractor shall manage the middleware and databases	
51	The contractor shall manage the hosting infrastructure	
52	The contractor shall manage the information security of the solution	
53	The service shall have an availability of at least 99%	
54	The contractor shall provide requirement management services	
55	The contractor shall provide change management services	
56	The service shall be agile and meet changing reporting and information requirements from stakeholders	
57	The service shall provide the option to add new Tier 2 data sources	
58	The service shall allow to add new assets	
59	The service shall allow changes to the data model	
60	The service shall be described and delivered in accordance with the Performance Work Statement (PWS) Template in Book II-Part IV-Statement of Objectives-Annex A.	

61	The contractor shall design and document a NATO Enterprise framework that will eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on asset, configuration and patch management through a federated approach.	

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK I – ANNEX D

CLARIFICATION REQUEST FORM

ANNEX D
CLARIFICATION REQUEST FORM

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

ADMINISTRATION or CONTRACTING OFFICER					
Serial Nr	**RFS Book**	**RFS Section Ref.**	**QUESTION**	**ANSWER**	**Status**
A.1					
A.2					
A.3					

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK I – ANNEX E

CROSS-REFERENCE TABLE

ANNEX E-1
Cross-Reference Table
SPRINT 2

Offeror shall complete column “OFFEROR REFERENCE” with Offer references that locate the technical proposal documentation required by the RFS, e.g. section, paragraph, table (if applicable), page number etc. One copy each of the duly completed Cross Reference/Compliance Table is to be included in the RFS Technical Proposal package. The Offer shall follow the instructions in section 3.4, and will be evaluated according to the instructions in section 4.5.

See separate Excel Workbook attached
“RFS-CO-115699-ACPV_Book1_Annex_E-F_Cross-Ref_and_Svc_Objectives_Compliance”

RFSInstructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.4.2.6	N/A	The Offeror shall include the completed Cross-Reference Table at ANNEX E-1 accompanying their offers in Sprint 2 and capturing all 4 Volumes included therein.	4.5.2.1.1	
3.4.2.7	N/A	Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report	N/A	
3.4.2.8.1	N/A	Executive Summary	4.5.2.2	
3.4.2.9.3	N/A	Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report	4.5.2.3	
3.4.2.9.4	Table 1 and Table 2	Offerors shall explain their proposed technical solution, including an overview of their technical solution design and system integration requirements in order to meet in the objectives in Book II-Part IV-Statement of Objectives.	4.5.2.3	

RFSInstructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.4.2.9.5	Table 1 and Table 2	Offerors shall explain their service delivery and service management approach in order to meet the objectives in Book II Part IV Statement of Objectives.3.4.2.9.3	4.5.2.3	
3.4.2.9.6	Table 1 and Table 2	Offerors shall propose a draft Performance Requirements Summary in accordance with the PWS template found in Book II Part IV Statement of Objectives-Annex A	4.5.2.3	
3.4.2.9.6.1	Table 1 and Table 2	Offerors shall explicitly state that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and service(s) shall be specified in accordance with the PWS template found in Book II Part IV Statement of Objectives-Annex A and shall comply (if applicable to the service in question) with the requirements in the PWS (including all annexes/exhibits).	4.5.2.3	
3.4.2.9.7	Table 1 and Table 2	Completed Service Objectives Compliance Table found in Book I ANNEX F.	4.5.2.3	
3.4.2.10.3	N/A	Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report.	4.5.2.4	
3.4.2.10.4	Table 1 and Table 2	The Offeror shall indicate in broad detail the service implementation approach and how the implementation project will be executed and managed from contract signature through to Final Service Acceptance in order to meet the objectives in Book II Part IV Statement of Objectives.	4.5.2.4	
3.4.2.10.5	Table 1 and Table 2	Offerors shall provide a draft PMS with the key contract events and milestones for the service implementation project.	4.5.2.4	

RFSInstructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.4.2.10.6	Table 1 and Table 2	Offerors shall describe their proposed testing, verification and validation approach in order to meet the objectives in Book II Part IV Statement of Objectives.	4.5.2.4	
3.4.2.11.3	N/A	Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Report.	4.5.2.5	
3.4.2.11.4	Table 1 and Table 2	Offerors shall identify the key risks in their project and their proposed response actions.	4.5.2.5	
3.4.2.11.5	Table 1 and Table 2	Offerors shall provide a description of the corporate capabilities of the Offeror, including corporate experience, and individual skills and experience, both in service implementation and service delivery.	4.5.2.5	
3.4.2.11.6	Table 1 and Table 2	Offerors shall describe which parts of the proposed service solution are based on already existing and working services and which parts will require new ad-hoc integrations or developments.	4.5.2.5	

ANNEX E-2
Cross-Reference Table
SPRINT 3

Offeror shall complete column “OFFEROR REFERENCE” with Offer references that locate the technical proposal documentation required by the RFS, e.g. section, paragraph, table (if applicable), page number etc. One copy each of the duly completed Cross Reference/Compliance Table is to be included in the RFS Technical Proposal package. The Offer shall follow the instructions in section 3.5, and will be evaluated according to the instructions in section 4.6.

See separate Excel Workbook attached
“RFS-CO-115699-ACPV_Book1_Annex_E-F_Cross-Ref_and_Svc_Objectives_Compliance”

RFS Instructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.5.2.7	N/A	The Offeror shall include the completed Technical Package Cross-Reference Table at ANNEX E-2 accompanying their offers and capturing all Volumes included therein.	4.6.2.1.1	
3.5.2.8	N/A	Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Package.	N/A	
3.5.2.9.2	N/A	Executive Summary	4.6.2.2.1	
3.5.2.10.3	N/A	Offeror shall compile a detailed Table of Contents which lists not only section headings but also major sub-sections, and topic headings required set forth in these Instructions or implicit in the organisation of the Technical Package.	N/A	
3.5.2.10.4	Table 1 and Table 2	The Offeror shall describe how the Enterprise ACPV service will be implemented with sufficient technical detail for the Purchaser to determine compliance with the Statement of Objectives.	4.6.2.3	

RFS Instructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.5.2.10.5	Table 1 and Table 2	The Offeror shall describe how the Enterprise ACPV service will be implemented with sufficient technical detail for the Purchaser to determine compliance with the Statement of Objectives.	4.6.2.3	
3.5.2.10.6	Table 1 and Table 2	The Offeror shall complete the service objectives compliance table found in Book I Annex F.	4.6.2.3	
3.5.2.11.3	N/A	Offeror shall compile a detailed Table of Contents which lists section headings, major sub-sections, and topic headings required in these Instructions or implicit in the organisation of the Technical Package.	4.6.2.3	
3.5.2.11.4	Table 1 and Table 2	The Offeror shall provide the Project Overview which shall provide an executive summary overview of the service implementation project.	4.6.2.4	
3.5.2.11.5	Table 1 and Table 2	PMP will be defining how the Offeror intends to manage the service implementation project from contract signature through to Final Service Acceptance in order to meet the objectives in Book II Part IV Statement of Objectives.	4.6.2.4	
3.5.2.11.6	Table 1 and Table 2	PMS shall contain all contract events and milestones for the service implementation project.	4.6.2.4	
3.5.2.11.7	Table 1 and Table 2	The Offeror shall describe their proposed testing, verification and validation plan explaining how it can meet the testing requirements and its methodology for conducting all related activities in accordance with the PWS in Book II Part IV Statement of Objectives Annex A.	4.6.2.4	
3.5.2.11.8	Table 1 and Table 2	The Offeror shall describe their input to the security accreditation documentation in support of the accreditation process in accordance with the PWS in Book II Part IV Statement of Objectives Annex A.	4.6.2.4	

RFS Instructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.5.2.11.9	Table 1 and Table 2	The Offeror shall cover the Quality Assurance and Quality Control aspects of the Project in accordance with the PWS in Book II Part IV Statement of Objectives Annex A.	4.6.2.4	
3.5.2.11.10	Table 1 and Table 2	The Offeror shall describe their Documentation Pack and proposed Project Portal in accordance with the PWS in Book II Part IV Statement of Objectives Annex A.	4.6.2.4	
3.5.2.11.11	Table 1 and Table 2	The Offeror shall describe their training plan in accordance with the PWS in Book II Part IV Statement of Objectives Annex A.	4.6.2.5	
3.5.2.12.3	N/A	Offeror shall compile a detailed Table of Contents which lists not only section headings but also major sub-sections, and topic headings required set forth in these Instructions or implicit in the organisation of the Technical Package.	4.6.2.5	
3.5.2.12.4	Table 1 and Table 2	The Offeror shall describe in the initial RMP how it will implement the Risk Management process in accordance with the PWS in Book II Part IV Statement of Objectives Annex A.	4.6.2.5	
3.5.2.12.5	Table 1 and Table 2	The Offeror shall describe how the experience and expertise of the prime Contractor and all nominated sub-Contractors will contribute to the successful execution of the Contract.	4.6.2.5	
3.5.2.12.6	Table 1 and Table 2	Offerors shall describe which parts of the proposed service solution are based on already existing and working services and which parts will require new ad-hoc integrations or developments.	4.6.2.5	
3.5.2.13.1	Table 1 and Table 2	The Offeror shall provide the proposed Performance Work Statement (PWS) for the delivered product(s) and service(s) which shall be specified in accordance with the PWS template in Book II Part IV Statement of Objectives-Annex A, (including all annexes/exhibits).	4.6.2.3.1	

RFS Instructions Requirement Ref.	SOO Ref	REQUIREMENT DESCRIPTION	Evaluation Criterion Ref.	OFFER REFERENCE
3.5.2.13.2	Table 1 and Table 2	The Offeror shall explicitly state that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and service(s) shall comply with the requirements in the PWS (including all annexes).	4.6.2.3.2	

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK I – ANNEX F

SERVICE OBJECTIVES COMPLIANCE TABLE

ANNEX F

Service Objectives Compliance Table

See separate Excel Workbook attached
"RFS-CO-115699-ACPV_Book1_Annex_E-F_Cross-Ref_and_Svc_Objectives_Compliance"

Service Objective ID			Service Objective Description		YES / NO / PARTIALLY
1		Provide users with enterprise visibility on technology assets, their ownership, context within the organisation and their security status.			
	1.1		Provide users with visibility on technical information about technology assets		
		1.1.1		Provide users with visibility of technical asset details and configuration from technology management systems	
		1.1.2		Provide users with visibility of data and information about (privileged) identity and access management of technology assets	
		1.1.3		Provide users with visibility of technical log data from technology assets	
	1.2		Provide users with visibility on ownership information about technology assets		
		1.2.1		Provide users with visibility of information about who manages the technology asset	
		1.2.2		Provide users with information about who the risk owner(s) are for the asset	
		1.2.3		Provide users with information about who the business owner(s) is for the asset	
	1.3		Provide users with contextual information about technology assets		
		1.3.1		Provide users with information about the function and importance of the technology asset	
		1.3.2		Provide users with information about the security accreditation status of technology assets	
		1.3.3		Provide users with information about the relationships between technology assets (logical and technical)	
		1.3.4		Provide users with information about the network context of assets (e.g. exposure to internet, security classification, etc.)	
	1.4		Provide users with security information about technology assets		
		1.4.1		Provide users with security exception information for technology assets	
		1.4.2		Provide users with security incident information for technology assets	
		1.4.3		Provide users with cyber threat information related to technology assets	
		1.4.4		Document when the last security audit occurred	
		1.4.5		Allow alarms or alerts to be created to remind of the need for a security audit	
	1.5		Provide users with visibility in different technology asset types		
		1.5.1		Provide users with information on physical servers and virtual machines	
		1.5.2		Provide users with information on OT / IoT / facility devices	

		1.5.3		Provide users with information on network components (e.g. router, switches, firewalls, etc.)	
		1.5.4		Provide users with information on IT services	
		1.5.5		Provide users with information on (web) applications and middleware	
		1.5.6		Provide users with information on software supply chain (e.g. software bill of materials)	
		1.5.7		Provide users with information on databases	
		1.5.8		Provide users with information on mobile and end user devices	
		1.5.9		Provide users with information on cloud based services	
2		Integrate with the Tier 2 data sources (management systems) as described in the reference scenario in Book II-Part IV-Statement of Objectives and display their data through a centralized interface			
	2.1		Handle and store classified information in accordance with NATO security policies		
	2.2		Retain historical data for the duration that stakeholders require to meet their use cases		
3		Be able to actively perform asset discovery on networks to identify online technology assets			
4	4.1	Perform advanced data engineering and analytics in order to meet the use cases and requirements of stakeholders			
	4.2		Join, aggregate and transform data from multiple data sources to create enriched datasets		
	4.4		Provide support from data analysts that can develop data, analysis, transformation and visualizations based on the requirements from the end user.		
5		Produce advanced reports, dashboards, alerting or self-service portals to meet the use cases and requirements of stakeholders			
	5.1		Other cyber capabilities are able to easily consult and access the information and produce advanced reports or dashboards themselves		
6		Keep the data and information on technology assets up-to-date and accurate			
	6.1		Make use, where possible, of automation to keep the data and information up-to-date		
7		Perform data governance for the technology asset data in scope for the service			
	7.1		Maintain a common data model and data dictionary based on the information requirements from stakeholders		
8		Assess and report on data quality and trustworthiness of the information it provides to other capabilities			
9		Users have access to the requested information in less than 1 hour from the time it is requested. The data covers at least 95% of the known assets, is no more than 24 hours old and is at least 95% correct.			
10		Support all the technology asset types described in the reference scenario in Book II-Part IV-Statement of Objectives			
11		The service shall be resilient and ensure business continuity and disaster recovery			
	11.1		Technology solutions part of the service have geographic redundancy and off-site backups		
12		The service shall adhere to the NATO cyber security policies and requirements in accordance with the references provided in Book II-Part IV-Statement of Objectives			

	12.1		The least privilege and need to know principles shall be adhered to by the service in order to protect sensitive information and data		
13		The service shall be delivered as a managed service in accordance with the ITIL service management framework			
	13.1		The service shall be delivered in accordance with the ITIL service management framework. Contractors may apply other service management frameworks in addition to ITIL if they deem it necessary.		
	13.2		The contractor shall manage the technology solutions required to meet the functional objectives		
		13.2.1		The contractor shall manage the software	
		13.2.2		The contractor shall manage the middleware and databases	
		13.2.3		The contractor shall manage the hosting infrastructure	
		13.2.4		The contractor shall manage the information security of the solution	
	13.3		The service shall have an availability of at least 99%		
14		It shall be possible to make changes to the service			
	14.1		The contractor shall provide requirement management services		
	14.2		The contractor shall provide change management services		
	14.3		The service shall be agile and meet changing reporting and information requirements from stakeholders		
	14.4		The service shall provide the option to add new Tier 2 data sources		
	14.5		The service shall allow to add new assets		
	14.6		The service shall allow changes to the data model		
15		The service shall be described and delivered in accordance with the Performance Work Statement (PWS) Template in Book II-Part IV-Statement of Objectives-Annex A.			
16		The contractor shall design and document a NATO Enterprise framework that will eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on asset, configuration and patch management through a federated approach.			

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK II, PART I

SCHEDULE OF SUPPLIES AND SERVICES

Asset, Configuration, Patching, and Vulnerability Management (ACPV) Enterprise Service							
CLIN	**Description**	**PWS Reference**	**Delivery Destination**	**Unit of measure**	**Quantity**	**Notes**	**Delivery Schedule EDC +**
	BASE NON-RECURRING + BASE RECURRING SERVICES (YEARS 1, 2 AND 3)						
1	**Project Management (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
1.1							
1.2							
1.3							
2	**Design (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
2.1							
2.2							
2.3							
3	**Equipment (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
3.1							
3.2							
3.3							
4	**Software / Licenses (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
4.1							
4.2							
4.3							
5	**Installation, integration and testing (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
5.1							
5.2							
5.3							
6	**Training (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
6.1							
6.2							
6.3							
7	**Warranty (Non-recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
7.1							
7.2							
7.3							
8	**Year 1 Service (Recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
8.1							
8.2							
8.3							
9	**Year 2 Service (Recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
9.1							
9.2							
9.3							
10	**Year 3 Service (Recurring service)**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
10.1							
10.2							
10.3							
	OPTIONAL RECURRING SERVICES - EVALUATED						
11	**Option Year 1 Service**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
11.1							
11.2							
11.3							
12	**Option Year 2 Service**	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3	To be provided in Sprint 3		To be confirmed in Sprint 3
12.1							
12.2							
12.3							

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK II, PART II

TERMS AND CONDITIONS

INDEX OF ARTICLES

1. ORDER OF PRECEDENCE

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

a. Signature sheet

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

c. Part II – Terms and Conditions (Special Provisions)

d. Part III – “Reserved”

e. Part IV – Statement of Objectives (SOO) and Annexes

f. The Contractor’s Proposed Solution including any clarifications thereto, incorporated by reference, and the formal documentation of pre-Contract discussions agreed by both parties.

2. TYPE OF CONTRACT

2.1. This is a Firm Fixed-Price (FFP) Contract established for the services defined in Part I – Schedule of Supplies and Services (SSS) and Part IV – Performance Work Statement (PWS).

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

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

2.4. The Total Contract price in this Contract is Delivered Duty Paid (INCOTERMS 2020).

3. SCOPE

3.1. The NCI Agency aims to contract an ACPV solution for the NATO Enterprise through a Dynamic Sourcing exercise. The initial scope of this solution is to deliver a single source of truth through a foundational asset, configuration and patch management solution across the NATO enterprise. This shall support the required visibility to the cybersecurity functions, with an initial focus on supporting a risk-informed Vulnerability Management function ("ACP for V"). This will form the core of the authoritative data source for the NATO Enterprise.

3.2. The secondary scope of the ACPV Dynamic Sourcing exercise is to create a NATO Enterprise framework that will eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on asset, configuration and patch management information through a federated approach.

3.3. The scope of this contract covers the services to be delivered by the contractor in order to support the execution of the ACPV Dynamic Sourcing acquisition process by the NCI Agency.

3.4. The full requirements, Contractor Deliverables and scope is as per the PWS.

4. PERIOD OF PERFORMANCE (POP)

4.1. The Period of Performance (POP) of this Firm Fixed-Price (FFP) Contract will be from the Effective Date of Contract until:

a. EDC + 36 months.

b. Option 1: 12 months

c. Option 2: 12 months

The Contractor shall implement the full service within eighteen (18) months from the effective date of contract.

5. LANGUAGE

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

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

6.1. Upon issuance of a contract, the successful Contractor will warrant that they and their Sub-contractors are duly authorised to operate and do business in the country or countries in which this Contract is to be performed and that they and their Sub-contractors have obtained or will obtain all necessary licences and permits required in connection with the Contract. No claim for additional monies with respect to any costs or delay to obtain the authorisations to perform shall be made by the Contractor.

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

7. PARTICIPATING COUNTRIES

7.1. The Contractor may issue subcontracts to firms and purchase from qualified vendors in any contributory NATO nations in the project, namely (in alphabetical order): ALBANIA, BELGIUM, BULGARIA, CANADA, CROATIA, CZECH REPUBLIC, DENMARK, ESTONIA, FINLAND, FRANCE, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, MONTENEGRO, NETHERLANDS, NORTH MACEDONIA, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TURKEY, UNITED KINGDOM, UNITED STATES OF AMERICA.

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

7.3. The Contractor shall notify in writing to the Purchaser immediately upon being informed of any change in the nationality of its Sub-contractor(s) which would prevent the Contractor from further complying with Article 7.3 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 Article 7.3 above.

7.4. The Intellectual Property Rights (IPR) to all designed documentation and 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 community.

8. SECURITY

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

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

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

8.4. It is the responsibility of the Contractor to ensure Facility Security Clearance (FSC) is obtained for access to, or generation of classified information at level of NATO SECRET (NS).

8.5. It is the responsibility of the Contractor to ensure that its personnel obtain the required security clearances and transmit this information to the sites to be visited in adequate time that the site may perform the appropriate administration. Contractors are advised that the personnel security process may be lengthy. The Purchaser bears no responsibility for the failure of the Contractor to secure the required clearances for its personnel within the necessary time.

8.6. Failure to obtain or maintain the required level of security for Contractor personnel for the period of performance of this Contract shall not be grounds for any delay in the scheduled performance of this Contract and may be grounds for termination under Articles 12 (Sub-Contracts) and 35 (Termination for Default).

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

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

8.9. At the end of the Contract, the Contractor shall deliver all the documentation and information collected and generated in support of this Contract to the Purchaser. This includes a certificate that no copies are retained at the Contractor’s facilities. Additionally,

any equipment that had been connected to a classified network during this Contract shall be returned to the Purchaser (i.e. laptops, USB-keys, etc.).

8.10. In the performance of all works under this Contract, it shall be the Contractor's responsibility to ascertain and comply with all applicable NATO and National security regulations as implemented by the Purchaser and by the local authorities.

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

8.12. The Performance Work Statement defines the level of security of information exchanged and used for performance of the Contract.

8.13. In particular, the Contractor undertakes to:

a) Appoint an official responsible for supervising and directing security measures in relation to the Contract and communicating details of such measures to the Purchaser on request;

b) Maintain, preferably through the official responsible for security measures, a continuing relationship with the national security authority or designated security agency charged with ensuring that all NATO classified information involved in the Contract is properly safeguarded;

c) Abstain from copying by any means, without the authorization of the Purchaser, the national security authority or designated security agency, any classified documents, plans, photographs or other classified material entrusted to him;

d) Furnish, on request, information to the national security authority or designated security agency pertaining to all persons who will be required to have access to NATO classified information;

e) Maintain at the work site a current record of his employees at the site who have been cleared for access to NATO classified information. The record should show the date of issue, the date of expiration and the level of clearance;

f) Deny access to NATO classified information to any person other than those persons authorized to have such access by the national security authority or designated security agency;

g) Limit the dissemination of NATO classified information to the smallest number of persons ("need to know basis") as is consistent with the proper execution of the Contract;

h) Comply with any request from the national security authority or designated security agency that persons entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding both of their obligations under national legislation affecting the

safeguarding of classified information, and of their comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

i) Report to the national security authority or designated security agency any breaches, suspected breaches of security, suspected sabotage, or other matters of security significance which would include any changes that may occur in the ownership, control or management of the facility or any changes that affect the security arrangements and security status of the facility and to make such other reports as may be required by the national security authority or designated security agency, e.g. reports on the holdings of NATO classified material;

j) Apply to the Purchaser for approval before Sub-contracting any part of the work, if the Sub- contract would involve that the Subcontractor would have access to NATO classified information, and to place the Sub-contractor under appropriate security obligations no less stringent than those applied to his own contract;

k) Undertake not to utilize, other than for the specific purpose of the Contract, without the prior written permission of the Purchaser or his authorized representative, any NATO classified information furnished to him, including all reproductions thereof in connection with the Contract, and to return all NATO classified information referred to above as well as that developed in connection with the Contract, unless such information has been destroyed, or its retention has been duly authorized with the approval of the Purchaser. Such NATO classified information will be returned at such time as the Purchaser or his authorized representative may direct;

l) Classify any produced document with the highest classification of the NATO classified information disclosed in that document.

9. RELEASE OF INFORMATION

9.1. Except as otherwise specified elsewhere in the RFS and to the extent that it is demonstratively unavoidable and without prejudice to the Article 8 (Security), the Contractor and/or his employees shall not, without prior authorisation from the Purchaser, release to third parties any information pertaining to this RFS its subject matter, performance there under or any other aspect thereof.

9.2. The Contractor shall seek the prior written approval of the Purchaser before publishing any press release or disclosing any other information, orally or in writing, in relation to the RFS. The approval of the Purchaser shall be required for both the opportunity and the content of the information.

9.3. This provision shall remain in effect after the completion of both pre-award and post-award contract activities and shall cease to apply to any particular piece of information once that information becomes public knowledge other than through an act, default or omission of the Contractor or its Sub-contractors.

10. INTELLECTUAL PROPERTY

10.1. Purchaser Background IPR

a. The Contractor is licensed to use, non-exclusively and royalty-free any Purchaser Background IPR that is or will be made available for the sole purpose of carrying out the Work.

b. The Contractor shall not use any Purchaser Background IPR other than for the purpose of carrying out the Work without the prior written agreement of the Purchaser. Any such agreement shall include the terms relating to such use.

c. The Purchaser gives no warranty as to the validity of any Purchaser Background IPR. The Contractor shall not do anything or act in any way which is inconsistent with or prejudicial to the ownership by the Purchaser of any Purchaser Background IPR.

10.2. Contractor Background IPR

a. Any use of Contractor Background IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to Purchaser. The Contractor hereby grants to NATO a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Contractor Background IPR for the purpose of exploiting or otherwise using the Foreground IPR.

b. Any use of Contractor Background IPR is not limited to the number of users or the number of licenses required by the Contract for the use of system. The Purchaser reserves the right to use the Contractor Background IPR for any number of users and number of licenses as required, at no additional cost to the Purchaser.

10.3. Foreground IPR

a) All Foreground IPR is the property of the Purchaser on behalf of NATO. Consequently, no statement shall be made restricting the rights of the Purchaser in the Foreground IPR.

b) The Contractor shall ensure that suitable arrangements are in place between its employees, agents, consultants and itself regarding Foreground IPR generated by said employees, agents, Subcontractors and consultants to allow the Contractor to fulfil its obligations under Article above.

c) The Contractor shall be entitled to use Foreground IPR on a non-exclusive, royalty free basis solely for the purpose of carrying out the Work.

d) The Contractor shall not use any Foreground IPR other than for the purpose of carrying out the Work without the Purchaser's prior written agreement. Any such agreement shall include terms relating to such use.

e) The Contractor shall provide the Purchaser, at the latest upon delivery of the Work and thereafter for the duration of the warranty and any purchased CLS

agreement period, with full documented records of information in relation to the Work, including but not limited to, all drawings, specifications and other data that is necessary or useful to further develop, maintain and operate the Work.

f) The Contractor shall:

- do all things necessary and sign all necessary or useful documents to enable the Purchaser to obtain the registration of the Foreground IPR as the Purchaser may require and select; and
- to execute any formal assignment or other documents as may be necessary or useful to vest title to any Foreground IPR in the Purchaser.

g) The Contractor undertakes:

- to notify the Purchaser promptly of any invention or improvement to an invention or any design conceived or made by the Contractor; and
- to provide the Purchaser with such information as the Purchaser may reasonably request in order to: (i) determine the patentability of such invention or improvement; (ii) assess the need for registering such invention or improvement; and (iii) evaluate the potential value to the Purchaser of such a patent or registration if issued.

h) If the Purchaser determines that it wishes to apply for one or more patents for the disclosed invention or improvement or for a registration for the disclosed design, it will prosecute such application(s) at its own expense. The Contractor undertakes to provide the Purchaser, at the Purchaser's expense, with such information and assistance as the Purchaser shall reasonably require to prosecute such application(s).

10.4. Third Party IPR

a) Any use of Third Party IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to the Purchaser. The Contractor hereby grants to NATO a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Third Party IPR for the purpose of exploiting or otherwise using the Foreground IPR.

b) With the exception of COTS items, any use of Third Party IPR is not limited to the number of users or the number of licenses required by the Contract for the use of system. With the exception of COTS items, the Purchaser reserves the right to use the Third Party IPR for any number of users and number of licenses as required, at no additional cost to the Purchaser.

c) For COTS items, the Contractor shall be responsible for obtaining licences from the Third Party in line with the requirements of the Statement of Work (including numbers and locations of licences).

d) Where Third Party IPR is the subject of a licence or other agreement between the third party and the Purchaser or the Contractor, the Contractor shall not

use any Third Party IPR for the purposes of carrying out work pursuant to the Contract without the prior written approval of the Purchaser. Contractor shall inform Purchaser in advance of any restrictions on the Purchaser's use.

e) If, after the award of the Contract, the Contractor becomes aware of the existence of any Third Party IPR which the Contractor is using or believes is needed for the performance of the Contract, the Contractor shall immediately give the Purchaser a written report identifying such IPR and if they are compliant with the other provisions in the contract. Any Third Party IPR under this Article is subject to the prior written approval by the Purchaser.

f) The Purchaser may consider open source solutions alongside proprietary ones in developments provided that such solutions are fully compliant with the requirements of this Contract. Contractor shall disclose in advance the open source license associated with the contemplated open source solution. The Purchaser reserves the right to refuse the incorporation of open source solutions that are deemed inadequate for incorporation in a NATO application (e.g. post-back obligations).

10.5. Subcontractor IPR

a) When placing a Sub-contract which is concerned with or involves the creation of IPR, the Contractor shall ensure that the Sub-contractor enters into the same agreement for the use of the IPR as stipulated in this Contract in such a way that the Purchaser will be entitled to use the IPR as agreed between the Purchaser and the Contractor. The Contractor shall include in the Sub-contract the content of the provisions of this Article.

11. PATENT AND COPYRIGHT INDEMNITY

11.1. The Contractor shall assume all liability against any and all third party claims that the services, Work and/or parts thereof, in whole or in part, infringe(s) an IPR in force in any countries, arising out of the manufacture, import, export, performance of the services or delivery of Work and/or out of the use or disposal by, or for the account of, the Purchaser of such Services and/or Work. The Contractor shall reimburse and/or indemnify the Purchaser, its officers, agents, employees and/or consultants: (i) for all costs, fees, damages, awards, settlement amounts and any other expenses awarded to the third party right holder against Purchaser and/or the final beneficiaries of the Work in relation to said third party claim; and (ii) for the costs and expenses incurred by the Purchaser in relation to said third party claims, including attorney fees. The Contractor shall be responsible for obtaining any licences necessary for the performance of this Contract and for making all other arrangements required to indemnify the Purchaser from any liability for IPR infringement in said countries.

11.2. Each Party shall immediately notify the other of any intellectual property infringement claims of which he has knowledge and which pertain to the Work under this Contract.

11.3. This indemnity shall not apply under the following circumstances:

a) Patents or copyright which may be withheld from issue by order of the applicable government whether due to security regulations or otherwise;

b) An infringement resulting from specific written instructions from the Purchaser under this Contract;

c) An infringement resulting from changes made to the Work by the Purchaser without the Contractor prior written consent;

d) An infringement resulting from changes or additions to the Work subsequent to final delivery and Acceptance under this Contract.

12. SUB-CONTRACTS

12.1. The Contractor shall place and be responsible for the administration and performance of all Sub-contracts including terms and conditions which he deems necessary to meet the requirements of this Contract in full.

12.2. Prior to the Sub-contractors being given access to any classified information, the Contractor shall ensure that any Sub-contractor that has a need to access classified information for the performance of any part of this Contract has been granted the appropriate facility and personnel security clearances by the Sub-contractor's national authorities and that such clearances are still in effect at the time the information is disclosed and remains in effect throughout the performance of the work to be carried out under the Sub-contract concerned.

12.3. The Contractor shall seek the approval in writing of the Purchaser prior to the placing of any Sub-contract if:

a) the Sub-contract was not part of the Contractor’s original proposal;

and

b) the value of the Sub-contract is known or estimated to exceed 15 per cent of the total Contract value; or

c) the Sub-contract is one of a number of Sub-contracts with a single Sub-contractor for the same or related Work under this Contract that in the aggregate are known or expected to exceed 15 per cent of the total Contract value.

12.4. The Contractor shall inform the Purchaser of any change in Sub-contractors for Sub-contracts of a value known or estimated to exceed 15 per cent of the total Contract value.

12.5. The Contractor shall submit a copy of any such proposed Sub-contract including prices when seeking approval to the Contracting Authority but such approval by the Contracting Authority shall in no way relieve the Contractor of his responsibilities to fully achieve the contractual and technical requirements of this Contract.

12.6. The Contractor shall, as far as practicable, select Sub-contractors on a competitive basis consistent with the objectives and requirements of the Contract.

13. CONTRACTOR'S PERSONNEL WORKING AT PURCHASER'S FACILITIES

13.1. The term "Purchaser Facilities" as used in this Article shall be deemed to include sites, property, utilities, ships or vessels and the term "Facility Representative" shall be deemed to refer to the authority designated by the Purchaser responsible for the site, property, utility, ship or vessel.

13.2. The Facility Representative shall provide such available administrative and technical facilities for Contractor's personnel working at Purchaser's Facilities for the purpose of the Contract as in the opinion of the Facility Representative may be necessary for the effective and economical discharge of Work. The Facility Representative shall also determine whether these facilities will be provided free of charge to the Contractor or determine what charges are payable. The Contractor shall have no claim against the Purchaser for any such additional cost or delay or any additional cost or delay occasioned by the closure for holidays of said facilities, or other reasons, where this is generally published or made known to the Contractor by the Purchaser or his authorised representatives.

13.3. The Contractor shall, except as otherwise provided for in the Contract, make good or, at the option of the Purchaser, pay compensation for all damage occurring to any Purchaser's Facilities occasioned by the Contractor, his servants, agents or Sub-contractors, arising from his or their presence and activities in, and use of, the Purchaser's Facilities; provided that this Condition shall not apply to the extent that the Contractor is able to show that any such damage was not caused or contributed to, by his neglect, or default or the neglect or default of his servants, agents or Sub-contractors, or by any circumstances within his or their control.

13.4. All property of the Contractor while at a Purchaser Facility shall be at the risk of the Contractor, and the Purchaser shall accept no liability for any loss or damage, except to the extent that any loss or damage is the result of a wilful act or gross negligence on the part of the Purchaser's employees or agents.The Contractor shall be responsible for ascertaining what necessary facilities will be available and whether they will be provided free of charge, or determining what charges are payable.

13.5. The Contractor shall have no claim against the Purchaser for any such additional cost or delay or any additional cost or delay occasioned by the closure for holidays of said facilities, or other reasons, where this is generally published or made known to the Contractor by the Purchaser or his authorised representatives.

14. INSPECTION OF SERVICES – FIRM FIXED PRICE

14.1. Services, as used in this provision, includes services performed, workmanship, and material furnished or utilized in the performance of services.

14.2. The Contractor shall provide and maintain an inspection system acceptable to the Purchaser covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Purchaser during contract performance and for as long afterwards as the contract requires.

14.3. The Purchaser has the right to inspect and test all services called for by the contract, to the extent practicable at all times and places where the Work is being performed by the

Contractor or a Subcontractor during the term of the contract. The Purchaser shall perform inspections and tests in a manner that will not unduly delay the work.

14.4. If the Work, or any part thereof, is performed using the Contractor's or a Subcontractor's equipment, the Purchaser may elect to perform inspections or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, at no increase in contract price, all reasonable facilities and assistance for the safe and convenient performance of these duties. As far as is practicable such specific inspections shall be notified to the Contractor in writing in advance of such inspection.

14.5. If any of the services do not conform with the contract requirements, the Purchaser may require the Contractor to perform the services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by re-performance, the Purchaser may (1) require the Contractor to take necessary action to ensure that future performance conforms to contract requirements and (2) reduce the contract price to reflect the reduced value of the services performed.

14.6. If the Contractor fails to promptly perform the services again or to take the necessary action to ensure future performance in conformity with contract requirements, the Purchaser may (1) by contract or otherwise, perform the services and charge to the Contractor any cost incurred by the Purchaser that is directly related to the performance of such service or (2) terminate the contract for default.

14.7. The services to be provided by the Contractor's personnel under this Contract shall conform to the specifications, conditions and performance requirements set forth in the Contract. Inspection of the services provided will be made by the Purchaser's Project Manager or assigned Technical Representative. Services performed by the Contractor which do not conform to the specifications, conditions and performance requirements set forth in the Contract may result in the Purchaser requesting that such work be performed again at no increase in the price of the Contract. Repeated instances of work performed which fails to meet the standards and practices may result in termination of the Contract for Default.

15. SUPPLY OF CONTRACTOR DELIVERABLES AND QUALITY ASSURANCE

15.1. The Contractor shall:

a) provide the Contractor Deliverables to the Purchaser, in accordance with the SSS and the PWS (including any standards or processes specified therein).

b) allocate sufficient resources to the provision of the Contractor Deliverables to enable it to comply with the obligations in the SSS and PWS.

15.2. The Contractor shall:

a) comply with any applicable quality assurance requirements specified in the PWS in providing the Contractor Deliverables;

b) comply with all applicable Law and Legislation;

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

15.3. The provisions of Article 15.2 shall survive any performance, acceptance or payment pursuant to the Contract and shall extend to any remedial services provided by the Contractor.

16. KEY PERSONNEL

16.1. The prospective Contractor shall identify and provide a list of proposed key personnel fulfilling the roles described in the PWS for successful Contract performance and are subject to the provisions of this Article as set forth in the following paragraphs.

16.2. Under the terms of this article, Key Personnel may not be voluntarily diverted by the Contractor to perform work outside the Contract unless approved by the Purchaser. In cases where the Contractor has no control over the individual's non-availability (e.g. resignation, sickness, incapacity, etc.), the Contractor shall notify the Purchaser immediately of a change of Key Personnel and offer a substitute with equivalent qualifications at no additional costs to the Purchaser within ten (10) days of the date of knowledge of the prospective vacancy.

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

16.4. In the event of a substitution of any Key Personnel listed above and prior to commencement of performance, the Contractor shall provide a CV for the personnel proposed. The CV shall clearly stipulate:

a. Full details of professional and educational background, and

b. Evidence that the personnel is qualified in pertinent Contract related areas prescribed in the PWS.

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

16.6. The interview, if required, may be conducted as a telephone interview, or may be carried out at the Purchaser's premises.

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

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

16.9. The Purchaser Contracting Authority will confirm any consent given to a substitution in writing through an Amendment to the Contract stating the effective date of change of personnel and only such written consent shall be deemed as valid evidence of Purchaser consent. Each of the replacement personnel will also be required to sign the Non-Disclosure Declaration at ANNEX A: NCI AGENCY NON-DISCLOSURE DECLARATION hereto prior to commencement of work.

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

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

16.12. In those cases where, in the judgment of the Purchaser, the inability of the Contractor to provide a suitable replacement in accordance with the terms of this Article may potentially endanger the progress under the Contract, the Purchaser shall have the right to terminate the Contract as provided under Article 37 (Termination for Default).

16.13. Each of the Contractor's Key Personnel shall be required to sign a Non-Disclosure Declaration at ANNEX A: NCI AGENCY NON-DISCLOSURE DECLARATION hereto prior to commencement of work.

17. INDEMNITY

17.1. The Contractor will indemnify and hold harmless NATO and its servants or agents, against any liability, loss or damage arising out of or in connection of the Deliverables and Services under this Contract, including the provisions set out in Articles 10 (Intellectual Property) and 11 (Patent and Copyright Indemnity) of the NCI Agency General Provisions.

17.2. The Contractor will indemnify NATO and its servants or agents, against claims made against NATO and its servants or agents, by their personnel, and their sub-Contractors (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.

17.3. The Contractor will consult with the Agency over the handling of any claim or action to which the provisions of this Article may be relevant and will consult with the Agency over the handling of any such claim and conduct of any such action and will not without prior consultation and without the concurrence of the Agency settle or compromise any such claim or action.

17.4. 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 Contractor shall involve the Agency in any investigation into the cause of the accident.

18. AUDITS

18.1. For the avoidance of any doubt, the scope of any audit(s) or access rights to facilities and/or records of Contractor set out in the Contract shall be limited to the types of audits set out in Article 18.2 below.

18.2. Contractor shall maintain all financial records and other records relating to its performance under this Contract in accordance with generally accepted accounting principles and in such a manner as to clearly document Contractor's performance of its obligations under this Contract. Contractor acknowledges and agrees that Purchaser, and their duly authorized representatives will have reasonable access, at their own cost and expense and only following reasonable notice to Contractor, to such records, in paper or electronic form.

19. DISRUPTION

19.1. The Contractor shall take reasonable care to ensure that in the performance of its obligations under this Contract it does not disrupt the operations of the Purchaser, its employees or any other contractor employed by the Purchaser.

20. THIRD PARTY CO-OPERATION

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

a. providing such information about the manner in which the Contractor Deliverables are provided as is reasonably necessary for Purchaser Third Parties to provide their services and deliverables to the Purchaser or carry out such activities as have been delegated to them by the Purchaser;

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

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

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

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

21. USE OF NON-NATO PERSONNEL IN EVALUATIONS

21.1. The NCI Agency intends to use one or more non-NATO personnel as advisor(s) in evaluating proposed solutions. These contractor-advisor(s) are required by the terms of their NATO contract to maintain the confidentiality of any materials to which they are given access. Submission of your proposal to the NCI Agency constitutes implied consent to allow review of your proposal by the contractor-advisor(s).

21.2. An Offeror shall require the contractor-advisor to execute a supplemental non-disclosure agreement (NDA) by including a copy of the NDA with their proposal. The NDAs are not considered part of the proposal and communications (if any) between the contractor-advisor(s) and the Offerors regarding the terms of the NDA are neither discussions nor clarifications.

21.3. In the unlikely event the Offeror and the contractor-advisor(s) are unable to agree on the terms and conditions to be set forth in the NDA, Offerors are advised that the inability of the NCI Agency to obtain the contractor-advisor's expertise in reviewing the offer may adversely impact the NCI Agency's evaluation of the proposal.

22. INSPECTION AND ACCEPTANCE OF WORK

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

22.2. The services to be provided by the Contractor's personnel under this Contract shall conform to the specifications, conditions and performance requirements set forth in the Contract. Inspection of the services provided will be made by the Purchaser's Technical representatives or another authorised designee in accordance with the specifications in the PWS. Services performed by the Contractor which do not conform to the specifications, conditions and performance requirements set forth in the Contract may result in the Purchaser requesting that such work be performed again at no increase in the price of the contract. Repeated instances of work performed which fails to meet the standards and practices may result in termination of the Contract for Default.

23. INVOICES AND PAYMENT

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

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

23.3. No payment will be made if CLIN items agreed for delivery before milestones are not complete as described in pricing sheets, SSS and PWS.

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

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

23.6. The invoice amount is exclusive of VAT and exclusive of all Taxes and Duties as per Article 24 (Taxes and Duties).

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

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

23.9. The Purchaser shall not bear any liability related to financial guarantees, if any.

23.10. 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:

a) Contract number

b) Purchase Order number,

c) Contract Amendment number (if any)

d) CLINs as they are defined in the priced SSS.

e) Bank Account details for International wire transfers

23.11. 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.

23.12. Invoices shall be addressed to Financial Management and submitted in electronic format only to: accountspayable@ncia.nato.int

AND

An electronic copy of the invoice shall be sent to the Purchaser's Contracting Authority, at RFS-CO-115699-ACPV@ncia.nato.int.

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

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

24. TAXES AMD DUTIES

24.1. The Purchaser, by virtue of his status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct taxes (incl. VAT) and all customs duties on merchandise imported or exported. The Contractor, therefore, certifies that the prices stipulated in this Contract do not include amounts to cover such direct taxes or customs duties.

24.2. The Contractor shall be responsible for ensuring that his respective Sub- contractors are aware that the Purchaser is exempt from taxes and customs duties. The Contractor (and his respective Sub-contractors) shall be responsible for complying with all applicable national and local legal and administrative procedures to ensure that authorities do not attempt to assess taxes and customs duties on goods and property imported or exported through NATO member nation frontiers under this Contract nor assess direct taxation (VAT) on goods sold to the NCI Agency under this Contract.

24.3. The Purchaser shall give reasonable assistance in providing evidence/documents which might be required by the Contractor to ensure that NCI Agency receives tax exemption by virtue of its status under the Ottawa Agreement.

24.4. If, after complying with all national and local legal and administrative procedures, the authorities persist in attempting to impose taxes or duties on goods provided under this Contract, the Contractor shall inform the Contracting Authority providing the particulars of the situation, the procedures which have been followed and the point of contact at the national authority which is attempting to impose taxation or duty. The Contracting Authority will examine the situation and attempt to clarify the legal and administrative basis of the difficulty. If the Contracting Authority so directs, the Contractor shall pay the required taxes and duties and file for reimbursement or rebate from the national authorities in accordance with national legislative and administrative procedures.

24.5. In the event that the petition for reimbursement or rebate is denied by the national authorities concerned and providing that the Contractor and/or his Sub-contractor have complied with the national legislative and administrative procedures, the Purchaser shall reimburse the full amount of the payment(s) upon receipt of the Contractor's invoice indicating such tax or duty as a separate item of cost and fully identified by reference to any governmental law, regulation and/or instruction pursuant to which such tax or duty is enforced. The Contractor shall offer assistance and execute any such document that may be useful or required to ensure that Purchaser obtains the reimbursement of any tax or duty retained by a national authority.

24.6. In the event of the Contractor and/or Sub-contractor not complying with national legislative or administrative procedures, taxes and duties paid by the Contractor and/or Sub-contractors shall not be reimbursed by the Purchaser.

24.7. Following payment by the Purchaser of the taxes and/or duties pursuant to Article 24.4 above, should the Contractor subsequently receive a rebate of any amount paid by the Purchaser, the Contractor shall immediately notify the Purchaser and the amount of such rebate shall be credited or reimbursed to the Purchaser, as directed. The Contractor shall

be responsible for taking any and all action that could reasonably be required in order to obtain such rebate.

24.8. The Contractor shall be liable for all other taxes, assessments, fees, licences, administrative charges or other Government assessments or charges which are applicable to the performance of this Contract. It is the Contractor's responsibility to inform himself of his liability in each country where such liability may arise.

25. WARRANTY OF SERVICES

25.1. Acceptance, as used in this Article, means the act of an authorized representative of the Purchaser by which the Purchaser assumes for itself, or as an agent of another, ownership of existing and identified supplies, or approves specific services, as partial or complete performance of the contract.

25.2. Notwithstanding inspection and acceptance by the Purchaser or any provision concerning the conclusiveness thereof, the Contractor warrants that all services performed under this contract will, at the time of acceptance, be free from defects in workmanship and conform to the requirements of this contract. The Purchaser shall give written notice of any defect or non-conformance to the Contractor within 30 days from the date of acceptance by the Purchaser; or other specified event whose occurrence will terminate the period of notice, or combination of any applicable events or period of time. This notice shall state either (1) that the Contractor shall correct or re-perform any defective or nonconforming services, or (2) that the Purchaser does not require correction or re-performance.

25.3. If the Contractor is required to correct or re-perform, it shall be at no cost to the Purchaser, and any services corrected or re-performed by the Contractor shall be subject to this Article to the same extent as work initially performed. If the Contractor fails or refuses to correct or re-perform, the Purchaser’s Contracting Authority may, by contract, otherwise, correct, or replace with similar services and charge to the Contractor the cost occasioned to the Purchaser thereby, or make an equitable adjustment in the contract price.

25.4. If the Purchaser does not require correction or re-performance, the Contracting Officer shall make an equitable adjustment in the contract price.

26. DYNAMIC SOURCING PROTEST & DISPUTE RESOLUTION PROCEDURE

26.1. Interested Parties may present a protest to the NCI Agency Procurement Authority, of any decision made as a result of Dynamic Sourcing that allegedly violated applicable solicitation provisions and, thus, prejudiced the Offeror.

26.2. Regardless of the timeframe of the submission of the protest as indicated in Article 26.4 below, the grounds for protests are limited to:

a) The non-observance of applicable procurement procedures, if it can be demonstrated that this has led to discrimination against one or more Offerors;

b) The non-admission of an Offeror to submit a proposal; if not in compliance with the applicable internal procedures;

c) The wording of the solicitation documents/specifications in such a way as to restrict competition unduly;

26.3. Protests shall be submitted in English and in writing. Protests shall be clear and concise. Failure to submit a coherent protest may be grounds for dismissal.

26.4. The Offeror must file its protest within 5 calendar days of when the protester knew or should have known of the basis for the protest in writing or by requesting a debriefing.

26.5. The NCI Agency Procurement Authority will review the protest or hold a debriefing and notify the Offeror of its decision within 5 calendar days of when the protest arrived or 5 calendar days of when the debriefing was held. The decision will be provided verbally or in writing.

26.6. Thereafter, if the Offeror is not satisfied with the decision made by the NCI Agency Procurement Authority, a dispute is deemed to exist and it must follow the periods specified below:

a) The Offeror may raise the dispute to their National Delegation within 5 calendar days of when the protest dismissal notification was obtained. Extension requests of up to 5 additional calendar days must be submitted in writing by the National Delegation.

b) Upon review of Offerors dispute, the National Delegation shall submit a formal notification to the NCI Agency within 5 calendar days.

c) The NCI Agency shall review the notification and make an immediate determination.

d) If an amicable settlement is not possible, the protest/dispute will be sent to an independent board and a decision shall be made within 10 calendar days. Timeline depicted below.

26.7. Protests/Disputes shall be addressed to the NCI Agency Procurement Authority at: RFS-CO-115699-ACPV@ncia.nato.int

27. BID/PERFORMANCE GUARANTEES

27.1. No Bid/Performance Guarantees shall be required from the Contractor for this Contract.

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

28.1. **Definitions**. As used in this clause-

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

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

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

information, such as necessary to process payments. Examples of NATO Information are:

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

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

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

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

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

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

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

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

b. For contractor CIS storing, processing, or transmitting NATO UNCLASSIFIED Information that are not part of a cloud computing service or IT service or system operated on behalf of NATO and therefore not subject to the security requirement specified at paragraph 28.2(a) of this clause, the ISO/IEC 27001 security standards shall apply

c. The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Purchaser. The scope of certification and the statement of applicability must be acceptable, following review, to the Purchaser, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

c. For contractor CIS storing, processing, or transmitting NATO RESTRICTED Information the security requirements specified in the PWS, Exhibit 4 "Safeguarding of NATO Restricted Information" as mandated in NATO's Security Committee reference document number, AC/35-D/2003-REV5, dated 13 May 2015, entitled, "Directive on Classified Project and Industrial Security" shall apply.

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

e. The Purchaser reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with this clause.

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

f. **Subcontracts**. The Contractor shall include the substance of this clause, including this paragraph (28.7), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or services in which the subcontractor may have NATO Information residing in or transiting through its CIS.

29. CYBER INCIDENT REPORTING

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

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

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

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

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

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

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

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

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

29.3. **Cyber incident reporting requirement.**

a. When the Contractor discovers a cyber incident that affects a contractor CIS or NATO Information residing therein, or that affects the contractor's ability to perform the requirements of the contract, the Contractor shall—

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

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

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

i. Company name

ii. Facility Clearance Level

iii. Company point of contact information (name, position, telephone, email)

iv. NCI Agency Project Manager point of contact (name, position, telephone, email)

v. Contract number(s) or other type of agreement affected or potentially affected

vi. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)

vii. Contract or other type of agreement classification level

viii. Impact to NATO Information and/or provided products/services

ix. Ability to provide operational support

x. Date incident discovered

xi. Location(s) of compromise

xii. NATO programs, platforms or systems involved

xiii. Classification of the systems involved

xiv. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)

xv. Description of technique or method used in the cyber incident

xvi. Incident outcome (successful compromise, failed attempt, unknown)

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

xviii. Confirm whether news media are already aware/informed of the incident

xix. Any additional information

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

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

ii. **Media preservation and protection**. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph 29.2(a) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow the Purchaser to request the media or decline interest.

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

iv. **Cyber incident damage assessment activities**. If the Purchaser elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph 29.2(d) of this clause.

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

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

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

g. **Subcontracts**. The Contractor shall—

i. Include this clause, including this paragraph (29.2(g)), in subcontracts, or similar contractual instruments, for which subcontract performance will involve NATO Information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as NATO Information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and,

ii. Require subcontractors to provide a copy of the incident report to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to the Purchaser as required in paragraph 29.2 of this clause.

30. LIMITATIONS ON LIABILITY

30.3. The Contractor and any Subcontractor shall not be liable to the Purchaser for any claims, liabilities, losses, damages, costs or expenses arising under or in connection with this Contract for an aggregate amount in excess of an amount equal to three times the fees paid or payable under this Contract by the Purchaser to the Contractor, except to the extent it is finally judicially determined to have resulted primarily from bad faith or wilful misconduct of the Contractor.

30.4. In no event shall the Contractor or any Subcontractor be liable whether in contract, tort or otherwise for any consequential, special, indirect, incidental, punitive or exemplary loss, damage or expense arising under or in connection with the Contract such as but not limited to any losses incurred as a result of loss of use, contracts, data, goodwill, revenues or profits (whether or not deemed to constitute direct claims) except to the extent it is

finally determined to have resulted primarily from the bad faith or intentional misconduct of the Contractor.

31. PENALTIES AND LIQUIDATED DAMAGES

31.3. If the Contractor fails to:

a. meet the delivery schedule of the Deliverables or any specified major performance milestones or required performance dates specified in the Schedule of Supplies and Services to this Contract, or any extension thereof, or

b. deliver and obtain acceptance of the Deliverables or to acceptably perform the services as specified in the SSS to this Contract, the actual damage to the Purchaser for the delay will be difficult or impossible to determine. Therefore, in lieu of actual damages the Contractor shall pay to the Purchaser, for each day of delinquency in achieving the deadline or milestone, fixed and agreed liquidated damages of 0.1% (one percent) per day of the associated payment.

31.4. In addition to the liquidated damages, the Purchaser shall have the possibility of terminating this Contract in whole or in part, as provided in Article 37 “Termination for Default”. In the event of such termination, the Contractor shall be liable to pay the excess costs provided in Article 37.5 “Termination for Default”.

31.5. The Contractor shall not be charged with liquidated damages when the delay arises out of causes beyond the control and without the fault or negligence of the Contractor as defined in Article 37.6 “Termination for Default”. In such event, the Purchaser shall ascertain the facts and extent of the delay and shall extend the time for performance of the Contract when in his judgement the findings of the fact justify an extension.

31.6. Liquidated damages shall be payable to the Purchaser from the first day of delinquency and shall accrue at the rate specified in Article 31.2(b) above to 20% of the value of each line item individually and an aggregate sum of all delinquent items not to exceed 15% of the value of the total Contract. These liquidated damages shall accrue automatically and without any further notice being required.

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

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

b. By reclaiming such damages through appropriate legal remedies.

31.8. The rights and remedies of the Purchaser under this Article are in addition to any other rights and remedies provided by law or under this Contract.

32. HEALTH, SAFETY AND ACCIDENT PREVENTION

32.3. If the Purchaser notifies the Contractor in writing of any non-compliance in the performance of this Contract with safety and health rules and requirements prescribed on the date of this Contract by applicable national or local laws, ordinances and codes, and the Contractor fails to take immediate corrective action, the Purchaser may order the Contractor to stop all or part of the Work until satisfactory corrective action has been taken. Such an order shall not entitle the Contractor to an adjustment of the Contract price or other reimbursement for resulting increased costs, or to an adjustment of the delivery or performance schedule.

33. CHANGES

33.3. The Purchaser may at any time, by written order of the Contracting Authority designated or indicated to be a change order (“Change Order”) make changes within the general scope of this Contract, including, without limitation, in any one or more of the following:

a. Specifications (including drawings and designs);

b. Method and manner of performance of the work, including engineering standards, quality assurance and configuration management procedures;

c. Marking and method of shipment and packing;

d. Place of delivery;

e. Amount, availability and condition of Purchaser Furnished

33.3. Property.

33.4. The Purchaser shall submit a proposal for Contract amendment describing the change to the Contract.

33.5. If any such Change Order causes an increase in the Contractor's cost of, or the time required for, the performance of any part of the Work under this Contract, whether or not changed by any such order, the Contractor shall submit a written proposal for adjustment to the Purchaser describing the general nature and amount of the proposal for adjustment. The Contractor shall submit this proposal for adjustment within thirty (30) days after receipt of a written Change Order under (a) above unless this period is extended by the Purchaser.

33.6. If any such Change Order causes a decrease in the Contractor's cost of, or the time required for, the performance of any part of the Work under this Contract, whether or not changed by any such order, the Purchaser shall submit a proposal for adjustment within thirty (30) days from the issuance of the Change Order by submitting to the Contractor a written statement describing the general nature and amount of the proposal for adjustment.

33.7. Where the cost of property made obsolete or in excess as a result of a change is included in the Contractor's claim for adjustment, the Purchaser shall have the right to prescribe the manner of disposition of such property.

33.8. The Purchaser reserves the right to reject the introduction of the change, after the evaluation of the change proposal, even if the Purchaser initiated such change.

33.9. Failure to agree to any requested adjustment shall be a dispute within the meaning of the Article 26 (Protest and Dispute Resolution Procedures). However, nothing in this Article shall excuse the Contractor from proceeding with the Contract as changed.

33.10. No proposal for adjustment by the Contractor for an equitable adjustment shall be allowed if asserted after final payment and acceptance under this Contract.

33.11. Any other written or oral order (which, as used in this paragraph includes direction, instruction, interpretation, or determination) from the Purchaser that causes a change shall be treated as a Change Order under this Article, provided, that the Contractor gives the Purchaser a written notice within thirty (30) Days after receipt of such order stating (i) the date, circumstances, and source of the order; (ii) that the Contractor regards the order as a Change Order; and (iii) a detailed cost and time analysis of the impact of the change, and that the Order is accepted in writing by the Purchaser as a Change Order. The timely written notice requirement, as detailed above, remains in force in all cases, even where, for example, the Purchaser has positive knowledge of the relevant facts.

33.12. All tasks and activities carried out by the Contractor in relation to the processing of the Change Order or in relation to this Article shall form part of the Contractor's routine work and cannot be charged as additional work.

34. STOP WORK ORDER

34.2. The Purchaser may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the Work called for by this Contract for a period of ninety (90) days after the order is delivered to the Contractor, and for any further period to which the Parties may agree.

34.3. Any such stop work order shall be specifically identified as a stop work order issued pursuant to this Article. The Stop Work Order may include a description of the Work to be suspended, instructions concerning the Contractor's issuance of further orders for material or services, guidance to the Contractor on actions to be taken on any Sub-contracts and any suggestion to the Contractor for minimizing costs.

34.4. Upon receipt of such a Stop Work Order, the Contractor shall forthwith comply with its terms and take all reasonable steps to minimise costs incurred allocable to the Work covered by the Stop Work Order during the period of work stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to the Contractor, or within any extension of that period to which the Parties shall have agreed, the Purchaser shall either:

a. cancel the Stop Work Order; or

b. terminate the Work covered by such Stop Work Order as provided in Article 36 (Termination for Convenience of the Purchaser).

34.5. If a Stop Work Order issued under this Article is cancelled or the period of the Stop Work Order or any extension thereof expires, the Contractor shall resume work.

34.6. An equitable adjustment shall be made in the delivery schedule or Contract price, or both, and the Contract shall be modified in writing accordingly, if:

a. the Stop Work Order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this Contract, and;

b. the Contractor asserts a Claim for such adjustment within thirty (30) days after the end of the period of work stoppage; provided that, if the Purchaser decides the facts justify such action, he may receive and act upon any such claim asserted at a later date but prior to final payment under this Contract.

34.7. If a Stop Work Order is not cancelled and the Work covered by such Stop Work Order is terminated for the convenience of the Purchaser the reasonable costs resulting from the Stop Work Order shall be allowed in arriving at the termination settlement.

35. CLAIMS

35.2. The Contractor shall specifically identify the Contract Article(s) under which the Claim(s) is/are based.

35.3. Claims shall be specifically identified as such and submitted:

a. within the time specified in the Article under which the Contractor alleges to have a Claim. If no time is specified in the Article under which the Contractor intends to base his Claim, the time limit shall be sixty (60) days from the date the Contractor has knowledge or should have had knowledge of the facts on which he bases his Claim; and

b. before final payment, if the Contractor could not have had earlier knowledge and were not foreseeable.

35.4. The Contractor shall be foreclosed from his Claim unless he presents complete documentary evidence, justification and costs for each of his Claims within ninety (90) calendar days from the assertion date of such Claims. Claims shall be supported by specifically identified evidence (including applicable historical and planned cost and production data from the Contractor's books and records). Opinions, conclusions or judgmental assertions not supported by such evidence will be rejected by the Purchaser.

35.5. An individual breakdown of cost is required for each element of Contractor's Claims at the time of claim submission or for any material revision of the Claim.

35.6. The Contractor shall present, at the time of submission of a Claim, an attestation as follows:

I .....the responsible senior company official authorised to commit the ..... with respect to its claims dated ..... being duly sworn, do hereby depose and say that: (i) the facts described in the claim are current, complete and accurate; and (ii) the conclusions in the claim accurately reflect the material damages or contract adjustments for which the Purchaser is allegedly liable.

.....……..

SIGNATURE Date

35.7. Failure to comply with any of the above requirements shall result in automatic foreclosure of the Claim. This foreclosure takes effect in all cases and also where, for example, the Claim is based on additional orders, where the facts are known to the Purchaser, where the Claim is based on defective specifications of the Purchaser or an alleged negligence in the pre-contractual stage.

35.8. Claims submitted by the Contractor will be reviewed by the Contracting Authority. The Contracting Authority will respond within sixty (60) days with a preliminary decision, based on an assessment and evaluation of the facts presented by the Parties, as to whether the Contracting Authority considers the Claim to have merit for consideration. If the preliminary decision of the Contracting Authority is that the Claim, as submitted is without merit, the Contractor shall have fourteen (14) days to present a rebuttal to the Contracting Authority and request reconsideration of the Contracting Authority's decision. Within thirty (30) days receipt of the Contractor's request for reconsideration, the Contracting Authority will issue a decision. The time requirements stated herein may be extended by the Contracting Authority in order to accommodate additional preparation efforts and fact finding discussions but the Contracting Authority may not unreasonable extend such a period. A decision that the submitted claim is without merit will be identified as such, will be issued in writing by the Contracting Authority and will be conclusive. A decision may only be challenged by the Contractor through the Disputes provisions described herein.

35.9. A decision by the Purchaser that the claim has merit will result in a Contracting Authority request to enter into negotiations with the Contractor to arrive at a mutually agreed fair and equitable settlement. The Contracting Authority's decision will contain a target date for the commencement and conclusion of such operations. If the Parties are unable to arrive at an agreement on a fair and reasonable settlement by the target date for conclusion, or any extension thereto made by the Contracting Authority, the latter may declare that negotiations are at an impasse and issue a preliminary decision as to the fair and reasonable settlement and the reasons supporting this decision. The Contractor shall have a period of thirty (30) days to present a rebuttal to the Contracting Authority and request reconsideration of the Contracting Authority's decision. Within sixty (60) days of receipt of the Contractor's request for reconsideration, the Contracting Authority will issue its decision on the request for reconsideration. This timeframe will be respected unless an authorisation is needed from a NATO or other authority, the schedule for which is beyond the Contracting Authority's control. A decision of the Contracting Authority on the reconsideration of the matter will be identified as such, will be issued in writing by the

Contracting Authority and will be conclusive. A decision on the reconsideration may only be challenged by the Contractor through the Disputes provisions described herein.

35.10. No Claim arising under this Contract may be assigned by the Contractor without prior approval of the Purchaser.

35.11. The Contractor shall proceed diligently with performance of this Contract, pending final resolution of any request for relief, claim appeal, or action arising under the Contract, and comply with any decision of the Contracting Authority.

36. TERMINATION FOR CONVENIENCE OF THE PURCHASER

36.2. The performance of Work under this Contract may be terminated by the Purchaser in accordance with this Article in whole, or from time to time in part, whenever the Purchaser shall determine that such termination is in the best interest of the Purchaser.

36.3. Any such termination shall be effected by delivery to the Contractor of a written notice of termination, signed by the Contracting Authority, specifying the extent to which performance of Work under the Contract is terminated, and the date upon which such termination becomes effective.

36.4. After receipt of a Notice of Termination and except as otherwise directed by the Contracting Authority, the Contractor shall:

a. stop the Work on the date and to the extent specified in the notice of termination;

b. place no further orders or Sub-contracts for Work, Parts, materials, services or facilities, except as may be necessary for completion of such portion of the Work under the Contract as is not terminated;

c. terminate all orders and Sub-contracts to the extent that they relate to the performance of Work terminated by the Notice of Termination;

d. assign to the Purchaser, in the manner, at the times and to the extent directed by the Purchaser, all of the right, title and interest of the Contractor under the orders and Sub-contracts so terminated, in which case the Purchaser shall have the right, in its discretion, to settle or pay any or all claims arising out of the termination of such orders and Sub-contracts;

e. settle all outstanding liabilities and all claims arising out of such termination of orders and Sub-contracts, with the approval or ratification of the Purchaser to the extent he may require, which approval or ratification shall be final for all the purposes of this Article;

f. transfer title and deliver to the Purchaser in the manner, at the times, and to the extent, if any, directed by the Contracting Authority of:

i. the fabricated parts, work in process, completed work, Work, and other material produced as a part of, or acquired in connection with the performance of the Work terminated by the notice of termination, and

ii. the completed or partially completed plans, drawings, information, and other property which, if the Contract had been completed, would have been required to be furnished to the Purchaser;

g. use his best efforts to sell, in the manner, at the times, to the extent, and at the price or prices directed or authorised by the Contracting Authority, any property of the types referred to in Article 36.3(f) above. However, the Contractor:

i. shall not be required to extend credit to any Buyer; and

ii. may acquire any such property under the conditions prescribed by and at a price or prices approved by the Purchaser; and provided further that the proceeds of any such transfer or disposition shall be applied in reduction of any payments to be made by the Purchaser to the Contractor under this Contract or shall otherwise be credited to the price or cost of the Work or paid in such manner as the Contracting Authority may direct;

h. complete performance of such part of the Work as shall not have been terminated by the Notice of Termination; and

i. take such action as may be necessary, or as the Purchaser may direct, for the protection and preservation of the property related to this Contract which is in the possession of the Contractor and in which the Purchaser has or may acquire an interest.

36.5. The Contractor may submit to the Purchaser a list, certified as to quantity and quality, of any or all items of termination inventory not previously disposed of, exclusive of items the disposition of which has been directed or authorised by the Purchaser, and may request the Purchaser to remove such items or enter into a storage agreement covering the same; provided that the list submitted shall be subject to verification by the Purchaser upon removal of the items, or if the items are stored, within forty-five (45) Days from the date of submission of the list, and any necessary adjustment to correct the list as submitted shall be made prior to final settlement.

36.6. After receipt of a notice of termination, the Contractor shall submit to the Purchaser his termination Claim for the Work covered by the notice of termination, in the form and with certification prescribed by the Purchaser. Such claim shall be submitted promptly but in no event later than six (6) months from the effective date of termination, unless one or more extensions are granted in writing by the Purchaser, upon request of the Contractor made in writing within such six-month period or authorised extension thereof. However, if the Purchaser determines that the facts justify such action, the Purchaser may receive and act upon any such termination claim at any time after such six-month period or any extension thereof. Upon failure of the Contractor to submit his termination claim within the time allowed, the Purchaser may determine on the basis of information available to him, the amount, if any, due to the Contractor by reason of the termination and shall thereupon pay to the Contractor the amount so determined.

36.7. Subject to the provisions of Article 36.5, the Contractor and the Purchaser may agree upon the whole or any part of the amount or amounts to be paid to the Contractor by reason of the total or partial termination of Work pursuant to this Article, which amount or amounts may include a reasonable allowance for profit on work done; provided that such agreed amount or amounts exclusive of settlement costs shall not exceed total Contract

price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of the Work not terminated. The Contract shall be amended accordingly and the Contractor shall be paid the amount agreed.

36.8. In the event of the failure of the Contractor and the Purchaser to agree as provided in Article 36.6 upon the whole amount to be paid to the Contractor by reason of the termination of Work pursuant to Article 36, the Purchaser shall pay to the Contractor the amounts determined by the Purchaser as follows, but without duplication of any amounts agreed upon in accordance with Article 36.6 the total of:

a. for completed Work accepted by the Purchaser (or sold or acquired as provided in Article 36.3 above) and not therefore paid for, a sum equivalent to the aggregate price for such Work computed in accordance with the price or prices specified in the Contract, appropriately adjusted for any saving of freight or other charges;

b. the costs incurred in the performance of the Work terminated including initial costs and preparatory expense allocable thereto, but exclusive of any costs attributable to Work paid or to be paid for under Article 36.7(a);

c. the cost of settling and paying claims arising out of the termination of work under Sub-contracts or orders, as provided in Article 36.3(e), which are properly chargeable to the terminated portion of the Contract, exclusive of amounts paid or payable on account of Work or materials delivered or services furnished by Sub-contractors or vendors prior to the effective date of the notice of termination, which amounts shall be included in the costs payable under Article 36.7(b); and

d. a sum, as profit on Article 36.7(a) above, determined by the Purchaser to be fair and reasonable; provided, however, that if it appears that the Contractor would have sustained a loss on the entire Contract, had it been completed, no profit shall be included or allowed and an appropriate adjustment shall be made reducing the amount of the settlement to reflect the indicated rate of loss; and

e. the reasonable costs of settlement, including accounting, legal, clerical and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination and settlement of Sub-contracts there under, together with reasonable storage, transportation, and other costs incurred in connection with the protection, or disposition of property allocable to this Contract.

36.9. The total sum to be paid to the Contractor under Article 36.7 shall not exceed the total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of Work not terminated.

36.10. Except for normal spoilage, and except to the extent that the Purchaser shall have otherwise expressly assumed the risk of loss, there shall be excluded from the amounts payable to the Contractor, as provided in Article 36.7 above, the fair value, as determined by the Purchaser, of property which is destroyed, lost, stolen, or damaged so as to become undeliverable to the Purchaser, or to a buyer pursuant to Article 36.3(g) above.

36.11. The Contractor shall have the right to dispute, under the Article 26 (Protest and Dispute Resolution Procedures), any determination made by the Purchaser under Articles 36.5 and 36.7, except that if the Contractor has failed to submit his claim within the time

provided in Article 36.5 and has failed to request extension of such time, the Contractor shall be foreclosed from his right to dispute said determination. In any case where the Purchaser has made a determination of the amount due under Articles 36.5 and 36.7, the Purchaser shall pay the Contractor the following:

a. if there is no right of appeal hereunder or if no timely appeal has been taken, the amount so determined by the Purchaser, or

b. if an appeal has been taken, the amount finally determined on such appeal.

36.12. In arriving at the amount due to the Contractor under this Article there shall be deducted:

a. all unliquidated advance or other payments on account theretofore made to the Contractor, applicable to the terminated portion of this Contract;

b. any claim which the Purchaser may have against the Contractor in connection with this Contract; and

c. the agreed price for, or the proceeds of the sale of, any materials, Work, or other things acquired by the Contractor or sold, pursuant to the provisions of this Article, and not otherwise recovered by or credited to the Purchaser.

36.13. If the termination hereunder is partial, prior to the settlement of the terminated portion of this Contract, the Contractor may file with the Purchaser, in accordance with Article 33 (Changes), a request in writing for an equitable adjustment of the price or prices relating to the continued portion of the Contract (the portion not terminated by the notice of termination), and such equitable adjustment as may be agreed upon shall be made in such price or prices.

36.14. The Purchaser may from time to time, under such terms and conditions as it may prescribe, make partial payments and payments on account against costs incurred by the Contractor in connection with the terminated portion of this Contract whenever in the opinion of the Purchaser the aggregate of such payments shall be within the amount to which the Contractor will be entitled hereunder. If the total of such payment is in excess of the amount finally agreed or determined to be due under this Article, such excess shall be payable by the Contractor to the Purchaser upon demand, together with interest calculated using the average of the official base rate(s) per annum of the deposit facility rate as notified by the European Central Bank or such other official source as may be determined by the Purchaser, for the period from the date the excess is received by the Contractor to the date such excess is repaid to the Purchaser, provided, however, that no interest shall be charged with respect to any such excess payment attributed to a reduction in the Contractor's claim by reason of retention or other disposition of termination inventory until ten days after the date of such retention or disposition or such later date as determined by the Purchaser by reason of the circumstances.

36.15. Unless otherwise provided for in this Contract, the Contractor, from the effective date of termination and for a period of three years after final settlement under this Contract, shall preserve and make available to the Purchaser at all reasonable times at the office of the Contractor, but without direct charge to the Purchaser, all his books, records, documents, computer files and other evidence bearing on the costs and expenses of the Contractor under this Contract and relating to the work terminated hereunder, or, to the extent

approved by the Purchaser, photographs, micro-photographs, or other authentic reproductions thereof.

37. TERMINATION FOR DEFAULT

37.2. The Purchaser may, subject to Article 37.6 below, by written notice of default to the Contractor, terminate the whole or any part of this Contract if the Contractor, inclusive but not limited to:

a. fails to make delivery of all or part of the Work within the time specified in the contract or any agreed extension thereof;

b. fails to make progress as to endanger performance of this Contract in accordance with its terms;

c. fails to meet the technical requirements or the Specifications of the Contract;

d. fails to comply with Article 8 (Security);

e. transfer this Contract without the Purchaser's prior written consent;

f. breaches any provision of this Contract; or

37.3. In the case of any of the circumstances set forth in Clause 39.1 above, the Purchaser shall issue a letter to the Contractor stating that an actual or potential default exists and requiring a response from the Contractor within ten (10) Days that identifies:

a. in the case of late delivery of Work, when the Contractor shall deliver the Work and what circumstances exist which may be considered excusable delays under Article 37.6.

b. in the case of the other circumstances identified in Article 37.1 above, what steps the Contractor is taking to cure such failure(s) within a period of ten Days (or such longer period as the Purchaser may authorise in writing) after receipt of notice in writing from the Purchaser specifying such failure and identifying any circumstances which exist which may be considered excusable under Article 37.6.

37.4. The Purchaser shall evaluate the response provided by the Contractor or, in the absence of a reply within the time period mentioned in Article 37.2, all relevant elements of the case, and make a written determination within a reasonable period of time that:

a. sufficient grounds exist to terminate the Contract in whole or in part in accordance with this Article and that the Contract is so terminated;

b. there are mitigating circumstances and the Contract should be amended accordingly; or

c. the Purchaser will enter a period of forbearance in which the Contractor must show progress, make deliveries, or comply with the Contract provisions as specified by the Purchaser. The Purchaser may apply other remedial actions as provided by this Contract during such period of forbearance. This period of forbearance shall in

no event constitute a waiver of Purchaser's rights to terminate the Contract for default.

37.5. At the end of the period of forbearance, which may be extended at the Purchaser's discretion, the Purchaser may terminate this Contract in whole or in part as provided in Article 37.1 if the Contractor has not made adequate progress, deliveries or compliance with the Contract provisions which were the terms of the period of forbearance.

37.6. In the event the Purchaser terminates this Contract in whole or in part, as provided in Article 37.1, the Purchaser may procure, upon such terms and in such manner as the Purchaser may deem appropriate, Work similar to those so terminated, and the Contractor shall be liable to the Purchaser for any excess costs for such similar Work; however, the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this Article.

37.7. Except with respect to the default of Sub-contractors, the Contractor shall not be held liable for a termination of the Contract for default if the failure to perform the Contract arises out of causes beyond the control and without the fault or negligence of the Contractor.

a. Such causes may include, but are not restricted to, acts of God, acts of the public enemy, acts of the Purchaser in its contractual capacity, acts of sovereign governments which the Contractor could not reasonably have anticipated, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

b. If the failure to perform is caused by the default of a Sub-contractor, and if such default arises out of causes beyond the control of both the Contractor and Sub-contractor, without the fault or negligence of either of them, the Contractor shall not be held liable for a termination for default for failure to perform unless the Work to be furnished by the Sub-contractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required delivery schedule.

37.8. If this Contract is terminated as provided in Article 37.1, the Purchaser, in addition to any other rights provided in this Article and the Contract, may require the Contractor to transfer title and deliver to the Purchaser, in the manner and to the extent directed by the Purchaser:

a. any completed Work with associated rights ;

b. such partially completed Work, materials, Parts, tools, dies, jigs, fixtures, plans, drawings, information, and Contract rights (hereinafter called "Manufacturing materials") with associated rights as the Contractor has specifically produced or specifically acquired for the performance of such part of this Contract as has been terminated;

37.9. In addition to Article 37.7, the Contractor shall, upon direction of the Purchaser, protect and preserve property in the possession of the Contractor in which the Purchaser has an interest.

37.10. Payment for completed Work delivered to and accepted by the Purchaser shall be at the Contract price.

37.11. Payment for manufacturing materials delivered to and accepted by the Purchaser and for the protection and preservation of property shall be in an amount agreed upon by the Contractor and Purchaser, failure to agree to such amount shall be a dispute within the meaning of Article 26 (Protest and Dispute Resolution Procedures).

37.12. The Purchaser may withhold from amounts otherwise due to the Contractor for such completed Work or manufacturing materials such sum as the Purchaser determines to be necessary to protect the Purchaser against loss because of outstanding liens or claims of former lien holders.

37.13. If, after notice of termination of this Contract under the provisions of this Article, it is determined for any reason that the Contractor was not in default under the provisions of this Article, or that the default was excusable under the provisions of this Article, the rights and obligations of the Parties shall be the same as if the notice of termination had been issued pursuant to Article 36 (Termination for the Convenience of the Purchaser).

37.14. If after such notice of termination of this Contract under the provisions of this Article, it is determined for any reason that the Contractor was not in default under the provisions of this Article and that the Parties agree that the Contract should be continued, the Contract shall be equitably adjusted to compensate for such termination and the Contract modified accordingly. Failure to agree to any such adjustment shall be a dispute within the meaning of Article 26 (Protest and Dispute Resolution Procedures).

37.15. The rights and remedies of the Purchaser provided in this Article shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

38. CONFLICT OF INTEREST

38.2. 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, 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.

38.3. The restrictions described herein shall apply to the Contractor and its affiliates, consultants and subcontracts under this contract. If the Contractor under this contract prepares or assists in preparing a statement of work, specifications and plans, the Contractor and its affiliates shall be ineligible to bid or participate, in any capacity, in any contractual effort which is based on such statement of work or specifications and plans as a prime contractor, subcontractor, and consultant or in any similar capacity. The Contractor shall not incorporate its products or services in such statement of work or specification unless so directed in writing by the Contracting Officer, in which case the

restriction shall not apply. This contract shall include this clause in its subcontractor's or consultants' agreements concerning the performance of this contract.

38.4. The Contractor shall provide a statement with their proposal which concisely describes all relevant facts concerning any past, present, or currently planned interest (financial, contractual, organizational, or otherwise) relating to the work to be performed hereunder. The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in Article 38.1, or that the Contractor has disclosed all such relevant information prior to award. If a potential conflict is discovered after award, the Contractor shall make a full disclosure in writing to the Contracting Officer. The disclosure shall include a description of action which the Contractor proposes to take, after consultation with the Contracting Officer, to avoid, mitigate, or neutralize the conflict of interest.

38.5. In addition, the Contractor shall for the term of this Contract and 12 months thereafter notify the Contracting Officer, in writing, of its intention to compete for, or accept the award of any contract for Identical Work for any NATO organization. Such notification shall be made before the Contractor either competes for or accepts any such contract. For the purpose of this Article 38.4, the term “Identical Work” shall mean the use of the same Key Personnel to offer the same scope of services as specified in the Schedule of Supplies and Services.

38.6. The Contractor's notice called for in Article 38.3 above shall describe the actual, apparent, or potential conflict of interest, the action(s) the Contractor has taken or proposes to take to avoid or mitigate any conflict, and shall set forth any other information which the Contractor believes would be helpful to the Purchaser’s Contracting Authority in analyzing the situation. Any changes to the contractors Conflict of Interest Mitigation Plan, if any is incorporated in the Contract, should be also detailed.

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

38.8. If the Purchaser’s Contracting Authority in his/her discretion determines that the Contractor's actual, apparent, or potential conflict of interest remains, or the measures proposed are insufficient to avoid or mitigate the conflict, the Purchaser’s Contracting Authority will direct a course of action to the Contractor designed to avoid, neutralize, or mitigate the conflict of interest. If the parties fail to reach agreement on a course of action, or if having reached such agreement the Contractor fails to strictly adhere to such agreement during the remaining period of Contract performance, the Purchaser’s Contracting Authority has the discretion to terminate the Contract for Default in accordance with Article 37 “Termination for Default”.

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

38.10. The Contractor further agrees to insert in any subcontract or consultant agreement hereunder, provisions which shall conform substantially to the language of this clause, including this paragraph 38.9.

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

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

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

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

39.2. Information Management and Information

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

39.3. Use of PFI

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

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

39.4. Information alteration and disposal

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

39.5. Subcontracts

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

40. PURCHASER FURNISHED PROPERTY

40.1. The Purchaser shall deliver to the Contractor, for use only in connection with this Contract, the Purchaser Furnished Property at the times and locations stated in the Contract. In the event that Purchaser Furnished Property is not delivered by such time or

times stated in the Schedule, or if not so stated, in sufficient time to enable the Contractor to meet such delivery or performance dates the Purchaser shall, upon timely written request made by the Contractor, and if the facts warrant such action, equitably adjust any affected provision of this Contract pursuant to Article 33 (Changes).

40.2. In the event that Purchaser Furnished Property is received by the Contractor in a condition not suitable for its intended use, the Contractor shall immediately notify the Purchaser. The Purchaser shall within a reasonable time of receipt of such notice replace, re-issue, authorise repair or otherwise issue instructions for the disposal of Purchaser Furnished Property agreed to be unsuitable. The Purchaser shall, upon timely written request of the Contractor, equitably adjust any affected provision of this Contract pursuant to Article 33 (Changes).

40.3. Title to Purchaser Furnished Property will remain in the Purchaser. The Contractor shall maintain adequate property control records of Purchaser Furnished Property in accordance with sound industrial practice and security regulations.

40.4. Unless otherwise provided in this Contract, the Contractor, upon delivery to him of any Purchaser Furnished Property, assumes the risk of, and shall be responsible for, any loss thereof or damage thereof except for reasonable wear and tear, and except to the extent that Purchaser Furnished Property is consumed in the performance of this Contract.

40.5. Upon completion of this Contract, or at such earlier dates as may be specified by the Purchaser, the Contractor shall submit, in a form acceptable to the Purchaser, inventory schedules covering all items of Purchaser Furnished Property.

40.6. The inventory shall note whether:

a. The property was consumed or incorporated in fabrication of final deliverable(s);
b. The property was otherwise destroyed;
c. The property remains in possession of the Contractor;
d. The property was previously returned

40.7. The Contractor shall prepare for shipment, deliver DDP at a destination agreed with the Purchaser, or otherwise dispose of Purchaser Furnished Property as may be directed or authorised by the Purchaser. The net proceeds of any such disposal shall be credited to the Contract price or paid to the Purchaser in such other manner as the Purchaser may direct.

40.8. The Contractor shall not modify any Purchaser Furnished Property unless specifically authorised by the Purchaser or directed by the terms of the Contract.

40.9. The Contractor shall indemnify and hold the Purchaser harmless against claims for injury to persons or damages to property of the Contractor or others arising from the Contractor's possession or use of the Purchaser Furnished Property. The Contractor shall indemnify the Purchaser for damages caused by the Contractor to the Purchaser, its property and staff and arising out of the Contractor's use of the Purchaser Furnished Property.

41. REACH CAPABILITY

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

41.2. The provision of the REACH capability is governed by Article 40, Purchaser Furnished Property, Article 41 and Annex B to the Terms and Conditions.

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

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

42.6. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to the NCI Agency's Cyber Incident Reporting clause (or derived from such information obtained under that clause):

42.6.1 The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Purchaser in support of the NATO activities related to stipulated clause and shall not be used for any other purpose.

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

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

42.6.4 The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the NCI Agency and the Contractor, as required by paragraph 42.6.3 of this clause.

42.6.5 A breach of these obligations or restrictions may subject the Contractor to—

42.6.5.1 Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by NATO.

42.6.6 Subcontracts. The Contractor shall include this clause, including this paragraph 42.6.6, in subcontracts, or similar contractual instruments, for services that include support for NATO activities related to cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

ANNEX A: NCI AGENCY NON-DISCLOSURE DECLARATION

We, the undersigned ……(Company) duly represented by the named individual below (hereinafter "prospective Contractor") do hereby certify that we shall ensure that the following conditions be accepted and observed by all (prospective Contractor) employees working under RFS-CO-115699-ACPV.

_____Date
Full name (in block capitals) Signature

TO BE SIGNED BY THE PROSPECTIVE CONTRACTOR'S EMPLOYEES COLLABORATING WITH NATO THROUGHOUT THE ACPV / DYNAMIC SOURCING INITIATIVE.

I UNDERSTAND:
That I must preserve the security of all classified /commercial-in-confidence information which comes to my knowledge as a result of this collaboration with NATO and that I undertake to comply with all applicable security regulations to Solicitation #RFS-CO-115699-ACPV.

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

That I must not, without the approval of the General Manager of the NCI Agency, publish (in any document, article, book, CD, video, film, play, or other form) any classified /commercial-in-confidence information which I have acquired in the course of my work under RFS-CO-115699-ACPV.

That, at the end of Dynamic Sourcing process and after contract award decision is made, I must surrender any official document or material made or acquired by me in the course of my work under RFS-CO-115699-ACPV, save such as I have been duly authorized to retain.

That the provisions of the above Declaration apply not only during the period of Dynamic Sourcing under RFS-CO-115699-ACPV, but also after a potential contract is issued and that I am liable to prosecution if either by intent or negligence I allow classified/commercial-in-confidence information to pass into unauthorized hands.

Parties agree that in case of breach of the obligations stipulated in this declaration by the individual who undersigned this, NATO can only claim damages from the Contractor itself under Solicitation RFS-CO-115699-ACPV (in its capacity of employer of the undersigned), and not from the undersigned. This does not affect other rights of the NATO under Solicitation RFS-CO-115699-ACPV.

ANNEX B: SERVICE LEVEL AGREEMENT (SLA) FOR THE PROVISION OF REACH LAPTOPS IN ACCORDANCE WITH ARTICLE 41 OF THESE TERMS AND CONDITIONS

Introduction

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

Parties

The REACH capability will be provided by the Purchaser to support the Contractor Team under Contract No CO-115699-ACPV.

General Overview

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

- Provision of REACH capability for the Contractor Team;
- General levels of response, availability, and maintenance associated with the REACH capability;
- Respective responsibilities of the Purchaser and the Contractor Team.

These provisions shall be in effect for an initial period of three years from the effective date of the Contract or until the end of Contract No CO-115699-ACPV, whichever occurs first. It can be extended based on a mutual agreement between the Parties.

Provided Capability

References

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

[TBD]

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

Scope

- As described in reference Service Descriptions above.

Aim

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

Limitations

- The use of the REACH capability requires a NATO Security clearance at NATO SECRET level. Proof of the users' security clearances will be provided to the Purchaser.
- The exchange and collaboration of information is provided through e-mail and Instant Messaging.
- Direct printing capability is not provided, but can be arranged through an extension of this contract requested by the Contractor's Team.
- In case of any problems which cannot be solved remotely from the service desk (The Hague, NLD), the equipment shall be sent to NCIA, The Hague at the Contractor's expenses. Any damages resulting from inappropriate operation or operation in harsh environment or adverse weather conditions, as well as a loss of the system shall be compensated by the Contractor.
- A maximum of two users can be configured to share one REACH laptop capability.

Assumptions

The following assumptions apply to this Agreement:

- Any support provided by Purchaser is documented in the service descriptions above
- Security violations of the non-NCIA REACH users are investigated through their local security officers/managers applying NATO rules (CM(2002)49, NCIA (CapDev)AD3-2, and NCIA(CapDev)NR SECOPS).
- Required changes to this Agreement and/or the provision of the REACH capability will be jointly assessed and the implementation agreed between the Parties. The implementation of changes may have an impact on the charges which will be handled through an update of this Agreement.

Roles and Responsibilities

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

- Contractor Team will receive [TBD] REACH terminal.
- The Purchaser will provide the REACH capability and related services.

Points of Contact

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

Purchaser's responsibilities

The Purchaser will:

- Provide to the Purchaser the necessary documentation required for the activation of user accounts and certifications;
- Provide the REACH capability including basic end-user training (1.5-hour duration) and deliver the REACH laptop(s);
- Set up and maintain the project web-portal at NR level;
- Provide introduction to the management of the portal (1-2 hours) and service desk for the portal on-site at NCIA, The Hague or through electronic media;
- Grant temporary use of REACH hardware and the software licences for the contracted period.

Contractor Team Responsibilities

The Contractor Team shall:

- Sign and return to the Purchaser the required security documentation;
- Provide the internet access required for Remote Access via NCIA REACH;
- Be responsible for the backup of files and data of the REACH on NR accredited media on an authorized Removable Storage Device provided by service provider;
- Ensure that Contractor personnel operating the REACH units possess security clearance of a minimum of NS;
- Provides Security clearance for up to and including NS for the personnel using the REACH capability;
- Provides the contact details of the local Security Officer/Manager and the commitment to apply NATO rules as defined in (CM(2002)49, NCIA (CapDev)AD3-2, and NCIA(CapDev)NR SECOPS)for the investigation;
- Return the equipment at the end of the Agreement at its expenses to the Purchaser;

- Not use the equipment for any other purposes than the purpose set out herein;
- Not lend, rent, lease and/or otherwise transfer the equipment to a third party;
- Not copy or reverse engineer the equipment.

Hours of Coverage, Response Times & Escalation

- As described in the service descriptions above.

Incidents

- As described in the service descriptions above.
- Resolution of disagreements

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

Changes

- For any changes of the REACH capability which will be required to be made during the term of this Agreement, the Purchaser will notify the Contractor CISAF Team at least one week prior to the event and inform about the required consequences.
- Any changes concerning the elements provided by the Contractor Team shall be communicated to the NCIA Service Desk at least one week prior to the event.

Maintenance

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

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK II PART IV

STATEMENT OF OBJECTIVES

Table of Contents

1 ACPV Background and Strategic objective

The NATO Enterprise is comprised of numerous NATO Entities and points of presence on which NATO Consultation, Command, and Control (C3) capabilities and services must run securely, to fulfil NATO's strategic goals and objectives and to conduct NATO's daily business process activities, operations, training and exercises.

Allied Nations have communicated a priority requirement with North Atlantic Council (NAC) tasking for mature, Enterprise-wide Asset, Configuration, Patching, and Vulnerability (ACPV) management and identified these areas as key enablers to defend its CIS and respond to incidents in a timely manner. NATO must be able to efficiently and effectively identify, prioritize, de-risk, fix and report cybersecurity issues, in order to make risk-based mitigation decisions and implement the mitigation in the most expeditious means possible, before vulnerabilities can be exploited by an adversary.

While Asset and Configuration management are not specifically cyber security functions, rather foundational ICT functions, they constitute a fundamental source of information to enable proper risk management and ensure efficient and effective vulnerability management and management of other key cybersecurity functions (e.g. network monitoring, intrusion detection) that directly impact NATO's cyber resilience.

The full ACPV ambition and vision can be summarized as follows:

- An Enterprise-wide 'Single Source of Truth' for information on assets, configurations, patching and vulnerability status of the larger ICT infrastructure; This shall support the required visibility to cyber security functions, with an initial focus on supporting a risk-informed Vulnerability Management function ("ACP for V").
- Seamless view of ACPV data in the NATO Enterprise;
- Mature management of foundational processes; established ACPV processes Enterprise-wide, which include localised and fragmented services;
- Necessary internal skills and work experience in managing assets, configurations, and patching with a cybersecurity focus.

The business benefits aimed to be realized are the following:

- Faster detection and adequate response to cyber vulnerabilities
    - Improved situational awareness with more accurate understanding and tracking of the level of control the organization has on cyber threats and more accurate identification of all technology systems in the NATO enterprise
    - Better identification of any blind spots in the NATO IT or OT environments
- Faster and better responses to security alerts and crises or incidents
    - Improved determination of the extension and severity of incidents
    - Improved determination of impact of actions during resolution of incidents

    - Reduction of help desk response times
- Visibility on completeness, accuracy and reliability of all ACPV data across the enterprise.
- Provision of detailed reports to security audits

Benefits not directly related to cyber resilience but to foundational IT service management:

- Increasing the efficiency and reliability of other IT service management processes by providing them with accurate information about configuration items and assets
- Provision of detailed system information to financial teams, audit teams, logistics teams
- Reduction of unwanted costs
- Identification of how many software licenses are actually used in relation to how many have been paid for. This is both a financial and legal side benefit.
- Improved obsolescence management

2 Goals of this procurement exercise

This procurement exercise focuses on one key aspect of the overall ACPV initiative.

NATO intends to actively engage with Industry to contract design and delivery of an “Enterprise ACPV Service” that will bring together ACP data and insights from management systems and tools from the local NATO Entities and will allow cyber security functions across the Enterprise to interface with, access, and dynamically query this asset and configuration data. This new service will be built on top of, and integrate with, existing asset, configuration and patching capabilities across NATO.

The procurement exercise also includes the design and documentation of a NATO ACPV Enterprise framework, which defines global common practices to comply with, based on existing practices and possible foreseen ones, so to facilitate smooth aggregation and amalgamation of data in a way that can eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on asset, configuration and patch management through a federated approach.

3 Three-tier high level reference model for ACPV

In order to better describe the goal, outcome, scope, objectives, positioning and context of the expected Enterprise ACPV service, the following indicative model is presented. This reference model is presented to illustrate and position the envisioned Enterprise ACPV service within the overall ACPV vision.

This model is based on a three-tiered model described in the United States National Institute of Standards and Technology (NIST) Special Publication SP-1800-5A[1].

The model describes how technology asset and configuration information can be viewed centrally, aggregated and enriched on an enterprise level to support cyber security and other non-cyber security functions. In the context of this paper, the scope of asset management is the financial and logistical details related to technology, while configuration management refers to where technology (technical data, design, development) information is accounted for together along with its change information,

Three tiers are introduced as a way to improve the visibility of technology asset information on the enterprise level:

- Tier 1 – a function which aims to centralize, aggregate and enrich technical, ownership, contextual and security information about technology assets in order to support other cyber functions;
- Tier 2 - a multitude of systems and inventories maintained by teams within all the technology services providers throughout an enterprise
- Tier 3 – all logical and physical assets that are owned by an enterprise

The Enterprise ACPV service, which is the goal of this procurement exercise, sits within the Tier 1 of the model. Tier 2 and Tier 3 cover asset, configuration, patch, and vulnerability management capabilities being executed with each of the NATO Enterprise entities.

The model should be understood as a reference for the description of the expected service and is by no means prescriptive. Bidders are welcome to propose alternative models or improvements to the one used in this statement of objectives if they deem that those improvements or alternatives better illustrate the challenge of addressing ACPV within the NATO Enterprise context.

Figure 1 shows the conceptual three tier model applied to the NATO Enterprise.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf

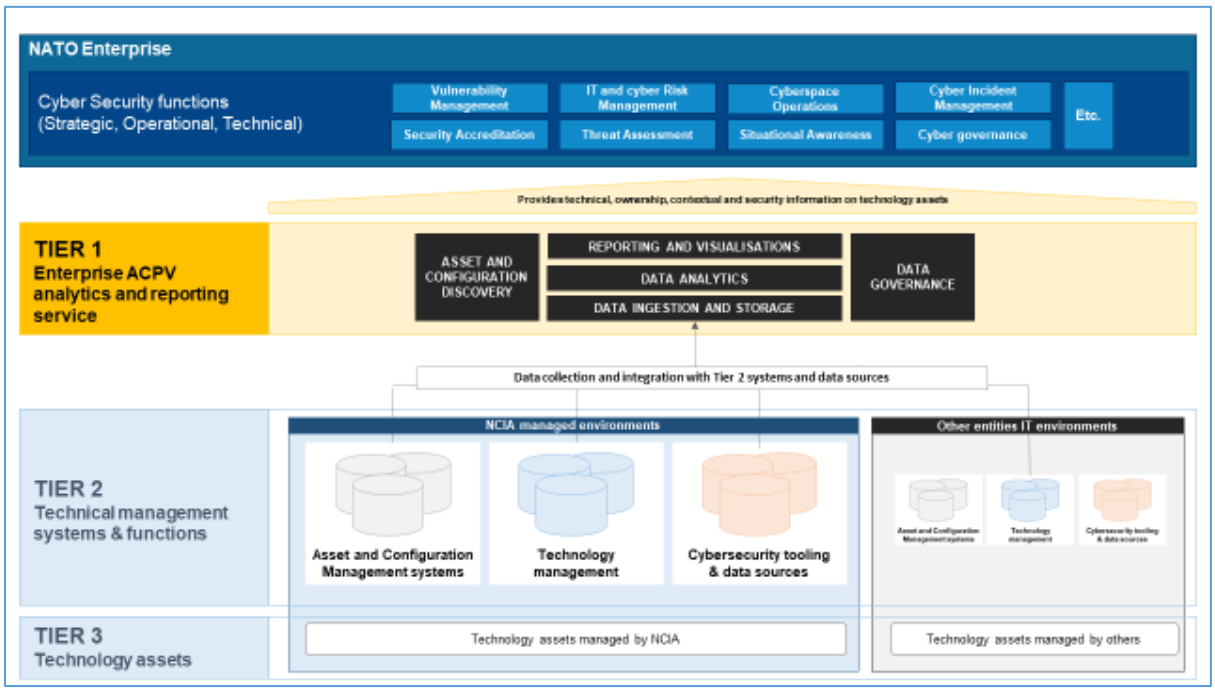

Figure 1: 3-Tier Concept for Enterprise ACPV Service

At the Tier 1 layer, visibility on technology assets will be brought together along with the following key contextual information and other required attributes to be specified, originating from Tier 2 and Tier 3:

Technical information	The technical information on IT assets is usually captured by configuration management systems, typically in a Product Life Cycle (PLM) system. These systems are used to facilitate the operational use of assets and focus on all relevant technical components that are in scope. Practically, a combination of multiple tools is in place to support operations and management of the assets on each of these levels. It is important to note that completeness and accuracy should be monitored to ensure a comprehensive coverage of all environments and the relevant information is captured in a reliable, up-to-date fashion.
Ownership information	To ensure proper management of the assets, it is required that ownership and responsibilities are clearly defined. Ownership of technology assets is typically allocated on at least two levels: technical ownership and business ownership. Technical ownership includes the tasks that revolve around ensuring the proper, ongoing usability of the asset. This includes – but is not limited to – for example: ensure proper patching, monitoring, tracking, etc. The business owner of the asset is a person or entity with the accountability and authority to manage a risk. Usually, the business owner has a more senior position within the organisation to ensure proper mitigation of the identified risks.
Business context	Contextual information provides details on the business processes supported by the assets provides, how it relates to other assets, how important the asset is, etc.
Security information	Each cyber security service generates information about specific cyber security controls they manage on the technology assets within their scope. Examples of

	useful information sources include: vulnerability scan results, accreditation status, threat intelligence, cyber security risk register, etc.

The following functional components are envisaged as part of the model at Tier 1:

Reporting and visualisations - provides visibility on the technology landscape through dynamic dashboards, custom reports or self-service interfaces that give access to information and insights provided through data analytics, and/or that give direct access to some raw data sources. It directly interacts with the function's stakeholders and the reporting and visualisations will be based on the requirements defined by them.

Data analytics – performs multiple operations on the different data sources to transform raw data into usable and actionable information and insights. It will provide advanced data filtering, sorting, searching, enrichment, joining, transforming and other functionalities to build manual and/or automatic data flows that support the reporting and visualisations offered to the stakeholders of the function.

Data ingestion and storage – interfaces with multiple Tier 2 systems and provides the ability to: access multiple data sources, perform initial data preparation activities to filter out data that is not relevant for data analysis or reporting & visualisation. Metadata management will capture information about the ingested data.

Data governance – relates to multiple aspects to ensure the quality, confidentiality, usability and other aspects of the data and information that will be handled by the function. Each of the Tier 2 data sources will require governance to allocate ownership of the data, perform data classification, manage security and access, retention management, etc.

Asset and configuration discovery – validates and/or enriches data sources received from Tier 2 systems and capabilities. This building block describes the functionality to scan internal and external networks and discover connected assets and relevant information (e.g. open ports, screenshots, service identification, operating system, websites, etc.).

4 Boundaries between the Enterprise ACPV service and other ACPV activities within Enterprise entities

As described in the previous section, the Enterprise ACPV Service is positioned at the Tier 1 layer, which sits above functions that are executed within the various local NATO Entities. These local Enterprise entities are responsible for implementing asset, configuration and patching management at the Tier 2 and Tier 3 layers, as well as programmes and projects to improve them.

The Enterprise ACPV Service is, therefore, a new effort over and above ongoing work in Asset and Configuration Management and Patch Management within NATO entities. The Enterprise ACPV Service is complementary to, while staying separate from, these efforts.

Complementary, but separate from, the Enterprise ACPV service effort, are parallel efforts underway to improve local NATO Entities' existing Asset, Configuration, Patching, and Vulnerability management solutions. While improvements to local NATO Entities' existing Asset, Configuration, Patching, and Vulnerability management solutions are not in scope of

this procurement exercise, direct integration to these (heterogeneous) systems in accordance with existing security policies is needed and included in the service. Local Entity Configuration Management functions, in particular, are key inputs to the Enterprise ACPV service. These provide the details related to decomposition and change status of assets, including the patch levels.

The Enterprise ACPV Service will take into consideration any the current state and any planned improvements of Tier 2 and Tier 3 systems across the Enterprise, integrating data coming from various sources to ensure that data is consolidated, harmonized, and offers a holistic view of the Enterprise scope.

Over time, enhancements to Asset, Configuration, Patching, and Vulnerability management in local Entities is expected to reduce dispersed and differently-formatted the situation is across the Enterprise, making the agglomeration of this information in the Enterprise ACPV Service more and more effective.

5 Goal and Expected Outcome of the Enterprise ACPV Service

The key goal of the ACPV Enterprise Service is to improve the NATO Enterprise cyber security posture by building, maintaining and providing a ‘Single Source of Truth’ for information on assets, configurations, patching and vulnerabilities. The service will be used primarily for Cyber security Vulnerability management, but will be available to various stakeholders with different use cases, with data compartmentalisation and role-based profiles taken into account. It will be an aggregator and organizer of contents/information. The data sources (good or bad) will be the underpinning asset and configuration management databases.

The expected outcome of the Enterprise ACPV Service is to provide users with enriched and consolidated information about technology assets with the ability to perform analysis, visualisation, and reporting.

6 Service Objectives

NATO intends to engage with industry to obtain the optimum service solution to achieve the desired goal and outcome for the Enterprise ACPV Service. Therefore, this Statement of Objectives document presents a set of service objectives in order to describe NATO’s ambition. Rather than prescribing a service with a fixed set of requirements, the dynamic sourcing approach allows for a collaborative series of engagements with industry to co-develop the desired solution against NATO’s stated objectives. It is desired that the ACPV Enterprise Service meets the following service objectives mandatory objectives.

Table 1: Service objectives

1		Provide users with enterprise visibility on technology assets, their ownership, context within the organisation and their security status	Overall service
	1.1	Provide users with visibility on technical information about technology assets	Overall service
	1.1.1	Provide users with visibility of technical asset details and configuration from technology management systems	Overall service
	1.1.2	Provide users with visibility of data and information about (privileged) identity and access management of technology assets	Overall service
	1.1.3	Provide users with visibility of technical log data from technology assets	Overall service
	1.2	Provide users with visibility on ownership information about technology assets	Overall service
	1.2.1	Provide users with visibility of information about who manages the technology asset	Overall service
	1.2.2	Provide users with information about who the risk owner(s) are for the asset	Overall service
	1.2.3	Provide users with information about who the business owner(s) is for the asset	Overall service
	1.3	Provide users with contextual information about technology assets	Overall service
	1.3.1	Provide users with information about the function and importance of the technology asset	Overall service
	1.3.2	Provide users with information about the security accreditation status of technology assets	Overall service
	1.3.3	Provide users with information about the relationships between technology assets (logical and technical)	Overall service
	1.3.4	Provide users with information about the network context of assets (e.g. exposure to internet, security zone, etc.)	Overall service
	1.4	Provide users with security information about technology assets	Overall service
	1.4.1	Provide users with vulnerability information about technology assets	Overall service
	1.4.2	Provide users with data and information about vulnerability mitigating actions	Overall service
	1.4.3	Provide users with data and information about anti-malware protection of assets	Overall service
	1.4.4	Provide users with security exception information for technology assets	Overall service
	1.4.5	Provide users with security incident information for technology assets	Overall service
	1.4.6	Provide users with cyber threat information related to technology assets	Overall service
	1.4.7	Document when the last security audit occurred	Overall service
	1.4.8	Allow alarms or alerts to be created to remind of the need for a security audit	Overall service
	1.5	Provide users with visibility in different technology asset types	Overall service
	1.5.1	Provide users with information on physical servers and virtual machines	Overall service
	1.5.2	Provide users with information on OT / IoT / facility devices	Overall service
	1.5.3	Provide users with information on network components (e.g. router, switches, firewalls, etc.)	Overall service
	1.5.4	Provide users with information on IT services	Overall service
	1.5.5	Provide users with information on (web) applications and middleware	Overall service
	1.5.6	Provide users with information on software supply chain (e.g. software bill of materials)	Overall service
	1.5.7	Provide users with information on databases	Overall service
	1.5.8	Provide users with information on mobile and end user devices	Overall service
	1.5.9	Provide users with information on cloud based services	Overall service
2		Integrate with the Tier 2 data sources (management systems) as described in the reference scenario in Book II-Part IV-Statement of Objectives and display their data through a centralized interface	Data ingestion and storage
	2.1	Handle and store classified information in a secure manner	Data ingestion and storage
	2.2	Retain historical data for the duration that stakeholders require to meet their use cases	Data ingestion and storage
3		Be able to actively perform asset discovery on networks to identify online technology assets	Asset and configuration discovery
4	4.1	Perform advanced data engineering and analytics in order to meet the use cases and requirements of stakeholders	Data analytics
	4.2	Join, aggregate and transform data from multiple data sources to create enriched datasets	Data analytics
	4.4	Provide support from data analysts that can develop data, analysis, transformation and visualizations based on the requirements from the end user.	Data analytics
5		Produce advanced reports, dashboards, alerting or self-service portals to meet the use cases and requirements of stakeholders	Reporting and visualisations
	5.1	Other cyber capabilities are able to easily consult and access the information and produce advanced reports or dashboards themselves	Reporting and visualisations
6		Keep the data and information on technology assets up-to-date and accurate	Overall service
	6.1	Make use, where possible, of automation to keep the data and information up-to-date	Overall service
7		Perform data governance for the technology asset data in scope for the service	Data governance
	7.1	Maintain a common data model and data dictionary based on the information requirements from stakeholders	Data governance
8		Assess and report on data quality and trustworthiness of the information it provides to other capabilities	Data governance
9		Users have access to the requested information in less than 1 hour from the time it is requested. The data covers at least 95% of the known assets, is no more than 24 hours old and is at least 95% correct.	Overall service
10		Support all the technology asset types described in the reference scenario in Book II-Part IV-Statement of Objectives	Overall service

Table 2: Mandatory objectives

11			The service shall be resilient and ensure business continuity and disaster recovery					Overall service
	11.1			Technology solutions part of the service have geographic redundancy and off-site backups				Overall service
12			The service shall adhere to the NATO cyber security policies and requirements in accordance with the references provided in section 8.3 of this Statement of Objective					Overall service
	12.2			The least privilege and need to know principles shall be adhered to by the service in order to protect sensitive information and data				Overall service
13			The service shall be delivered as a managed service in accordance with the ITIL service management framework					Overall service
	13.1			The service shall be delivered in accordance with the ITIL service management framework. Contractors may apply other service management frameworks in addtition to ITIL if they deem it necessary.				Overall service
	13.2			The contractor shall manage the technology solutions required to meet the functional objectives				Overall service
		13.2.1			The contractor shall manage the software			Overall service
		13.2.2			The contractor shall manage the middleware and databases			Overall service
		13.2.3			The contractor shall manage the hosting infrastructure			Overall service
		13.2.4			The contractor shall manage the information security of the solution			Overall service
	13.3			The service shall have an availability of at least 99%				Overall service
14			It shall be possible to make changes to the service					Overall service
	14.1			The contractor shall provide requirement management services				Overall service
	14.2			The contractor shall provide change management services				Overall service
	14.3			The service shall be agile and meet changing reporting and information requirements from stakeholders				Overall service
	14.4			The service shall provide the option to add new Tier 2 data sources				Overall service
	14.5			The service shall allow to add new assets				Overall service
	14.6			The service shall allow changes to the data model				Overall service
15			The service shall be described and delivered in accordance with the Performance Work Statement (PWS) Template in Book II-Part IV-Statement of Objectives-Annex A					Overall service
16			The contractor shall design and document a NATO Enterprise framework that will eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on asset, configuration and patch management through a federated approach.					Overall service

7 NATO context

The service to be implemented will need to take into account the current NATO asset and configuration landscape.

7.1 Structure of the NATO asset landscape

The NATO technology assets and associated management systems are described using the following technology asset stack.

Figure 2 below links the logical concepts of NATO systems, referred to as NATO Communications and Information Systems (CIS), as well as technical services to the underlying technical assets. This illustrates the linkage between technology components (assets) and the business systems and services that they enable. These connections should be visible within the Enterprise ACPV service.

Such a model can be built in many ways. For example, additional generic technical or logical data entities could be added (e.g. physical location, person, windows domain, security zone, etc.) and / or generic data entities can be further specified, for example a specification of “Technical Infrastructure” is a “Virtual Machine” or a “Physical Server”.

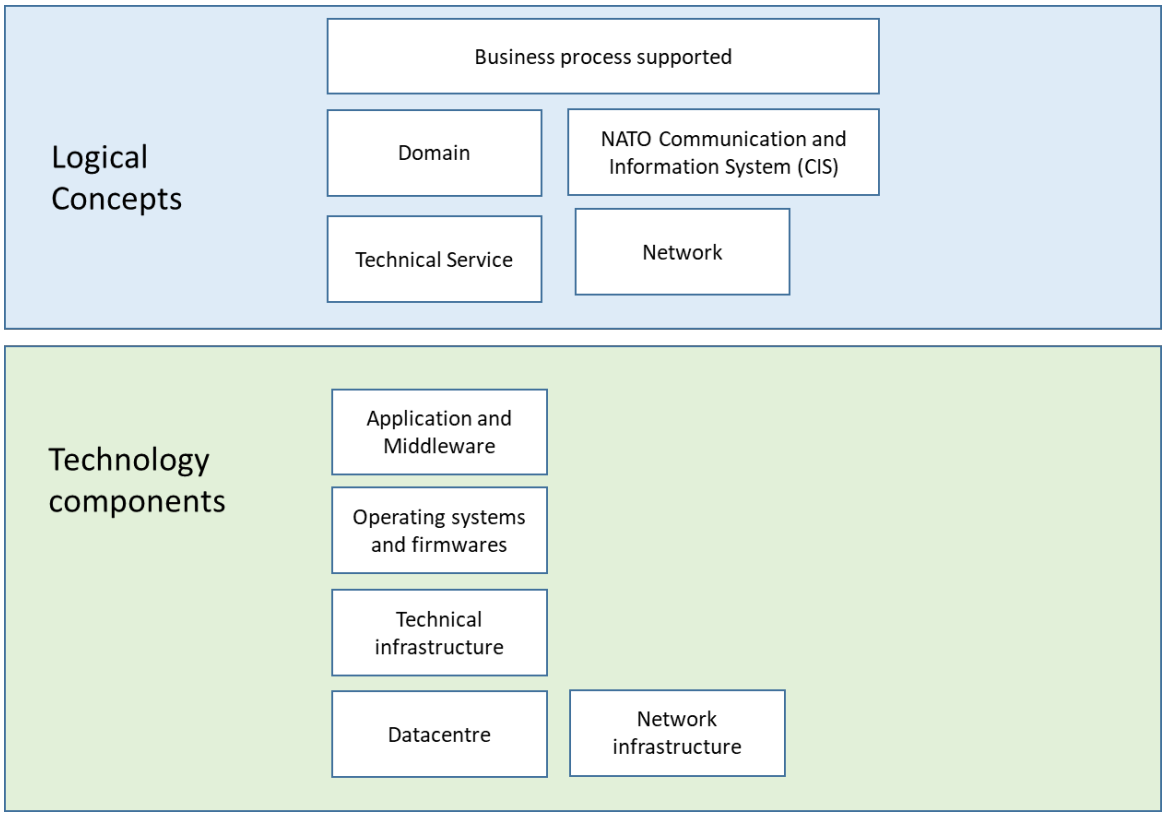

Figure 2 - Conceptual data model

7.2 Technology environment reference scenario

For the purpose of this dynamic sourcing exercise, and in order to allow bidders to propose and quote a solution at Sprint 2, a sample scenario representative of the NATO Enterprise technology environment is used. This table focuses on volumes and technologies, recognizing that cross-domain, access management, security constraints, data standardisation are additional dimensions.

A more detailed description of the NATO Enterprise specific environment will be shared with bidders during Sprint 3 of the dynamic sourcing exercise.

This sample reference scenario is described below. The asset types are considered Tier 3 assets, which are (mostly) managed by Tier 2 technology management systems.

Table 1: Technology environment reference scenario

	Asset Type	**Volume**	**Tier 2 systems where this information is tracked**
	Communication and Information System (CIS)	400	Accredited and non-accredited CIS systems

	Technical Service	200	Business, functional services
	Domains	250	SCCM
	Network	2000	IP ranges, DNS domains (internal and external). This is a logical construct on top of a network infrastructure (e.g., VLANS, FQDNs *.org). IT Environments on various classification levels.
	Application & middleware	1500 SW applications	Info captured in Global CMDB and/or manual excel sheets in which individuals are responsible for updating the content
		1200 pieces of middleware	Info captured in Global CMDB and/or manual excel sheets in which individuals are responsible for updating the content
	Operating systems and firmwares	25	Windows RHEL, Linux, VM Ware, Solaris, Cisco, IoT infrastructures Info captured in Asset management solutions (e.g., Oracle E-Business Suite for logistics and financial aspects of HW and SW)
	Technical Infrastructure	80K assets (endpoints) • 60K clients • 20K servers 80K users	These are assets with an individual IP address / range. (e.g. Servers, workstations, laptops) SCCM, Active Directory, BMC Remedy VMware vCenter tracking virtual devices Patch Manager for networking and technical infrastructure Info captured in Asset management solutions (e.g., Oracle E-Business Suite for logistics and financial aspects of HW and SW)
		>6000 IoT devices	VOIP phones, IP cameras, etc. Hardware components excluding network infrastructure. BMC Remedy, Azure/AWS Cloud Administration console

			Info captured in Asset management solutions (e.g., Oracle E-Business Suite for logistics and financial aspects of HW and SW)
	Network Infrastructure	5000 network components	Cisco Prime, VMWare Vcenter,Checkpoint SmartConsole,Azure/AWS Cloud Administration console Info captured in Asset management solutions (e.g., Oracle E-Business Suite for logistics and financial aspects of HW and SW)
	Datacentre	4	

~~A more detailed description of the NATO-specific Enterprise environment will be shared with bidders during Sprint 3 of the dynamic sourcing exercise in order to inform the eventual contract~~.

7.3 Classification domains

The systems and inventories across the Enterprise are of varying classification levels, accessed by different communities of interest, with variation of access policies in place.

Security classifications are applied to classified Information in order to indicate the possible damage to the security of NATO and/or its member Nations if the information is subjected to unauthorised disclosure. It is the prerogative of the originator of the classified information to determine or modify the security classification.

The security classification assigned determines the physical and CIS Security provided to the information in storage, transfer and transmission, its circulation, destruction and the Personnel Security Clearance (PSC) required for access. Therefore, both over-classification and under-classification shall be avoided in the interests of effective security as well as efficiency.

NATO security classifications and their significance are:

- COSMIC TOP SECRET (CTS) unauthorised disclosure would result in exceptionally grave damage to NATO;
- NATO SECRET (NS) unauthorised disclosure would result in grave damage to NATO;
- NATO CONFIDENTIAL (NC) unauthorised disclosure would be damaging to NATO; and
- NATO RESTRICTED (NR) unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

NATO security classifications indicate the sensitivity of NATO Classified Information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure.

The overall security classification of a document shall be at least as high as that of its most highly classified component. Covering documents shall be marked with the overall NATO security classification of the information to which they are attached. Where possible, component parts like paragraphs, enclosures, annexes, etc., of documents classified NR and above should be marked appropriately by the originator to facilitate decisions on further dissemination.

When a large amount of NATO Classified Information is collated together, the original security classification markings shall be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

NATO Publication C-M(2002)49-REV1 / PDN(2021)0002, “Security Within the North Atlantic Treaty Organization”, sets out the full policy and minimum standards for the security of NATO Classified Information, including the aforementioned key NATO Security Classifications, Special Designations, Markings and General Principals.

7.4 NATO security policies

The Enterprise ACPV service will need to comply with NATO security policies. Key policies are provided in Part 6 of ANNEX A – Performance Work Statement (PWS) and will introduce various constraints to be considered in the high-level solution. Detailed reviews of these documents will be needed as the solution becomes better defined.

ANNEX A

Performance Work Statement (PWS)

See separate MS Word document attached

“Book_II_Part_IV_Annex_A_Performance_Work_Statement_(PWS)_Template”

RFS-CO-115699-ACPV

ASSET, CONFIGURATION, PATCHING AND VULNERABILITY MANAGEMENT (ACPV) ENTERPRISE SERVICE

BOOK II, PART IV - ANNEX A

PERFORMANCE WORK STATEMENT (PWS)

[The content of this PWS template is subject to adaptation and refinement as a result of the collaborative discussions taking place during dynamic sourcing Sprints 2 and 3.]

Part 1

GENERAL INFORMATION

1.0 **GENERAL:** This is a ~~non-personnel~~ non-personal services contract to provide a NATO Enterprise Asset, Configuration, Patching and Vulnerability Management (ACPV) Service. The NCI Agency ~~shall~~ will not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to NATO.

1.1 Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform the NATO Enterprise Asset, Configuration, Patching and Vulnerability Management (ACPV) Service as defined in this Performance Work Statement except for those items specified as government furnished property and services. The contractor shall perform to the standards in this contract.

1.2 Background: The NCI Agency is procuring an Asset, Configuration, Patching and Vulnerability Management (ACPV) Service for the NATO Enterprise. The NCI Agency intends to contract for these service utilizing a Firm Fixed-Price (FFP) contract using a Best Value (BV) methodology through a Dynamic Sourcing (agile procurement approach).

1.3 Objectives: The key goal of the ACPV Enterprise Service is to improve the NATO Enterprise cybersecurity posture by building, maintaining and providing a 'Single Source of Truth' for information on assets, configurations, patching and vulnerabilities. The service will be used primarily for Cybersecurity Vulnerability management, but will be available to various stakeholders with different use cases. The outcome of the Enterprise ACPV Service is to provide users with enriched and consolidated information about technology assets with the ability to perform analysis, visualisation, and reporting.

1.4 Scope: This procurement is a contributor to the full ACPV ambition. Its primary scope is to provide a service to which cybersecurity functions across the Enterprise will interface, to access and dynamically query the asset, configuration, and patch information of the NATO Enterprise.

This service will provide the required visibility of ACP data to the cybersecurity functions at NATO Enterprise, with a special focus on vulnerability management (ACP for V). It will draw this ACP data from management systems and tools in the local entities, and will allow cybersecurity functions across the Enterprise to interface with, access and dynamically query the asset and configuration data of the NATO Enterprise. ~~This new service will be built on top of existing asset, configuration and patching capabilities across NATO.~~ This new service will be built on top of existing Asset, Configuration and Patching solutions across NATO; this service can be referred to as the "Enterprise ACPV Service."

1.4.1 The secondary scope of the ACPV Dynamic Sourcing exercise is to create a NATO Enterprise framework that will eventually support the needs of other key functional areas (e.g. wider IT service management, financial, audit, logistics, etc.) relying on

asset, configuration and patch management information through a federated approach.

1.5 Period of Performance: The period of performance shall be for three (3) Base Years of 36 months and two (2) 12-month option years. The Period of Performance reads as follows:

Base Years (Years 1-3)
Option Year I (Year 4)
Option Year II (Year 5)

1.6 General Information

1.6.1 Quality Control/Assurance: The Contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall comply with Quality Control requirements as laid out in Part 6 APPLICABLE MANUALS, DIRECTIVES, AND PUBLICATION.

1.6.2 Official Holidays: For planning purposes, the Purchaser will provide the Contractor with applicable list of NATO holidays per year.~~vary based on location. *[The Contractor shall provide this information as part of their proposed solution.]*~~

1.6.3 Hours of Operation: *[The Contractor shall provide this information as part of their proposed solution.]*

1.6.4 Place of Performance: *[The Contractor shall provide this information as part of their proposed solution.]*

1.6.5 Type of Contract: The NCI Agency will award a Firm Fixed-Price (FFP) contract using a Best Value (BV) methodology through a Dynamic Sourcing (agile procurement approach).

1.6.6 Security Requirements: The Contractor personnel performing work under this contract shall possess the appropriate level of security clearance required prior to contract award, and shall maintain the level of security required for the life of the contract.

NATO has multiple security domains which are associated with various elements of its infrastructure, the networks upon which systems are operated, and the data and information processed across them. For the purpose of this project, the following four security classification domains are involved:

(1) NU – NATO UNCLASSIFIED
(2) NR – NATO RESTRICTED
(3) NS – NATO SECRET
(4) CTS – COSMIC TOP SECRET

The contractor shall comply with Security requirements as laid out in Part 6 APPLICABLE MANUALS, DIRECTIVES AND PUBLICATION.

1.6.6.1 PHYSICAL Security: The contractor shall be responsible for safeguarding all NATO equipment, information and property provided for contractor use. *[The Contractor shall provide this information as part of their proposed solution.]*

1.6.6.2 *Key Control: The Contractor* shall establish and implement methods of making sure all keys/ access cards issued to the Contractor by the NATO are not lost or misplaced and are not used by unauthorized persons. *[The Contractor shall provide this information as part of their proposed solution.]*

1.6.7 Special Qualifications: *[The Contractor shall provide this information as part of their proposed solution.]*

1.6.8 Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the Purchaser's Contracting Officer (PCO) or Project Manager. The Purchaser's Contracting Officer (PCO), Project Manager, and other NATO personnel, as appropriate, may meet periodically with the Contractor to review the contractor's performance. At these meetings the Purchaser's Contracting Officer (PCO) and Project Manager will apprise the contractor of how the NATO views the contractor's performance and the contractor will apprise the NATO of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to NATO.

1.6.9 NCI Agency Project Manager: The Project Manager monitors all technical aspects of the contract and assists in contract administration. The Project Manager is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements; monitor Contractor's performance and notifies both the Purchaser's Contracting Officer (PCO) and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. The Project Manager will not commit NATO or accept changes in cost or price, estimates or changes in delivery dates. The Project Manager is not authorized to change any of the terms and conditions of the contract.

1.6.10 Contractor Key Personnel: The following personnel shall be considered as key personnel for the performance of the Contract: Contracts Manager and Alternate, Contractor Project Manager, Technical Lead, Test Director, Quality Manager, Service Delivery Manager. Without prejudice to other applicable stipulations of the contract, key personnel shall be subject to the below.

1.6.10.1 All key personnel assigned to this Contract shall remain working on the Contract for as long as required by the terms of the present Contract unless the Purchaser agrees to a replacement who is equal or better qualified.

1.6.10.2 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.

1.6.10.3 The Purchaser reserves the right to reject a Contractor's staff member after prior acceptance if the Purchaser determines during Contract performance that the individual is not providing the required level of support. The Purchaser will inform the Contractor in writing in case such a decision is taken, and the Contractor shall propose a replacement within fifteen (15) days after the Purchaser's written notification.

1.6.10.4 The Purchaser shall approve any replacement or additional key personnel according to the following procedure:

1.6.10.4.1 The Contractor shall provide the name(s) and qualifications statement(s) of a nominee(s) for review by the Purchaser a least twenty (20) days before the intended date of replacement or the date when the nominee(s) is/are required to start work under the contract. If the Purchaser accepts the nominations, this acceptance will be notified in writing to the Contractor, who will be authorised to assign the nominated personnel to the Contract on the date(s) established in the stated notification.

1.6.10.4.2 If the Purchaser considers a nominee or nominees to be inappropriate for the required services, the Contractor will be so notified and shall have not more than ten (10) days to submit alternate nominees.

1.6.10.5 Contractor Key Personnel qualifications:

1.6.10.5.1 Contractor Project Manager (CPM): The CPM shall have at least six years' experience as the PM for an effort of similar scope, duration, complexity and cost, including the application of a formal project management methodology ~~such as PRINCE2~~.

1.6.10.5.2 Technical Lead (TL): The TL shall possess a degree in engineering or computer science ~~or shall have equivalent work experience~~and have at least 7 years of experience as system engineer on similar project. ~~The TL shall: have at least seven years in engineering positions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use.; be a member of recognized professional body;~~The TL shall have at least seven years in communication information system design and integration of networking and communication component parts similar to those being utilized for the purpose of this contract.

1.6.10.5.3 Test Director: The Test Director shall have at least five years' experience in the design and execution of communication information systems tests. .

1.6.10.5.4 Quality Assurance Manager: The Quality Assurance Manager shall have at least seven years' experience in working with quality control methods and tools and have a broad knowledge of NATO Standards (e.g. STANAG 4107 Ed. ~~11~~ 12 and underpinning AQAPs), processes and procedures applicable to Quality Assurance (QA) and Quality Control (QC) in the industry. The ~~CQAR~~ CQAM shall be independent from the project team, report directly to the senior management and be involved in any project review, acceptance and delivery.

1.6.10.5.5 Service Delivery Manager (SDM): The Service Delivery Manager shall have at least six years' experience in the delivery of similar services. The SDM shall hold an ITIL v4 Managing Professional (ITIL MP) or ITIL v3 Expert certification.

1.6.10.5.6 Contracts Manager: ~~Contract Manager and Alternate. The Contract Manager and Alternate must have 24 semester hours in mathematical, engineering, and/or quantitative analysis courses; 15 or more years cost analysis experience; and familiarity with Defense Department Data Sources (e.g. cost and software data reporting, EVM).~~ The Contracts Manager must possess contract authority to make decisions on behalf of his/her employer and liaise directly with the Purchaser's Contracting Officer (PCO) to discuss any matters related to the resulting contract. The Contracts Manager must have prior Procurement experience, preferably working with a public organization, directly or indirectly.

1.6.11 Identification of Contractor Employees: All Contractor and Subcontractor personnel shall be required to wear NATO provided identification badges when on site. Contractors and subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signatures shall identify company affiliation.

1.6.12 Other Direct Costs *[The Contractor shall ~~provide this information~~ briefly describe the level of effort related to proposed other direct costs as part of their proposed solution.]*

1.6.13 Data Right: This paragraph supplements Article 10 Intellectual Property of Book II Part II Terms and Conditions. NATO has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be NATO owned and are the property of NATO with all rights and privileges of ownership/copyright belonging exclusively to NATO. These documents and materials may not be used or sold by the contractor without written permission from NATO. All materials supplied to NATO shall be the sole property of NATO and ~~may~~ shall not be used for any other purpose. This right does not abrogate any other NATO rights.

1.6.14 Organizational Conflict of Interest: 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 prospective contract work, or might be otherwise impaired, or the Contractor has an unfair competitive advantage. Conflict of interest includes situations where the capacity of an 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.

1.6.15 PHASE IN /PHASE OUT PERIOD: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the thirty (30) day, phase in/ phase out periods. During the

phase in period, the Contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

PART 2

DEFINITIONS & ACRONYMS

2. **DEFINITIONS AND ACRONYMS:**

2.1. DEFINITIONS: *[List any terms used within the PWS that require further definition. At a minimum, insert the definitions provided below.]*

2.1.1. CONTRACTOR. A Firm or Company awarded a contract to provide specific service to NATO. The term used in this contract refers to the prime.

2.1.2. CONTRACTOR'S CONTRACTS MANAGER. Also referred to as the Contracts Manager is a member of the Contractor's Key Personnel responsible for the management and administration of the contract.

2.1.3. PURCHASER'S CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of NATO. Note: The only individual who can legally bind NATO.

2.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5. DELIVERABLE. Anything that can be physically or digitally delivered, but may include non-manufactured things such as meeting minutes or reports.

2.1.6. SERVICE DELIVERY MANAGER (SDM). Member of the Contractor's Key Personnel involved in the seamless delivery of the service according to the agreed performance targets.

2.1.7. KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract: Contractor Project Manager (CPM), Technical Lead (TL), Test Director, Quality Assurance Manager, Service Delivery Manager, Contract Manager. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.8. PHYSICAL SECURITY. Actions that prevent the loss or damage of NATO property.

2.1.9. PROJECT MANAGER. An employee of the NCI Agency with the authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

~~2.1.10. QUALITY ASSURANCE. NATO procedures to verify that services being performed by the Contractor are performed according to acceptable standards.~~

2.1.10. CONTRACTOR QUALITY ASSURANCE MANAGER (CQAM). Member of the Contractor's Key Personnel ~~involved in any project review, acceptance and delivery~~

responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the life-cycle of the Contract.

~~2.1.12. QUALITY ASSURANCE Surveillance Plan (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.~~

~~2.1.13. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.~~

2.1.11. SUBCONTRACTOR. One that enters into a contract with a prime contractor. NATO does not have ~~privity of~~a contract relationship with the subcontractor.

2.1.12. TECHNICAL LEAD (TL). Member of the Contractor's Key Personnel responsible for the system design and integration~~involved in the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use.~~

2.1.13. TEST DIRECTOR. Member if the Contractor's Key Personnel ~~involved in~~ leading all test activities such as test planning, design, execution and test tools selection.

2.1.14. WORK DAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.15. WORK WEEK. Monday through Friday, unless specified otherwise.

2.2. ACRONYMS:

ACPV	Asset, Configuration, Patching and Vulnerability Management (ACPV)
AD	Agency Directive (NCI Agency)
AI	Agency Instruction (NCI Agency)
AQAP	Allied Quality Assurance Publication
BV	Best Value
~~CDR~~	~~Critical Design Review~~
CM	Contracts Manager
CoC	Certificate of Conformity
COTS	Commercial-Off-the-Shelf
COTS	Commercial of the Shelf
CPM	Contractor Project Manager
~~CQAR~~	~~Contractor Quality Assurance Representative~~
CQAM	Contractor Quality Assurance Manager
CSRS	Community Security Requirement Statement
ERM	Event Review Meeting
ETP	Event Test Plan
FFP	Firm-Fixed-Price
FOC	Final Operating Capability
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITS	Issue Tracking System
MTP	Master Test Plan
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information
~~NQAR~~	~~NATO Quality Assurance Representative~~
NQAM	NATO Quality Assurance Manager
OATM	Operational Acceptance Traceability Matrix
OCI	Organizational Conflict of Interest
ODC	Other Direct Costs
PCO	Purchaser's Contracting Officer
PDR	Preliminary Design Review
PFE	Purchaser Furnished Equipment
PFI	Purchaser Furnished Information
PIPO	Phase In/Phase Out
PM	Project Manager
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAM	Quality Assurance Manager
QAP	Quality Assurance Program
QAP	Quality Assurance Plan

~~QASP Quality Assurance Surveillance Plan~~
QC Quality Control
QCP Quality Control Program
QMS Quality Management System
RFC Request for Change
ROM Rough Order of Magnitude
RTM Requirements Traceability Matrix
SADS Security Accreditation Document Set
SAP Security Accreditation Plan
SISRS System Interconnection Security Requirements Statement
SIVP Security Implementation Verification Procedure
SME Subject Matter Expert
SOO Statement of Objectives
SoW Statement of Work
SSRS System-Specific Security Requirements Statement
SRA Security Risk Assessment
SRR System Requirements Review
STANAG Standardization Agreement
STVP Security Test & Verification Plan
STVR Security Test and Validation Report
TD Test Director
TE Technical Exhibit
TL Technical Lead
TRR Test Readiness Review
TV&V Test, Verification, Validation and Acceptance

PART 3

PURCHASER FURNISHED ~~MATERIAL~~PROPERTY

[This section should identify those items such as equipment, facility, external systems, information, software or service ~~property, information and/or services~~ that will be provided by NCIA for the contractor's use (without cost to the contractor) to allow them to ~~provide the required services, such as materials, facilities, training, etc. Examples provided below.~~meet the performance requirements of this contract. Initial list and any change of this list during implementation is subject to Purchaser acceptance]

3. PURCHASER FURNISHED ~~MATERIAL~~PROPERTY:

3.1 NATO will provide to the Contractor all the PFPs listed below at the location, in the quantities and during the planned period indicated in table below [contractor to insert table reference]. Any change of requirements (PFP description, location where it should be made available, quantity or planned period of use) shall be requested and approved by the Purchaser no later than 30 days prior to the need date.

3.2 Required PFP shall be grouped into the following categories
3.2.1 Purchaser Furnished Equipment
3.2.2 Purchaser Furnished Facility (e.g. access to sites, offices in NATO premises)
3.2.3 Purchaser Furnished External system (e.g. external interfaces that would be required for testing)
3.2.4 Purchaser Furnished Information (e.g. reference material, any type of NATO documentation)
3.2.5 Purchaser Furnished Software (e.g. SW used for vulnerability assessment)
3.2.6 Purchaser Services (e.g. REACH service)

~~workspace, workstations, office supplies, computer equipment, telephone, fax, electronic mail, reproduction facilities, and proper building access identification badges as required. NATO will furnish computer software which may be needed to accomplish tasks at the NATO site, subject to previous approval. NATO will provide access to appropriate reference material and databases necessary in the performance of this effort. The contractor will be provided the authority to access all information required to perform duties. NATO will provide coordination assistance to assist the contractor in accessing required information. NATO will provide the following information: access to relevant NATO organizations, information and documentation, manuals, texts, briefs and associated materials, as required and available.~~

~~3.1.1 PFE: Access to NATO databases and seats e.g., MS Word, Excel, PowerPoint, Access, [Insert applicable systems] and other databases required to perform this effort.~~

~~3.1.2 PFE: Access via internet using security protocols required by NATO to assure secure data transmission: [Insert applicable systems] required to perform this effort.~~

~~3.1.3 PFI: Required programmatic and financial information (verbal or written) required in order to complete deliverables.~~

PART 4

CONTRACTOR FURNISHED ~~MATERIAL~~PROPERTY

[This section is used to identify the materials and equipment that the contractor must provide. Examples provided below. Contractor may choose to provide this information as part of Exhibit 6]

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: *[The Contractor shall provide this information as part of their proposed solution.]*

4.2 Secret Facility Clearance: *[The Contractor shall provide this information as part of their proposed solution.]*

4.3. Materials. The Contractor shall *[The Contractor shall provide this information as part of their proposed solution.]*

4.4. Equipment. *[The Contractor shall provide this information as part of their proposed solution.]*

PART 5

SPECIFIC TASKS

[All of the required services to be performed under the contract should be described in sufficient detail here. This includes all general tasks required by NATO in accordance with the Exhibits to this document. The Contractor shall include here all required services as per their proposed solution]

5. Specific Tasks:

5.1. Basic Services. The contractor shall provide a ~~services~~ NATO Enterprise Asset, Configuration, Patching and Vulnerability Management (ACPV) Service.

5.2. [Task Heading.] *[The Contractor will insert the specific tasks in sequential order, i.e.,5.2, 5.3, etc.]*

PART 6

APPLICABLE MANUALS, DIRECTIVES, AND PUBLICATIONS

[Part 6 lists all applicable and reference documents to this contract. If applicable, new versions of the documents described here or new relevant documents will be provided at the time of contract award. Applicable documents are cited within the relevant parts of this PWS. Reference documents are provided for guidance]

6. REFERENCES (CURRENT EDITIONS)

6.1. NATO Standardization Agreements (STANAG) and Publications

6.1.1. STANAG 4107 Ed. 12 - Mutual acceptance of Government Quality Assurance and usage of the Allied Quality Assurance Publications (AQAPs) - and underpinning Allied Quality Assurance Publications ~~6.1.16.1.16.1.1 (AQAPs) – and underpinning AQAPs~~

6.1.2. STANAG 4427 Ed. 3 - Configuration Management in System Life Cycle Management – and underpinning Allied Configuration Management Publications (ACMPs)

6.1.3. STANAG 4728 Ed. 3 – System Life Cycle Management – and underpinning Allied Administrative Publications (AAPs)

6.1.4. STANAG 6001 Ed. 5, Language Proficiency Levels.

6.2. NATO Security Documents

6.2.1. C-M(2002)49-REV1 Security Within the North Atlantic Treaty Organisation, 20 November 2020

6.2.2. AC/35-D/2004-REV3 Primary Directive on CIS Security, 15 November 2013

6.2.3. AC/35-D/2005-REV3 Management Directive on CIS Security, 12 October 2015

~~6.2.4. AC/35-D/1017-REV3 Guidelines for Security Risk Management (SRM) of Communication and Information Systems (CIS), 29 June 2017~~

6.2.4. AC/35-D/2003-REV5 Directive on Classified Project and Industrial Security, 13 May 2015 (Corrigendum 1, 19 May 2015)

6.2.5. AC/35-N(2015)0022 (CISS) Rules of engagement for security audits of NATO CIS, 20 October 2015

6.2.6. AC/322-D(2004)0024-REV3-COR1 CIS Security Technical and Implementation Directive on the NATO PKI Certificate Policy, 28 March 2018 (Corrigendum 1, 30 April 2018)

6.2.7. AC/322-D/0048-REV3 Technical and Implementation Directive on CIS Security, 18 November 2019

6.2.8. AC/322-D/0030~~-REV5~~ REV6 ~~INFOSEC~~ Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS), ~~23 February 2011~~06 July 2023 – Approved draft – Official Publication under AC/322-D(2023)0042 (INV) is to be published in the incoming weeks

~~6.2.10. AC/322-D(2010)0058 Supporting Document on the Interconnection of NATO RESTRICTED CIS to the Internet, 21 December 2010~~

6.2.9. AC/322-D/0047-REV2 (INV) InfoSec Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009

6.2.10. AC/322-D(2019)0041 (INV) Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off the Shelf (COTS) Products into NATO, 1 October 2019

6.2.11. AC/322-N(2014)0158-ADD3 SECAN Doctrine and Information Publication (SDIP) 29, Selection and Installation of Equipment for the Processing of Classified Information (SDIP-29/2)~~Published as C3B Notice AC/322-N(2014)0158-ADD3 Selection and Installation of Equipment for the Processing of Classified Information~~, March 2015

6.2.12. C-M(2002)60 The Management of Non-Classified Information, 11 July 2002

6.2.13. C-M(2007)0118 NATO Information Management Policy, 11 December 2007

6.2.14. AC/35–D/2000–REV8 Directive on Personnel Security, 25 November 2020

6.2.15. AC/35–D/2001–REV3 Directive on Physical Security, 25 November 2020

6.2.16. AC/35–D/2002–REV5 Directive on the Security of NATO Classified Information, 25 November 2020

6.2.17. AC/322-D/0049-REV1 CIS Security Technical & Implementation Directive for Transmission Security (TRANSEC), 29 November 2018

6.2.18. AC/322-D(2004)0030 INFOSEC Technical & Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools, 17 May 2004

6.2.19. AC/322-D(2019)0021 Technical and Implementation Directive on Emission Security, 25 April 2019

6.2.20. AC/322-N(2011)0130 Guidance on the Marking of NATO Information, 16 June 2011

6.2.21. AC/322-D(2012)0011 INFOSEC Technical & Implementation ~~Guidance~~ Directive on Downgrading, Declassification and Destruction of System Equipment and Storage Media, 07 June 2012 (Corrigendum 1, 10 July 2012)

6.2.22. AC/322-D(2012)~~0011~~ 0012 INFOSEC Technical & Implementation Guidance on Downgrading, Declassification and Destruction of System Equipment and Storage Media, 07 June 2012

6.2.23. AC/322-D(2015)0029 CIS Security Technical and Implementation Guidance on Protecting Authentication Credentials, 27 November 2015

6.2.24. AC/322-D(2017)0016 Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products, 30 March 2017

~~6.2.27. AC/322-D(2019)0041 Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off the Shelf (COTS) Products Into NATO, 01 October 2019~~

6.2.25. AC/322-D(2019)0038 CIS Security Technical and Implementation Directive for the Security of Web Applications, 10 September 2019

6.2.26. AC/35-D/1019-REV1 Guidelines for the Security Evaluation and Certification of CIS, 12 December 2008

~~6.2.30. AC/322-D/0030-REV5 INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS), 23 February 2011~~

~~6.2.31. AC/322-D(2005)0040 INFOSEC Technical & Implementation Guidance for the Interconnection of Communication and Information Systems (CIS), 17 October 2005~~

6.2.27. AC/322-D(2004)0019 INFOSEC Technical and Implementation Guidance for the Protection of CIS from Malicious Software, 09 March 2004

6.2.28. AC/322-D(2005)0044 INFOSEC Technical & Implementation Guidance on Identification and Authentication, 26 October 2005

6.2.29. AC/35-D/1021-REV3 Guidelines for the Security Accreditation of Communication and Information Systems (CIS), 31 January 2012

6.2.30. AC/35-D/1017-REV3 Guidelines for Security Risk Management (SRM) of Communication and Information Systems (CIS), 29 June 2017

6.2.31. AC/35-D1015~~-REV3~~ REV4 (INV) Guidelines for the Development of Security Requirement Statements (SRSs), ~~31 January 2012~~05 July 2023

6.2.32. AC/35-D/1014-REV3 Guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for CIS, 31 January 2012

6.2.33. SDIP-28/1 NATO Zoning Procedures, December 2009

~~6.2.39. SDIP-29/2 Selection and Installation of Equipment for the Processing of Classified Information, March 2015~~

6.2.34. SDIP-293/1 Instructions for the Control and Safeguarding of NATO Cryptomaterial, March 2011

6.2.35. C-M(2014)0061 The NATO Enterprise Approach for the Delivery of C3 Capabilities and the Provision of ICT Services, 14 November 2014 with Annex from AC/322-D(2015)0014-REV4 (INV) dated 04 July 2023

6.2.36. AC/35-D/1034 Supporting Document on the Security Protection of NATO RESTRICTED Information, 25 May 2005

6.2.37. AC/322-D(2019)0032-REV2 (INV) NATO CLOUD COMPUTING DIRECTIVE, 12 March 2020

6.2.38. AC/322-D/0049-REV1 CIS Security Technical and Implementation Directive for Transmission Security (TRANSEC), 29 November 2018

6.2.39. AC/322-D(2007)0047 INFOSEC Technical and Implementation Supporting Document on the Use of Shared Peripheral Switches, 12 September 2007

6.2.40. AC/322-D(2006)0041-REV2 Directive on the Selection and Procurement of NATO Common-Funded Cryptographic Systems, Products and Mechanisms, 21 Sep 2018

6.2.41. AC/322-D(2017)0044-REV1 CIS Security Technical and Implementation Directive on the Procurement and Use of Commercial PKI Certificates for Internet Facing NATO Websites, 18 January 2018

6.2.42. AC/322-D(2018)0016 NATO Secure Voice Strategy, 14 March 2018

6.2.43. AC/35-D/1037 Supporting Document for the Security of Electronic Registry Systems, 25 July 2006

6.2.44. AC/322-D(2022)0058 (INV) Classified Cyber Defence Information Sharing

6.2.45. AC/35-D/1039 Guidelines on Business Continuity Planning for Communications and Information Systems (CIS), 8 October 2008

6.2.46. AD70-001 ACO Security Directive, 22 December 2021

6.2.47. AD70-005 ACO Communication and Information Systems (CIS) Security, 18 May 2021

6.2.48. NCIA/BRU/NES/SO/009/2022 Guidance for Contracting Companies Regarding the Submission of a Request For Visit (RFV) and Certificate of Security Obligation (CSO) Procedures and Security POCs for Accessing NCI Agency Sites and NATO Classified Information - Release No 3, 15 December 2022.

6.2.49. Add transportation and packing references

~~6.3. NCI Agency Policy Documentation~~

~~6.3.1. AD 06.00.03 Risk Management, latest published version~~

~~6.3.2. PDED 06.01.03 Govern Risk Management, latest published version~~

~~6.3.3. PDED 06.03.04 Test, Verification and Validation~~

~~6.3.4. AI 06.04.08 - Comments Collector, version 4.2~~

~~6.3.5. AI 16.31.04 – Requirements for the preparation of TRNP~~

~~6.3.6. AI 16.31.04 Annex A – Training POAP (Plan On A Page)~~

~~6.3.7. AI 16.31.04 Annex B – Training Feedback Form~~

~~6.3.8. AI 16.31.04 Annex C – Training Evaluation Report Form~~

~~6.3.9. AI 16.32.04 Annex A ABL Template~~

~~6.3.10. AI 16.32.05 Annex A PBL Template~~

~~6.3.11. AI 16.32.02 – Preparation of Engineering Change Proposal (ECP) forms~~

~~6.3.12. AI 16.32.02 Annex A – Engineering Change Proposal (ECP) Form~~

~~6.3.13. AI 16.32.03 – Preparation of Request For Deviation/Waiver (RFD/W) forms~~

~~6.3.14. AI 16.32.03 Annex A – Request For Deviation/Waiver (RFD/W) Form~~

6.3. International Standards and Specifications

6.3.1. ISO 9001:2015 – Quality Management Systems

6.3.2. ISO 10007:2017 – Quality Management - Guidelines for Configuration Management

6.3.3. ISO 27001-2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements

6.3.4. ISO/IEC/IEEE 15288:~~2015~~ 2023 – Systems and Software Engineering – System Life Cycle Processes

6.3.5. ISO/IEC/IEEE 29119-1:2022 – Software and systems engineering - Software testing

6.3.6. ISO/IEC 25010:2011 – Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models

6.3.7. IEEE Standard 15288-2:2014 – IEEE Standard for Technical Reviews and Audits on Defense Programs

6.3.8. IEEE Standard 1016-2009, IEEE Standard for information technology - systems design - software design descriptions;

6.3.9. ISO/IEC/IEEE 29148 - Systems and software engineering - Life cycle processes - Requirements engineering, 01 Dec 2011.

6.4. NCSC Security Settings Guides

6.4.1. Security Configuration Catalogue, NATO Cyber Security Centre v.1.25, June 2023

6.4.2. VLAN Usage for Logical Separation of Networks, v2.1, September 2010 (or newer version available at time of Contract Award)

~~6.6 Testing, Verification, Validation and Quality (TVVQ) Documentation~~

~~6.6.1. 1.5STANAG 4107, Mutual Acceptance Of Government Quality Assurance And Usage Of The Allied Quality Assurance Publications (AQAP), and all underpinning AQAPs;~~

~~6.6.2. AD 070-001 ACO Security Directive dated 28 Jan 2019;~~

~~6.6.3. ISO 9000:2015 Quality management systems — Fundamentals and vocabulary;~~

~~6.6.4. ISO 9001:2015 Quality management systems — Requirements;~~

~~6.6.5. ISO/IEC/IEEE 29119 Software Testing, parts 1 to 4;~~

~~6.6.6. ISO/IEC 25010-2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models;~~

~~6.6.7. IEEE Standard 15288.2:2014, IEEE Standard for Technical Reviews and Audits on Defense Programs;~~

~~6.6.8. IEEE Standard 1016-2009, IEEE Standard for information technology - systems design - software design descriptions;~~

~~6.6.9. ISO/IEC/IEEE 29148 - Systems and software engineering - Life cycle processes - Requirements engineering, 01 Dec 2011.~~

PART 7
EXHIBIT LISTING

7. **Exhibit List:**

7.1. Exhibit 1 – Performance Requirements Summary

7.2. Exhibit 2 – Deliverables Schedule

7.3. Exhibit 3 - Security Management/Information Protection

7.4. Exhibit 4 - Safeguarding of NATO Restricted Information

7.5. Exhibit 5 - Contractor Cyber Incident Management Plan

7.6. Exhibit 6 - Project Management

7.7. Exhibit 7 - Quality

7.8. Exhibit 8 - Testing, Verification and Validation

7.9. Exhibit 9 – Security Accreditation

7.10. Exhibit 10 – Training

7.11. Exhibit 11 – Technical Solution Design

EXHIBIT 1

PERFORMANCE REQUIREMENTS SUMMARY

[The Contractor shall provide this information as part of their proposed solution.]

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective (The Service required—usually a shall statement)	**Standard**	**Performance Threshold** (This is the maximum error rate. It could possibly be "Zero deviation from standard")	**Method of Surveillance**
PRS # 1. The contractor shall provide [*Insert an objective that relates directly to a mission essential required item, i.e., analysis of NATO Business Process and Agency Operating Models and the PWS paragraph number, i.e.*, PWS paragraph 5.5.]	The contractor provided *[Insert the standard that should be followed, i.e, analysis of NATO Business Process and Agency Operating Model.]*	*[Insert the minimum acceptable level of service, i.e., No more than one customer complaint per report.]*	*[Insert the method of surveillance (see listing below) and who performs, i.e., Validated Customer Complaint received by PM.]*
PRS # 2 *[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*
PRS # 3 *[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*
PRS # 4 *[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*	*[See example provided in PRS 1.]*

The following listing provides various types of Surveillance as examples to select from and should not be included on the final document:

Random Sampling: Appropriate for frequently recurring tasks. Evaluate randomly selected samples of the lot to determine the acceptability of the entire lot.

Random Inspection Guide, Method of surveillance, Lot size, Sample size, Performance requirement, Sampling procedure, Inspection procedure

100 Percent Inspection: Appropriate for tasks that occur infrequently. Inspect and evaluate performance each time task is performed

Periodic Surveillance: Evaluation of samples selected on other than 100% or statistically random basis. (i.e., monthly, quarterly, semi-annually etc.)

Validated Customer Complaint: Complaints must be validated.

NOTE: You may also identify any surveillance method used in the commercial market to survey the required service. (This will be discovered when market research is conducted).

EXHIBIT 2

DELIVERABLES SCHEDULE

[The Contractor shall provide this information as part of their proposed solution. This Exhibit lists any reports or documentation that is required as a deliverable to include the frequency, # of copies, medium/format and who/where it is to be submitted. A deliverable is anything that can be physically delivered but may include non-physical things such as meeting minutes. Note: All PWS deliverables (also listed in exhibit 6) should be included in this exhibit.]

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
[Insert the deliverable, i.e., the NATO Business Process and Agency Operating Models Report and the PWS paragraph number, i.e., PWS *paragraph* 5.5.*]*	*[Insert how often it is to be provided, i.e., by the 5th of every month, within 30 days of contract award, etc.]*	*[Insert the number of copies, i.e., 1 original and 2 copies, how often it is to be provided, i.e., by the 5th of every month, within 30 days of contract award, etc.]*	*[Insert the medium/format that the deliverable is to be provided in, i.e., paper (hard copy), CD in MS Word, DVD, Briefing Slides on CD, Excel Spreadsheet, etc.]*	*[Insert where the deliverable is to be delivered, i.e., Name of Activity, ATTN: POC, and Address.]*
[Continue to insert the deliverables in accordance with the example provided above.]	*[Same as above.]*	*[Same as above.]*	*[Same as above.]*	*[Same as above.]*
[Same as above.]	*[Same as above.]*	*[Same as above.]*	*[Same as above.]*	*[Same as above.]*

EXHIBIT 3

SECURITY MANAGEMENT/INFORMATION PROTECTION REQUIREMENTS

1. Security Management / Information Protection

1.1 The Contractor shall, upon request, provide to the Purchaser, a system security plan (or extract thereof) and any associated plans of action developed to satisfy the security requirements of Special Provisions clause, "Basic Safeguarding of Contractor Communication Information Systems (CIS)", in effect at the time the solicitation is issued or as authorized by the Purchaser's Contracting Officer (PCO), to describe the contractor's CIS/network(s) where NATO Information associated with the execution and performance of this contract is processed, stored, or transmitted.

1.1.1 The Contractor shall, upon request, provide the Purchaser with access to the system security plan(s) (or extracts thereof) and any associated plans of action for each of the Contractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), who process, store, or transmit NATO Information associated with the execution and performance of this contract.

1.2 The Contractor shall identify all NATO Information associated with the execution and performance of this contract. At the post-award conference, the Contractor and Purchaser Project Manager and Purchaser's Contracting Officer (PCO) shall identify and affirm marking requirements for all NATO Information to be provided to the Contractor, and/or to be developed by the Contractor, associated with the execution and performance of this contract.

1.3 The Contractor shall track all NATO Information associated with the execution and performance of this contract. The Contractor shall document, maintain, and upon request, provide to the Purchaser, a record of tier 1 level subcontractors, vendors, and/or suppliers who will receive or develop NATO Information and associated with the execution and performance of this contract.

1.4 The Contractor shall restrict unnecessary sharing and/or flow down of NATO Information associated with the execution and performance of this contract – in accordance with NATO marking and dissemination requirements and based on a 'need-to-know' to execute and perform the requirements of this contract. This shall be addressed and documented at the post-award conference.

1.5 The contractor shall develop and store all NATO technical data (e.g., source code) in a secure facility. The contractor shall prevent computer software, in the possession or control of non-NATO entities on non-NATO information systems, from having connections to the network through segregation control (e.g., firewall, isolated network, etc.) and document meeting this requirement in the contractor security plan.

1.6 The Contractor shall flow down the requirements of this clause to their tier 1 level subcontractors, vendors, and/or suppliers.

1.7 All deliveries should be annotated in the Project Implementation Plan (~~PMP~~ PIP).

EXHIBIT 4

SAFEGUARDING OF NATO RESTRICTED INFORMATION

Introduction

1. This exhibit is in accordance with the guidelines and requirements published by the Security Committee (AC/35) in support of NATO Security Policy, C-M (2002)49, and its supporting directives.

Background

2. This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract. This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

3. This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

Section I- Responsibility

4. Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by the Contracting Authority. The SO shall also act as the point of contact with the Contracting Authority or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

Section II – Personnel Security

5. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the facility security officer.

Section III – Physical Security

6. NR information classified NR shall be stored in a locked cabinet or Office Furniture (e.g. office desk drawer) within an Administrative Zone**,** Class I Security Area**,** or Class II Security Area. Information classified NR may also be stored in a locked cabinet, vault, or open storage area approved for information classified NC or higher shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet, or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone[1]).

[1] An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

7. NR information shall be handled in Administrative Zones or National equivalent to Class I or II security areas. NR information can be also held under personal custody.

Section IV- Security of Information

Control and Handling

8. Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

9. Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5, second sentence.

Reproduction

10. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

Destruction Requirements

11. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

12. Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

13. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

14. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transmission

15. The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

    a) moved by postal or commercial services;

    b) carried by Contractor's personnel; or

    c) transported as freight by commercial services.

Release

16. NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

17. Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the Contracting Authority.

Section V- Sub-Contracting

18. Sub-contracts shall not be let without the prior approval of the Contracting Authority.

19. Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

20. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

International Visits

21. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

Section VI- Handling of NATO RESTRICTED Information on Communication and Information Systems (CIS)

Security Accreditation of Communication and Information Systems (CIS)

22. Security accreditation shall be performed by the National Security Accreditation Authority (SAA) (or their delegated SAA) for all contractors' CIS that are used to handle (store, process or transmit) NATO RESTRICTED (NR) information. The security accreditation process shall ensure that the NATO's minimum security standards[2] are met.

23. This contract security clause contains the rules and regulations that shall be applied by the contractor's SO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the contractor as a result of the contract. This clause includes specific provisions to be satisfied by the contractor under delegation from the Contracting Authority for the accreditation of the contractor's CIS handling NR information. Under this delegated authority the contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the contractor's response in acknowledgement of the receipt and requirements of the Security Aspects Letter associated with the contract.

24. It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

25. The SO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

26. The following describes the minimum security requirements for handling NR information on contractors' CIS that shall be met:

[2] As described in the policy on Security Within the NATO and its supporting Directives on CIS Security

26.1 Identification and Authentication

26.1.1 An up-to-date list of authorised users shall be maintained by security management staff.

26.1.2 Credentials shall be established and maintained to identify authorised users.

26.1.3 Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.

26.1.4 Passwords shall be a minimum of 9 characters long and shall include numeric and “special” characters (if permitted by the system) as well as alphabetic characters;

26.1.5 Passwords shall be changed at least every 180 days. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.

26.1.6 The re-use of a number of previous passwords shall be denied.

26.1.7 The system shall provide only limited feedback information to the user during the authentication process.

26.1.8 Accounts that are no longer required shall be locked or deleted.

26.1.9 When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

26.2 Access Control

26.2.1 The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security-related documentation.

26.2.2 From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.

26.2.3 Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.

26.2.4 Access to security and system information shall be restricted to only authorised security and system administrators.

26.2.5 Access privileges shall be implemented to restrict the type of access that a user may be permitted (e.g., read, write, modify, and delete).

26.2.6 The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.

26.2.7 The system shall allow user-initiated locking of the user’s own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.

26.2.8 Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

26.3 Security Audit

26.3.1 An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:

- all log on attempts whether successful or failed;
- log off (including time out where applicable);
- the creation, deletion or alteration of access rights and privileges;
- the creation, deletion or alteration of passwords.

26.3.2 The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in humanreadable format either directly (e.g., storing the audit trail in human-readable format) or indirectly (e.g., using audit reduction tools) or both.

26.3.3 Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.

26.3.4 The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.

26.3.5 A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security violation).

26.4 Protection against Malicious Software

26.4.1 Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependant upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).

26.4.2 The virus/malicious code detection software shall be regularly updated.

26.5 Mobile Code

26.5.1 The source of the mobile code shall be appropriately verified.

26.5.2 The integrity of the mobile code shall be appropriately verified.

26.5.3 All mobile code shall be verified as being free from malicious software.

26.5.4 Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

26.6 Availability

26.6.1 Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

26.7 Import/Export of Data

26.7.1 Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.

26.7.2 All data imported to or exported from the CIS shall be checked for malware.

26.8 Configuration Management

26.8.1 A detailed hardware and software configuration control system shall be available and regularly maintained.

26.8.2 Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.

26.8.3 Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.

26.8.4 An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.

26.8.5 The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.

26.8.6 The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects i.e. any potential adverse affects of the modification on existing security measures, shall be considered and appropriate action taken.

26.8.7 The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.

26.8.8 The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.

26.8.9 Changes to the system or network configuration shall be assessed for their security implications/impacts.

26.8.10 The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

26.9 Security Management

26.9.1 Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.

26.9.2 The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

26.10 Approved products

26.10.1 An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

26.10.2 The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

26.11 Security Testing

26.11.1 The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

26.12 Transmission Security

26.12.1 NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using approved cryptographic products.

26.13 Wireless LAN

26.13.1 The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

26.13.2 NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

26.14 Virtualisation

26.14.1 When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

26.14.2 A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

26.14.3 Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

26.14.4 Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure. For example, a firewall shall not be virtualised.

26.14.5 The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

26.14.6 Access to the hypervisor functions shall be appropriately controlled.

26.14.7 The ability to “cut-and-paste” between virtual machines shall be appropriately configured and controlled.

26.14.8 The ability to create virtual machines shall be appropriately configured and controlled.

26.14.9 Virtual Machines shall be suitably de-commissioned after use.

26.14.10 Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

26.14.11 Virtual Servers and Virtual Workstations shall not be located on the same physical host.

26.14.12 Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be located on the same physical host as those operating in the LAN.

26.14.13 The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti-malware and Active Directory communication mode shall be allowed.

26.14.14 Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative account.

26.14.15 The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.

26.14.16 The SAN used to host Virtualisation operating at different security classifications shall be isolated onto separate Logical Unit Numbers.

26.14.17 Modifications to the 'Master Copy/Version' of a Virtual Machine shall be appropriately controlled.

26.14.18 Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

26.15 Interconnections to a CIS not accredited to handle NR information

26.15.1 Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" (current reference AC/322-D/0030-~~REV5~~ REV6) ~~and "Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet" (current reference AC/322-D(2010)0058)~~. These Directives may be obtained from the Contracting Authority.

26.15.2 Interconnection to another CIS, especially the internet, will significantly increase the threat to a contractor's CIS and therefore the risk to the security of the NR information handled by the contractor's CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process. Security requirements can also be found in the latest version of the NATO document entitled "Technical and Implementation Directive on CIS Security (current reference AC/322-D/0048-REV3). This Directive may be obtained from the Contracting Authority.

26.15.3 When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

26.16 Disposal of IT Storage Media

26.16.1 For IT storage media that has at any time held NR information the following sanitisation shall be performed to the entire storage media prior to disposal:

- EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives):
- overwrite with random data at least three times, then verify storage content matches the random data;
- Magnetic Media (e.g. hard disks): overwrite or degauss;
- Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of 10mm2 or less;
- Other storage media: seek security requirements from the Security Accreditation Authority.

26.17 Portable Computing Devices (laptops, tablets, etc)

26.17.1 Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR information that do not use approved encryption shall not be taken outside the contractor's premises unless held under personal custody. The term "drives" includes all removable media. Any authentication token and/or password(s) associated with the encryption product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

Physical Security of CIS Handling NR information

27. Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

28. CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

Security of NR Removable Computer Storage Media

29. Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle.

Use of CIS Equipment Privately Owned by Contractor's Personnel

30. The use of privately-owned equipment of contractor's personnel (hardware and software) for processing NR information shall not be permitted.

CIS Users' responsibilities

31. CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

Advice

32. Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

Audit/inspection

33. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor shall provide evidence of compliance with this ~~SoW~~ PWS Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.

EXHIBIT 5

CONTRACTOR CYBER INCIDENT MANAGEMENT PLAN

1. Contractor Cyber Incident Management Plan

1.1.1 The contractor shall deliver a Cyber Incident Management Plan (CIMP) that is aligned to cyber security controls in line with NATO Security Policy and its supporting directives. The contractor shall integrate the CIMP activities in the Project Master Schedule (PMS) part of the Project Implementation Plan (PIP).

1.1.2 The Contractor shall create, maintain and operate a formal incident response and forensic capability for protection of NATO Information residing on non-NATO Information Systems. The Contractor shall include the subcontractors and suppliers that perform support work that involves NATO Information.

1.1.3 The Contractor shall establish an incident-handling capability plan that consists of:

1) incident response policy and plan,

2) procedures for performing incident handling and reporting

3) guidelines for communicating with outside parties regarding incidents

4) incident team structure and staffing model

5) relationships and lines of communication between the incident response team and other groups, both internal and external

6) services the incident response team should provide, and

~~6.~~ 7) staffing and training the incident response team

1.1.3.1 The final approved Programme CIMP shall be in Adobe Acrobat format with a digital signature from the contractor cognizant authority.

1.1.3.2 If no approved Program CIMP currently exists between the contractor and NATO, then one must be created and submitted. If an approved Program CIMP already exists and sufficiently satisfies the CIMP requirements for the contract, then no new CIMP delivery is required. In such cases, the Contractor in consultation with the Purchaser shall only submit a Contract Letter to the Purchaser's Contracting Officer (PCO) stating that all CIMP requirements are satisfied by the existing Program CIMP.

1.1.4 The Contactor shall be prepared and report cyber incidents that result in an actual or potentially adverse effect on the Contractor CIS and/or NATO Information residing therein, or on a contractor's ability to deliver on the requirement.

1.1.5 The Contractor shall report status of the incident-handling capability including plan-of-actions for capabilities not at full operational status, and periodic operational status.

1.1.6 The Contractor shall provide status of a cyber-incident from first identification to closure as described in the ~~NCI Agency Special Provisions Clause, Cyber Incident Reporting~~ CIMP.

1.1.7 The contractor shall report cyber incidents for all section of the ~~SoW~~ PWS to the Purchaser as described in the NCI Agency Terms and Conditions, Cyber Incident Reporting.

1.1.8 The Contractor shall establish and document a digital forensics readiness plan, and upon an incident execute the plan on the Contractor CIS to include the collection, examination, analysis, and reporting.

1.1.9 The contractor shall use a community-developed, standardized specification language for representing and exchanging information in the broadest possible range for cyber-investigation domains, including forensic science, incident response, and counter terrorism.

1.1.10 The Contractor forensic team assessment as required shall initiate corrective actions to include securing identified vulnerabilities, improve existing security controls, and provide recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

1.1.11 Subject to the Purchaser's consultation with the Contractor's national cyber defense authority and/or as prescribed in the contractor's nation's Memorandum of Understanding (MoU) on Cyber Defence with NATO, the Purchaser reserves the right to examine and audit all records and other evidence sufficient to reflect proper program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of NATO Information. If the Purchaser identifies any security deficiencies during the audit, the contractor shall implement corrective actions to address the shortfalls identified during these assessments at its own expense within a timeframe agreed with the Purchaser. The Purchaser reserves the right to re-examine and audit evidence of the implemented corrective actions.

EXHIBIT 6

PROJECT MANAGEMENT

1.1 Project Organization

1.1.1 Purchaser Project Organization and Responsibilities

1.1.1.1 The Project will be managed and subject to review by the Purchaser who will be represented by the NCIA Project Management Team (PMT). The PMT will include NCIA functional elements, including Purchaser's Contracting Officer (PCO). It will be chaired by the NCIA Project Manager (PM).

1.1.1.2 The PMT will be responsible for reviewing the deliverables for the supervision of the implementation and for acceptance of the service. The PMT will constitute the interface with the Contractor.

1.1.2 Contractor's Responsibilities, Organization and Personnel

1.1.2.1 The Contractor shall establish a project management organization for the purpose of performing and managing the efforts necessary to satisfactorily discharge their responsibilities under this Contract. As a minimum, the contractor's project organization leadership team shall consist of the Contractor Project Manager (CPM), Technical Lead (TL), Test Director, Quality Assurance Manager, Service Delivery Manager, and Contract Manager as identified in the Key Personnel. Because of their role in coordinating with the Purchaser, all Key Personnel shall be fluent in English.

1.1.2.2 The Contractor shall also provide the necessary manpower and resources to conduct and support the management and administration of their operations to meet the overall objectives of the contract.

1.1.2.3 The Contractor shall apply the PRINCE2 or equivalent recognized project management methodology to the planning and delivery of the implementation of the service under this Contract.

1.1.2.4 Contractor shall provide highlight reports and attend project progress meetings as required.

1.1.2.5 During project execution, the project shall be controlled in accordance with the approved Project Implementation Plan (PIP). As part of the monitoring and control function, the Contractor shall advise the Purchaser at all times of potential problems and schedule risks.

1.1.2.6 Both the Contractor Project Manager and the Contractor Technical Lead identified below shall be considered as Key Personnel in accordance with the Special Provisions of this Contract. Because of their role in coordinating with the Purchaser, all Key Personnel must be fluent in English.

1.1.3 Contractor Project Manager (CPM)

1.1.3.1 The Contractor shall designate a CPM, who will direct and coordinate the activities of the Contractor's project team.

1.1.3.2 The CPM shall be the Contractor's primary contact for the Purchaser's PM and shall conduct all major project design, test, and status reviews.

1.1.3.3 The CPM shall be prepared at all times to present and discuss the status of Contract activities with the Purchaser's PM, Purchaser's Contracting Officer (PCO), or Technical Lead (TL).

1.1.4 Contractor Technical Lead

1.1.4.1 The Contractor shall designate a Technical Lead (TL) for the project. The TL shall lead the system analysis, design, development, integration, and follow-on efforts of the Contractor.

1.1.5 Contractor Test Director

1.1.5.1 The Contractor shall designate a Test Director for all test activities conducted under this Contract. The Test Director shall direct test planning, design and tools selection, establish guidelines for test procedures and reports, and co-ordinate with the Purchaser on test support requirements and manage the Contractor test resources.

1.1.6 Contractor Quality Assurance ~~Representative~~ Manager

1.1.6.1 The Contractor shall designate a qualified individual to serve as the Contractor Quality Assurance ~~Representative~~ Manager (~~CQAR~~ CQAM), who will act as the Quality Assurance Manager for activities under this Contract. The ~~CQAR~~ CQAM shall report to a separate manager within the Contractor's organization at a level equivalent to or higher than the PM.

1.1.7 Service Delivery Manager

1.1.7.1 The Contractor shall designate a qualified individual to serve as Service Delivery Manager who shall transition the service design into service and act as the service manager when the service is delivered

1.2 Project Implementation Plan (PIP)

1.2.1 Scope of the PIP

1.2.1.1 The Contractor shall submit a PIP that describes how the Contractor shall implement project/contract administration, including details of the controls that shall be applied to supervise Sub-Contractor performance. The plan shall also define the details of liaison amongst the Purchaser, the Contractor and any Sub-Contractors. The sections of a draft PIP shall be furnished with the quotation and its related documentation shall be the primary guideline in developing the PIP to be provided in accordance with the requirements set forth therein. Pending the approval of the PIP, the bid draft PIP sections shall constitute the documentation to which

reference shall be made on any question that may arise in the preparation of the PIP. After approval by the Purchaser, any new version of the PIP shall constitute the unique Contractor's reference for the project implementation.

1.2.1.2 The PIP shall consider all project implementation aspects, which include management provisions, facilities, schedules, personnel assignments, external relationships and project control. The PIP shall be in sufficient detail to allow the Purchaser to assess the Contractor's plans and capabilities in implementing the entire project in conformance with the requirements specified. The PIP to be prepared by the Contractor shall include as a minimum the following sections:

Section 1: Project Overview
Section 2: Applicable Documents
Section 3: Project Management
Section 4: Technical solution design and Integration
Section 5: Quality Assurance and Quality Control
Section 6: Testing, verification and validation
Section 7: Documentation
Section 8: Training
Section 9: Security Accreditation
Section 10: Project Master Schedule (PMS)

1.2.2 Project Overview

1.2.2.1 Section 1 of the PIP shall contain a Project overview, which shall provide an executive summary overview of the Enterprise ACPV service, summarizing the main features of each of the PIP sections and indicate how the Project will be executed during the full lifetime of the Project.

1.2.3 Applicable Documents

1.2.3.1 Section 2 of the PIP shall contain the list of documents or standards referenced by the other sections of the PIP.

1.2.4 Project Management

1.2.4.1 Section 3 of the PIP shall provide the Project Management Plan (PMP), which shall include:

1.2.4.1.1 The management structure of the Contractor's team.

1.2.4.1.2 A list of Key Personnel assigned to the Contractor's team and their respective roles, responsibilities and authority, as well as their qualifications, experiences and security clearances.

1.2.4.1.3 The PMP shall identify all major Contractor operating units and any Sub-Contractors and suppliers involved in the delivery of the capability, and a description of the portion of the overall effort or deliverable item for which they are responsible.

1.2.4.1.4 The PMP shall include a Project Breakdown Structure (PBS) that shall

contain the critical work elements (tasks) of the project and illustrate their relationships to each other and to the project as a whole.

1.2.4.1.5 The PBS shall be represented either as a hierarchical list, or mind map.

1.2.4.1.6 The PMP shall include the details of the Contractor's methodology for Project Control, including Project Reporting (Section 1.5.1) and Project Meetings (Section 1.5.2).

1.2.4.1.7 The PMP shall include the details of the Contractor's Risk Management approach.

1.2.4.1.8 The PMP shall include the details of the Contractor's Issue Management approach.

1.2.4.1.9 The PMP shall include the details of the Contractor's PFP management approach.

1.2.4.1.10 The PMP shall include the contact details of all Contractor and Sub-Contractor personnel.

1.2.4.1.11 The PMP shall include a current and maintained Calendar for all Contractor and Sub-Contractor resources, identifying any periods of leave, National or Official holidays.

1.2.5 Technical solution design and Integration

1.2.5.1 Section 4 of the PIP shall cover the Technical Solution Design and Integration aspects of the Project.

1.2.5.2 The Contractor shall include all the areas as detailed in Exhibit 11 of this PWS and present how the functional, performance and technical specifications of this PWS shall be met.

1.2.5.3 The Contractor shall include a Site Implementation Plan, detailing the strategy that will be followed to enable the successful implementation of the service at one or multiple sites to achieve acceptance.

1.2.5.4 The Contractor shall include a Service Transition Plan, detailing the strategy to successfully deploy service releases into required environment and set correct expectations on the performance and use of the new / changed service and plan service changes, manage risks related to new / changed / retired services.

1.2.5.5 The Contractor shall include a Service Management Plan, detailing the strategy for governance management and delivery of the services. In this plan, the Contractor shall describe how the performance requirements of exhibit 1 will be met for each identified service.

1.2.6 Quality Assurance and Quality Control

1.2.6.1 Section 5 of the PIP shall cover the Quality Assurance and Quality Control aspects of the Project, as specified in Exhibit 7 of this PWS.

1.2.6.2 This Section shall include the QA Plan (QAP), with details of how the

Contractor shall establish, execute, document and maintain an effective Quality Assurance (QA) program, throughout the Contract lifetime.

1.2.7 Testing, Verification and Validation

1.2.7.1 Section 6 of the PIP shall define the Contractor's Master Test Plan (MTP).

1.2.7.2 The MTP shall include a description of the allocation of personnel, testing strategy and the schedule to accomplish all the test and acceptance activities, up to and including Final Service Acceptance (FSA), as specified in Exhibit 8 of this PWS. Testing, Verification related to the accreditation process is specified in Exhibit 9.

1.2.8 Documentation

1.2.8.1 Section 7 of the PIP shall define all Documentation being delivered by the Contractor and all referenced documentation.

1.2.9 Training

1.2.9.1 Section 8 of the PIP shall define the Contractor's Training Plan.

1.2.9.2 The Training Plan shall include a description of the allocation of personnel, training strategy and the schedule to accomplish all the training activities, as specified in Exhibit 11 of this PWS.

1.2.10 Security accreditation

Section 9 of the PIP shall define the Security Accreditation Plan as specified in Exhibit 9 of this PWS.

1.2.11 Project Master Schedule (PMS)
Section 10 of the PIP shall define the Project Master Schedule (PMS).

1.2.11.1. The Contractor shall establish and maintain a Project Master Schedule (PMS) that contains all contract events and milestones for the Project.

1.2.11.2. The Contractor shall ensure all planned deliverables are completed in accordance with the Schedule of Supplies and Services (SSS) and that all deliverables are completed on or before the Effective Date on Contract (EDC) plus (+) dates in accordance with the SSS.

1.2.11.3. The PMS shall show all contractual deliverables, the work associated with them, and their delivery dates.

1.2.11.4. The PMS shall not be cluttered with events or tasks internal to the Contractor, unless they are of major importance to the Project.

1.2.11.5. The PMS shall be provided in Microsoft Project format. For each task, the PMS shall identify the start and finish dates, duration, predecessors, constraints, and resources.

1.2.11.6. The PMS shall provide network, milestone, and Gantt views, and identify the critical path for the overall project.

1.2.11.7. The Contractor shall produce a PMS Plan on a Page (PMSPOAP) representing the whole project as detailed in the PMS.

1.2.11.8. The PMSPOAP shall be produced in Microsoft Visio Format, and be updated on a monthly basis as part of the Project Status Reporting cycle.

1.3 Documentation

1.3.1 The Contractor shall submit all documents listed in the following table based on the timelines defined as EDC+NN weeks.

NOTE: Completion dates are indicative to be proposed by the Offeror, unless dependent on event (eg. Testing events)

Serial	Name	Description	PWS Reference	To be completed by	Format
1	DPIP	Draft Project Implementation Plan	Exhibit 6	BID	DOCX
2	PMP	Project Management Plan	Exhibit 6	EDC+2 weeks	DOCX
3	RISK*	Risk Log	Exhibit 6	EDC+2 weeks	XLSX**
4	ISSUE*	Issue Log	Exhibit 6	EDC+2 weeks	XLSX**
5	PMS*	Project Management Schedule	Exhibit 6	EDC+2 weeks Updated monthly	MPP
6	PMS-POAP*	Project Management Schedule Plan on a Page	Exhibit 6	EDC+2 weeks Updated monthly	VSDX
7	PIP*	Project Implementation Plan	Exhibit 6	EDC+4 weeks and reviews	DOCX
8	SIPS	Site Implementation Plan Strategy	Exhibit 6	EDC+4 weeks	DOCX
9	QAP	Quality Assurance Plan	Exhibit 7	EDC+4 weeks	DOCX
10	TRNP*	Training Plan	Exhibit 10	Draft: EDC+4 weeks	DOCX XLSX
11	CFP	Contractor Furnished Property	Exhibit 4	TBD	DOCX XLSX
12	TNA	Training Needs Analysis	Exhibit 10	Draft: EDC+6 weeks	DOCX XLSX
13	DP	Documentation Plan	Exhibit 7	EDC+4 weeks	DOCX
14	TSD	Technical Solution Design	Exhibit 11	EDC+6 weeks	DOCX
15	MTP	Master Test Plan	Exhibit 8	EDC+6 weeks	DOCX
16	ETP	Event Test Plan	Exhibit 8	EDC+6 weeks	DOCX
17	TR-Templates	Training Templates and Formats	Exhibit 10	TBD	DOCX PPTX PDF

Serial	Name	Description	PWS Reference	To be completed by	Format
19	TR-MAT*	Training Material	Exhibit 10	TBD	DOCX PPTX PDF SCORM
20	TR	Test Report	Exhibit 8	1 week after each test event	DOCX
21	SIP	Site Implementation Plan	Exhibit 6	4 weeks before each site deployment	DOCX
22	SIS	Site Implementation Specification (updated and validated)	Exhibit 6	The (updated and validated) SIS will be submitted as a Draft 4 weeks before each site deployment. Final 2 weeks after each site deployment	DOCX
23	SSR	Site Survey Report (updated and validated)	Exhibit 6	~~The (updated and validated) SSR will be submitted 4 weeks before each site deployment (or 2 weeks after a site survey event if required)~~TBD	DOCX
24	~~S~~AT	~~Site~~ Acceptance Test (Plan and procedures)	Exhibit 8	4 weeks before each ~~site deployment~~acceptance test	DOCX
25	SAP	Security Accreditation Plan	Exhibit 9	TBD	DOCX
26	SRA	Security Risk Assessment Report	Exhibit 9	TBD	DOCX
27	SSRS	System Specific Security Requirement Statement	Exhibit 9	TBD	DOCX
28	SISRS	Generic System Interconnection Security Requirement Statement	Exhibit 9	TBD	DOCX
29	CSRS	Community Security Requirement Statement	Exhibit 9	TBD	DOCX

Serial	Name	Description	PWS Reference	To be completed by	Format
30	SecOPs	Security Operating Procedures	Exhibit 9	TBD	DOCX
31	STVP	Security Test and Verification Plan	Exhibit 9	TBD	DOCX
32	STVR	Security Test and Verification Report	Exhibit 9	TBD	DOCX
33	CIMP	Cyber Incident Management Plan	Exhibit 5	TBD	DOCX
34	SMP	Service Management Plan	Exhibit 6	TBD	DOCX
35	STP	Service Transition Plan	Exhibit 6	TBD	DOCX

1.3.2 Documents marked with an asterisk* are living documents and shall be updated throughout the life of the project.

1.3.3 File formats marked with double asterisk ** may be managed as SharePoint forms on the portal rather than the format defined in the table – subject to approval by the Purchaser Project Manager.

1.3.4 Documents shall be mastered in the SharePoint Portal provisioned by the Purchaser.

1.3.5 Any formal submission of any document on the portal will not be recognized unless an email is submitted to the Purchaser's Contracting Officer (PCO), Contracts Manager and Project Managers of both parties (Purchaser and Contractor).

1.3.6 Document reviews must adopt Track Changes (for Microsoft Word documents). Review comments for other file formats will be managed as separate files

1.4 Documentation Review and Acceptance

1.4.1 With the exception of security accreditation documentation, which has an extended period review of up to 90 days, the Purchaser will review each Document in detail for a period of up to ~~10~~ 20 working days after submission on to the Portal. During this review period, the Contractor shall make available to the Purchaser technical and contractual support as necessary to enable the Purchaser to perform the review. At the end of this period, the Purchaser will provide the Contractor with a detailed review.

1.4.2 Within 10 working days of receiving the Purchaser's review of a document, the Contractor shall incorporate all the modifications, additions and expansions required by the Purchaser. The Purchaser, provided that all comments are incorporated, will then formally accept the document.

1.4.3 The Purchaser reserves the right to request one additional cycle of review for each document should the Contractor not incorporate all the modifications,

additions and expansions required by the Purchaser. Any delays to the project will be the responsibility of the Contractor.

1.4.4 The Purchaser reserves to the right to exercise Articles defined in the Special Provisions should the second review cycle of a document be incomplete.

1.4.5 The Purchaser reserves the right to require the Contractor to make further changes to any document, to correct any errors detected during the implementation or to reflect any technical or contractual changes necessary as a result of any supplemental agreement made to the contract.

1.4.6 The approval of the PIP by the Purchaser signifies that the Purchaser agrees to the Contractor's approach in meeting the requirements. This approval in no way relieves the Contractor from their responsibilities to achieve the contractual and technical requirements of this contract. The requirements of the Contract supersede any statement in the PIP in case of any conflict, ambiguity or omission.

1.5 Project Controls

1.5.1 Project Status Reports (PSR)

1.5.1.1 The Contractor shall provide a Project Status Report (PSR), five (5) working days prior to the Project Review Meeting (PRM) as detailed in Section 1.5.5.

1.5.1.2 Failure to submit the PSR onto the project portal 5 working days prior to the PRM may result in a delay of the PRM – any additional costs or expenses as a result of this delay will be borne by the Contractor.

1.5.1.3 The PSR shall include the following items:

- Summary of project activities during the preceding month, as well as including the status of current and pending activities
- Progress of stage plan, exception plan(s), and schedule status, highlighting any changes since the preceding report
- Description of any identified issues and high risk areas with proposed solutions and corrective actions
- Test(s) conducted and results
- Proposed changes in Contractor personnel
- Summary of Change Requests requested or approved (e.g. service change request) to be included then in STP or SMP
- Plans for activities during the following reporting period, identifying all dependencies
- PFP tracking status
- Project Master Schedule and Project Master Schedule on a Page (PMS and PMSOAP)
- Risk and Issues log update

1.5.1.4 The Purchaser shall by mutual agreement with the Contractor amend the content, format and regularity of the PSR throughout the life of the project.

1.5.2 Project Meetings

1.5.2.1 Except otherwise stated in the Contract, the following provisions shall apply to all meetings to be held under the Contract.

1.5.2.2 Meetings shall normally take place at NCI Agency premises (either Mons, BLL, Brussels or The Hague). However, at the discretion of the Purchaser PM, alternative locations or virtual meetings may be permitted.

1.5.2.3 The Contractor shall submit a meeting request and meeting agenda 5 working days prior to any meeting. However, at the discretion of the Purchaser PM, meetings may be arranged with shorter notice.

1.5.2.4 The Contractor shall take meeting minutes and reach agreement at the meeting~~., submit them in draft version to the Purchaser for approval within 3 working days of the meeting, on the Project Portal as well as notifying by email.~~

1.5.2.5 ~~The Purchaser will respond within 3 working days of receipt of the draft minutes, and subject to Purchaser approval, the Contractor will finalized the minutes in the portal.~~

1.5.2.5 The participants shall not regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract, or as a vehicle to alter the design or configuration of equipment or systems. Any such changes shall only be made by authorized mechanisms as set forth in the Contract.

1.5.2.6 Any documentation, even in draft format, that may be useful to the Purchaser in preparing for meetings and ensuring efficient discussions during the meetings shall be provided to the Purchaser no later than 2 working days before the meeting. .

1.5.3 Project Kick-Off Meeting

1.5.3.1 The CPM shall participate in the ACPV Enterprise Service project kick-off meeting with the Purchaser's Project Team no later than two weeks after EDC. The meetings shall be held at the Purchaser's premises and shall be arranged by the Purchaser.

1.5.3.2 The Contractor shall propose which resources shall be in attendance (including Sub-Contractor personnel). This must be agreed by the Purchaser PM in advance 2 weeks prior to the meeting.

1.5.3.3 The Contractor (and Sub-Contractor) Project personnel shall introduce themselves, and explain which project deliverables they are accountable for and what work they are responsible for.

1.5.3.4 The CPM shall explain how the Contractor intends to manage the service implementation, service management ~~and~~ (including deployment approach) and service transition.

1.5.3.5 The Contractor's Technical Lead resources shall introduce how the Contractor intends to fulfil the technical implementation. This shall include the Site Survey aspects.

1.5.3.6 The Contractor's Test Director shall introduce how the Contractor intends to fulfil the Testing scope of work (as described in Exhibit 8).

1.5.4 Design Review Meetings

1.5.4.1 The Contractor shall co-ordinate the Design Reviews.

1.5.4.2 Meetings shall take place at NCI Agency premises. However, at the discretion of the Purchaser PM, alternative locations or virtual meetings may be permitted.

1.5.4.3 In addition to the scope and requirements for design reviews as described in Section 4, the Contractor shall provide the following, if applicable, at all design reviews:

- Changes to the PMS
- Risk assessment of proposed changes, and an update of the Risk Log and Issue Logs

1.5.5 Project Review Meetings

1.5.5.1 The Contractor shall coordinate and hold Project Review Meetings (PRM) with the Purchaser.

1.5.5.2 The PRMs shall be held at least once a month throughout the Period of Performance, and one every three (3) months during the Warranty period.

1.5.5.3 The Contractor shall provide a PSR, five (5) working days prior to each PRM, as per Section 1.5.1.

1.5.5.4 The Contractor shall submit a meeting request and meeting agenda 5 working days prior to the PRM.

1.5.5.5 Project delivery problems shall be identified, discussed and escalated with the Purchaser PM promptly, and shall not be held until PRMs.

1.5.5.6 The PRMs shall be conducted in one of the Purchaser's premises or the Contractor's sites and the location shall be subject to the Purchaser PM's approval. However, the location of PRMs may vary and, where possible, be scheduled with other project meetings.

1.5.5.7 ~~The PRM shall be held on the first Tuesday of each month. Deviation from this is subject to approval by the Purchaser PM.~~

1.5.5.7 The Contractor shall conduct a PRM ~~once a month throughout the Contract period of performance and~~ once a quarter ~~during the warranty period (if required)~~. This cadence may increase or decrease if deemed necessary by the Purchaser.

1.5.6 Other Meetings

1.5.6.1 The Purchaser shall host all other meetings unless there is a specifically agreed need to review material, witness technical demonstrations or testing, or perform any other activity outside of the Purchaser's premises, as part of the meeting.

1.5.6.2 The Contractor shall identify to the Purchaser's PM any other meetings with NATO personnel required to support this Contract.

1.5.6.3 Upon approval by the Purchaser's PM, the Contractor shall schedule, organize, and conduct such meetings.

1.6 Risk Management

1.6.1 The Contractor shall establish and maintain an overall Risk Management process for the project.

1.6.2 The Risk Management data shall be presented in a Risk Log to be created and maintained on the SharePoint Portal. The Contractor shall be responsible for maintaining the log throughout the project.

~~1.6.2 This Risk Management process shall identify all risks (management, technical, schedule, and cost risks), evaluate each risk, and select a proposed response for each risk.~~

~~1.6.3 Evaluating each risk shall result in the risk being rated as High, Medium, or Low, based on its probability and impact.~~

~~1.6.4 For each risk, the proposed response shall be selected from the following list:~~

~~1.6.4.1 Prevention: Terminate the risk by doing things differently and thus removing the risk, where it is feasible to do so. Countermeasures are put in place that either stop the threat or problem from occurring or prevent it from having any impact on the project or business.~~

~~1.6.4.2 Reduction: Treat the risk by taking action to control it in some way where the action either reduces the likelihood of the risk developing or limits the impact on the project to acceptable levels.~~

~~1.6.4.3 Acceptance: Tolerate the risk – e.g. if nothing can be done at a reasonable cost to mitigate it or the likelihood and impact of the risk occurring are at an acceptable level.~~

~~1.6.4.4 Contingency: plan and organize actions to come into force as and when the risk occurs.~~

~~1.6.4.5 Transference: Pass the management of the risk to a third party (e.g. insurance policy or penalty clause), such that the impact of the risk is no longer an issue for the health of the project.~~

~~1.6.5 The Risk Management data shall be presented in a Risk Log.~~

~~1.6.5.1 The Contractor shall create a Risk Log in the SharePoint Portal and shall be responsible for maintaining the log throughout the project.~~

~~1.6.5.2 The Risk Log shall be a table listing the risks, and shall include the following information:~~

- ~~Risk identifier: unique code to allow grouping of all information on this risk~~
- ~~Description: brief description of the risk~~

- ~~Risk category (e.g. commercial, legal, technical)~~
- ~~Impact: effect on the project if this risk were to occur~~
- ~~Probability: estimate of the likelihood of the risk occurring~~
- ~~Proximity: how close in time is the risk likely to occur~~
- ~~Countermeasure(s): what actions have been taken/will be taken to counter this risk~~
- ~~Owner: who has been appointed to keep an eye on this risk~~
- ~~Author: who submitted the risk~~
- ~~Date identified: when was the risk first identified~~
- ~~Date of last update: when was the status of this risk last checked~~
- ~~Status: e.g. dead, reducing, increasing, no change~~

1.7 Issue Management

1.7.1 An issue is anything that could have an effect on the Project, either detrimental or beneficial (change request, problem, error, anomaly, risk occurring, query, change in the project environment). An Issue Log shall be established, to record and track all issues and their status.

1.7.2 The Contractor shall create an Issue Log in the SharePoint Portal, and shall be responsible for maintaining the log throughout the project.

1.7.3 The Issue Log shall be a table and shall comprise the following information:

- Project Issue Number
- Project Issue Type (Request for change, Off-specification, general issue such as a question or a statement of concern)
- Author
- Date identified
- Date of last update
- Description
- Action item
- Responsible (individual in charge of the action item
- Suspense date (Suspense date for the action item)
- Priority
- Status

1.8 Project Portal

1.8.1 The Contractor shall also maintain a Project Portal (provided by the Purchaser) on which all relevant (classified up to NATO RESTRICTED) documentation and datasets shall be maintained. The Contractor shall be

able to access the Portal using the Purchaser provided REACH laptops (refer to the contract's special provision entitled Reach Capability) or any other approved device/mechanism for the exchange of NATO RESTRICTED information.

1.8.2 The Contractor shall make available to the Purchaser access to the Issue Log, Risk Log, Project Master Schedule, and other datasets and tools required by this ~~SOW~~ PWS on the Project Portal.

1.8.3 The Contractor shall make available the Project Websites to allow the Purchaser access to the finished and in-progress items, including design specifications and documentation. The Contractor shall use version control for all documentation published in the project portal.

1.8.4 The portal shall include all contractor-provided technical documentation.

1.8.5 The portal shall include other documents as directed by the Purchaser's PM, CO or ~~NQAR~~ NQAM.

1.8.6 The documents posted to the portal shall clearly indicate the version number inside the document.

1.8.7 The Contractor shall keep the portal up to date, in support of access by the users, or the Purchaser, through the warranty period, and any subsequent extensions.

EXHIBIT 7

QUALITY

[This Exhibit shall list and explain contractor's organization, processes and tools in two areas:

1. *Quality Assurance inherent to the organization and relevant certifications (based on ISO 9001 and STANAG 4107 Ed 12, or equivalent, as per guidelines given below).*
2. *Service Quality and its improvement inherent to the services being delivered (based on CMMI Security or CMMI Services Level 3 or equivalent in the project implementation phase, and then how it could be improved after 1 year of service(for example to Level 4 or other suggestions)*

The Contractor shall provide certifications and explain how internal QA processes will boost the Quality of the Services establishing a framework for continuous feedback management and service improvement.

Narratives provided below as for guidance only and to provide an example of how it could be structured in the PWS.]

1.1. Definitions

1.1.1. Unless otherwise specified in the ~~SoW~~ PWS, STANAG 4107 and underpinning AQAPs, ISO 9000:2015 (references found in PWS Part 6), PRINCE2 and ITIL definitions shall apply

1.1.2. Quality Assurance (QA) is a process and set of procedures intended to ensure that a product or service, during its definition, design, development, test and deployment phases will meet specified requirements.

1.1.3. Quality Control (QC) is a process and set of procedures intended to ensure that a manufactured product or performed service adheres to a defined set of quality criteria and meets the requirements of the customer.

1.1.4. Under the Contract, the terms "QA process" will also include Quality Control process.

1.1.5. A "Project document" is a document developed and maintained to help in the management of the project. Typically the plans (amongst which, the Quality Assurance Plan (QAP)) are project documents.

1.1.6. The term "NATO Quality Assurance ~~Representative~~ Manager" (~~NQAR~~ NQAM) shall apply to any of the Purchaser appointed Quality Assurance ~~Representative~~ Manager.

1.1.7. The term "Contractor Quality Assurance ~~Representative~~ Manager" (~~CQAR~~ CQAM) shall apply to any of the Contractor appointed Quality Assurance ~~Representative~~ Manager.

1.2. Introduction

1.2.1. The Contractor shall establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the Contract's lifetime.

1.2.2. The QA programme shall apply both the contractual requirements and the NATO requirements for quality identified by AQAP 2110, AQAP 2210 and AQAP 2310 and AQAP 2105 (references found in PWS Part 6) to provide confidence in the Contractor's ability to deliver products that conform to the Contractual requirements.

1.2.3. The Contractor's QA effort shall apply to all services and products (both management and specialist) to be provided under the Contract. This includes all hardware, software, firmware and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract (including deliverable and non-deliverable items like test and support hardware and software), without limitation.

1.2.4. The Contractor's QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.

1.3. Roles and Responsibilities

1.3.1. During the entire Contract implementation, the ~~NQAR(s)~~ NQAM(s) assures the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirements. The Purchaser, through its ~~NQAR(s)~~ NQAM(s), is the authority concerning all Quality related matters. The Contractor shall be responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the life-cycle of the Contract.

1.3.1.1. The ~~CQAR~~ CQAM shall be accountable for the provision of the QA Plan and the compliance to the defined QA process.

1.3.1.2. The ~~CQAR(s)~~ CQAM(s) shall define the major quality checkpoints that will be implemented while executing the project and the quality process to be used at each checkpoint.

1.3.1.3. The ~~CQAR(s)~~ CQAM(s) shall be responsible for assessing that the Contractual requirements have been complied with, prior proposing the Contractual services and products.

1.3.1.4. The ~~CQAR~~ CQAM shall report to a distinct manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.

1.3.1.5. The ~~CQAR~~ CQAM shall be the point of contact for interface with and resolution of quality matters raised by the NCI Agency or its delegated ~~NQAR~~ NQAM.

1.3.1.6. The Contractor shall support any NCI Agency or its delegated ~~NQAR~~ NQAM activity focused on monitoring Contractor activities at

Contractor's facilities or other sites related to the development, testing and implementation. In particular, the Contractor shall:

- Make himself/herself available to answer questions and provide information related to the project,
- Allow the Purchaser representatives to inspect and monitor testing activities, and management, technical and quality processes applicable to the project.
- Transfer to the Purchaser representatives all information deemed necessary to perform the QA activities, on his/her own initiative or on request by the Purchaser representative.

1.3.2. The Contractor shall ensure that ~~CQAR(s)~~ CQAM(s) have the required qualifications, knowledge, skills, ability, practical experience and training for performing their tasks.

1.3.3. The ~~CQAR(s)~~ CQAM(s) shall have sufficient responsibility, resources, authority and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective actions.

1.3.4. The ~~CQAR(s)~~ CQAM(s) shall participate in the early planning and development stages to ensure that all quality related requirements are specified in plans, standards, specifications and documentation.

1.3.5. After establishment of attributes, controls and procedures, the ~~CQAR(s)~~ CQAM(s) shall ensure that all elements of the QA Process are properly executed, including inspections, tests, analysis, reviews and audits.

1.3.6. The Contractor, through its ~~CQAR(s)~~ CQAM(s), shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services which conform to contractual requirements only.

1.3.7. The Contractor shall maintain and, when required, deliver objective evidence of this conformance.

1.3.8. The Contractor shall give written notice to the ~~NQAR(s)~~ NQAM(s) at least four weeks in advance that the services and/or products are being presented for review, testing, verification, validation and acceptance.

1.3.9. Testing shall only be permitted by using test procedures and plans approved by the Purchaser.

1.4. Quality Management System (QMS)

1.4.1. The Contractor shall ~~establish, document and maintain~~have a Quality Management System in accordance with the requirements of ISO 9001:2015 (references found in PWS Part 6).

1.4.2. The Contractor's and Sub-Contractor's QMS relevant to performance under the Contract shall be subject to continuous review and surveillance by the cognizant ~~NQAR(s)~~ NQAM(s).

1.4.3. The Contractor shall include in orders placed with its Sub-Contractor(s) and Supplier(s), the QMS requirements necessary to ensure the supplies and services covered by the Sub-Contract(s) and/or Purchase Orders conform to the requirements of the prime Contract.

1.4.4. The Contractor shall specify in each order placed with its Sub-Contractor(s) and Supplier(s), the Purchaser's and its ~~NQAR(s)~~ NQAM(s) rights of access to all premises where contractual work is performed, in order to carry out audits, inspections, tests and other functions as may be required by the ~~NQAR(s)~~ NQAM(s).

1.4.5. If sub-contracted quality resources are used, the Contractor's Quality Management process shall describe the controls and processes in place for monitoring the Sub-Contractor's work against agreed timelines and levels of quality.

1.5. Quality Assurance process

1.5.1. The Contractor's QA process shall ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.

1.5.2. The requirements for these processes shall be derived from the Contract, the QMS, the applicable AQAPs and referenced best practices, in that sequence of priority.

1.5.3. The Contractor shall prepare the testing process according to the contractual requirements

1.5.4. The Contractor shall prepare the test documentation in accordance to the contractual requirements The Contractor shall perform verification and validation of the Contractual deliverables before proposing them for the Purchaser review and approval.

1.5.5. The Contractor's QA process shall be described in the QA Plan as outlined below. The process is subject to approval by the Purchaser.

1.5.6. The Contractor shall demonstrate, with the Quality Assurance process, that the processes set up for design, develop, test, produce and maintain the product will assure the product will meet all the requirements.

1.5.7. The Contractor shall assure that all the test and procedure used to demonstrate the requirements will be monitored and controlled under the QA process.

1.5.8. On request, the Contractor shall provide the Purchaser with a copy of any Sub-Contracts or orders for products related to the Contract.

1.5.9. The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser ~~NQAR(s)~~ NQAM(s).

1.5.10. The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

1.6. The Quality Assurance Plan (QAP)

1.6.1. The Contractor shall provide a Quality Assurance Plan (QAP) for review to the Purchaser in accordance with the requirements identified in the AQAP-2105 (references found in PWS Part 6) and the ~~SoW~~ PWS requirements.

1.6.2. The Contractor's QAP shall be compatible and consistent with all other plans, specifications, documents and schedules, which are utilised under the Contract.

1.6.3. All Contractor procedures referenced in the QA Plan shall either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.

1.6.4. The QA Plan and all related QA procedures, and all their versions/revisions, shall be subject to ~~NQAR(s)~~ NQAM(s) approval based on an agreed checklist.

1.6.5. The acceptance of the QAP by the Purchaser only means that the Purchaser agrees to the Contractor’s approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

1.6.6. The Contractor shall review his QA programme periodically and audit it for adequacy, compliance and effectiveness.

1.6.7. The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

1.6.8. The Contractor shall inform the ~~NQAR(s)~~ NQAM(s)of deficiencies identified during internal audit unless otherwise agreed between the ~~NQAR~~ NQAM and/or the Purchaser and the Contractor.

1.6.9. The Contractor shall include a risk management section within the QAP including the risks connected to the sub-Contractors of the Contractor.

1.6.10. The Contractor shall make its quality records, and those of its Sub-Contractors, available for evaluation by the ~~NQAR(s)~~ NQAM(s) throughout the duration of the Contract.

1.6.11. The Contractor shall update the document, as required, from the delivery date of the initial QAP through Final Operating Capability (FOC), under Configuration control. The Contractor shall provide a copy

of each new version of the QAP to the Purchaser for review and approval.

1.7. Quality for Project Documents

1.7.1. A formal change management process shall be applied to all project documents, including documents naming conventions as defined by the Purchaser and coordinated with the Contractor.

1.7.2. Project documents shall be configuration controlled. Each version of a project document is subject to Purchaser approval (unless otherwise specified).

1.7.3. The Contractor shall ensure that any change related to the project documents are controlled, with the identity, approval status, version and date of issue are clearly identified.

1.7.4. Project documents file names shall not contain any variable part, like version number, reviewer initials or maturity status. Version numbers and maturity status shall be marked in the document content and/or attributes.

1.8. Deficiencies

1.8.1. The Contractor shall establish and implement a quality/product assurance Issue Tracking System (ITS) to ensure prompt tracking, documentation and correction of problems and deficiencies, during the lifecycle of the Contract.

1.8.2. The ITS shall implement a lifecycle (status, responsibilities, relationship to affected Contract requirements, if applicable, and due dates) for each recorded deficiency.

1.8.3. If the Contractor becomes aware at any time before acceptance by the Purchaser that a deficiency exists in any supplies, the Contractor shall log it in the ITS, coordinate with the Purchaser and promptly correct it.

1.8.4. The Contractor shall demonstrate that all deficiencies are solved / closed before product acceptance.

1.8.5. When the Contractor establishes that a Sub-Contractor or a Purchaser Furnished Equipment (PFE) product is unsuitable for its intended use, it shall immediately report to and coordinate with the Purchaser the remedial actions to be taken.

1.8.6. The Contractor shall ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.

1.9. Support Tools

1.9.1. All tools used by the Contractor in the context of project execution shall be available for demonstration to the Purchaser, upon Purchaser request.

1.9.2. The Contractor shall also make available to the Purchaser for review upon request, associated records and documentation, including but not limited to, control, authorization for use, calibration, validation, qualification, as applicable, per respective Contract requirement.

1.10. Certificates of Conformity

1.10.1. A Certificate of Conformity (CoC) is a document, signed by the Supplier / Vendor of a product, stating that the product conforms to contractual requirements and regulations. A Certificate of Conformity template is available in AQAP-2070 (references found in PWS Part 6).

1.10.2. The CoC, provides evidence that the items produced or shipped comply with test procedures and quality specifications prescribed by the customer.

1.10.3. The Contractor is accountable for the conformance to requirements, of products provided to the Purchaser.

1.10.4. The Contractor shall deliver all the CoC's for Commercial-off-the-Shelf (COTS) products (software, including firmware and hardware) released by the COTS Vendors.

1.10.5. The CoCs delivered by the Contractor shall be part of the acceptance data package of the product.

1.10.6. The Contractor shall provide a CoC at release of product to the Purchaser unless otherwise instructed.

EXHIBIT 8

TEST, VERIFICATION AND VALIDATION (TV&V)

[This Exhibit shall list and explain contractor's organization, processes, procedures and tools in three areas:

1. *User Acceptance Tests (UAT)*
2. *Measurement and Acceptance of the MoPs/KPIs/KPPs during the Service implementation phase, based on the list of MoPs/KPIs/KPPs to be defined by the Contractor in Exhibit 2*
3. *Continuous Assessment of the KPIs during the (in) Service Delivery phase*

Both areas shall include a description of the methodology (e.g. algorithms, datasets, filters and or weights) used to asses each MoPs/KPIs/KPPs or equivalent quantitative value.

The Contractor shall include in this exhibit its proposed approach to IV&V to meet requirements / objectives above and provide the above elements in a document as part of the Sprint 3 proposal submission, to be used as baseline for updates during the project development, delivery and in-service phase for IV&V activites.

Narratives provided below as for guidance only and to provide an example of how it could be structured in the PWS.]

1.11. Introduction

1.11.1. This Exhibit details the Test, Verification and Validation (TV&V) processes and requirements to be applied and performed under this contract.

1.11.2. All contract-related deliverables supplied by the Contractor will be verified and validated to ensure they meet the ACPV Statement of Objectives.

1.11.3. For each solution, the Contractor shall select a verification method, which shall be approved by the Purchaser.

1.12. TV&V activities

~~1.12.1. All information items used during the verification and validation activities are to be handled according to their security classification, in accordance with AD 070-001 (6.6.2).~~

1.12.1. The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities. This includes the development of all TV&V documentation required under the Contract, the conduct of all independent verification and validation as well as the evaluation and documentation of the results.

~~1.12.3. All Contract-related deliverables supplied by the Contractor shall be verified and validated to meet the requirements of this Contract.~~

~~1.12.4. All document-based deliverables shall be produced in a manner compliant with the templates provided by the Purchaser.~~

1.12.2. The Contractor shall support Purchaser led Validation activities to confirm that the solution is fit for purpose.

1.12.3. The Contractor shall be responsible for the planning, execution and follow-up of all TV&V events.

1.12.4. The Contractor shall demonstrate to the Purchaser that there is a Test Process in place for the project, supported by Contractor Quality Assurance (QA) described in Annex E of PWS.

~~1.12.8. The Contractor shall follow the Purchaser defined TV&V processes.~~

~~1.12.9. If the Contractor wishes to propose a modification to the process, the proposal shall be approved by the Purchaser and documented accordingly.~~

1.12.5. The Contractor shall ensure that rigorous testing, including regression testing when required, is performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.

1.12.6. All test, verification and validation material developed and used under the Contract shall be delivered to the Purchaser.

1.12.7. The Contractor shall appoint a Test Director (TD) for the phases defined in Table 1. The TD will work closely with the Purchaser's assigned TVV Manager and NATO Quality Assurance ~~Representative~~ Manager (~~NQAR~~ NQAM).

1.12.8. The Purchaser will appoint TV&V Test Engineers and Subject Matter Experts (SME) for each test event.

1.12.9. The Contractor shall use Key Performance Indicators (KPIs) to measure process execution and identify opportunities for quality improvement, provide solutions and update the plans, the achievement of defined objectives like coverage of risks, requirements, supported configurations, supported operational scenarios, etc.

1.12.10. The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities defined in Table 1 below.

TV&V Phases	Scope	Purchaser Involvement
Engineering Phase	Internal Contractor activities executed during development phase of the system to ensure the system conforms to the technical solution design specifications.	**Review**: Test Reports
TV&V Assessment Phase	Independent assessment performed with Purchaser and led by Contractor to determine whether or not a proposed Solution Purchaser needs.	Review: Review: Test Plan, Test Cases, Test Report, Existing defects

Table 1 - List of TV&V Phases

1.12.11. The Purchaser reserves the right to monitor and inspect the Contractor's TV&V activities to verify their compliance with the Service Objective forth in this Contract.

1.12.12. The Contractor shall only proceed to the next formal TV&V activity, after the successful completion of the previous TV&V activity and after the agreement/approval by the Purchaser.

1.13. Deliverables

The Contractor shall provide a System Test Documentation Package, following documentation templates provided by the Purchaser that is comprised of the following documents:

Work Product Name	First Draft	Sent to Review/Approve
The Test Plan (TP)		
The Test Cases		
Test Report		
~~System under test Documentation~~		

Table 2 - Test Documentation

~~Modification of inaccurate or inadequate TV&V deliverables and any subsequent work arising as a result shall be carried out at the Contractor's expense.~~

All TV&V materials developed and used under the Contract shall be delivered to the Purchaser.

Templates provided by the Purchaser are to be utilized by the Contractor as structure guides and for the content the Purchaser expects to be detailed. If the Contractor would like to propose a modification of the templates, it shall be approved by the Purchaser.

All deliverables shall undergo as many review cycles are required, and shall be approved once all deficiencies have been corrected.

1.13.1. Test Plan (TP)

1.13.1.1. The Contractor shall identify and describe in the Test Plan (MTP) which best practices and international standards will be applied and how.

1.13.1.2. The Contractor shall produce a Test Plan (TP) to address the plans for each TV&V activities listed in this document. The Purchaser will monitor and inspect the Contractor's TP activities to ensure compliance.

1.13.1.3. The Contractor shall keep the TP always up to date.

1.13.1.4. The Contractor shall describe all formal TV&V activities in the TP with a testing methodology and strategy that fit the development methodology chosen by the project.

1.13.1.5. The Contractor proposed testing methodology shall describe the method of achieving all the test phases.

1.13.1.6. The Contractor shall describe in the TP how the Service objectives will be met.

1.13.1.7. The Contractor shall describe the Contractor's test organization and its relationship with the Contractor's Project Management Office and Quality Assurance (QA) functions in the TP.

1.13.1.8. The Contractor shall describe in the TP "Entry and "Exit" criteria for each of the formal TV&V events.

1.13.1.9. The Contractor shall provide in the TP the schedule, When the Contractor identifies that multiple events are required for a phase, this shall also be specified in the TP.

1.13.1.10. Together with the TP, the Contractor shall provide a defect reporting and management process to be applied during the TV&V activities.

1.13.1.11. The Contractor shall describe how defects/non-conformances encountered during TV&V events will be reported, managed and remedied.

1.13.2. Test Cases

1.13.2.1. The execution of test cases during each phase shall be incorporated into the relevant test cases by the Contractor for use during independent verification, validation and acceptance. All changes shall be made with the agreement and approval of the Purchaser.

1.13.2.2. The Contractor shall develop test and use cases to verify and validate all requirements in the ~~SoW~~ PWS, requirements specifications and final design.

1.13.3. Service Acceptance Criteria

1.13.3.1. The Contractor SHALL translate each solution, in an acceptance criteria that will clearly detail how the requirement will be fully met (clear pass/fail or yes/no outcome). This shall include User Acceptance Testing of the Service (UATs).

~~1.13.3.2. The Contractor SHALL address the Purchaser's comments and update the Acceptance Criteria accordingly.~~

1.13.3.2. The Acceptance Criteria SHALL be agreed by both contractor and purchaser prior to the creation of the Test Cases.

1.13.3.3. The agreed Acceptance Criteria SHALL be translated into Test Cases to provide details of full requirements coverage.

1.13.4. Test Report

1.13.4.1. The Test Report provides a summary of the testing performed during the Test Event.

1.13.4.2. The Contractor shall provide, in the Test Report, a log/record of the event, including but not limited to individual test results, defects found (with a way forward for the ones remaining open), requirement coverage (planned and executed), test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

1.14. TV&V Events and results

The Contractor shall conduct testing during the Project lifecycle compliant with the following requirements:

The Contractor is responsible for conducting all testing during the entire Project and Service lifecycle. The Contractor shall provide evidence to the Purchaser of the results of these testing activities. The Contractor shall respond to any Purchaser clarification requests regarding test results or performance within two working days.

Progress and results measurement shall be approved by the Purchaser and focused on KPIs.

1.14.1. TV&V Event

1.14.1.1. During formal TV&V phases, a daily progress debrief shall be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.

1.14.1.2. For each TV&V event, the Contractor shall provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

1.14.1.3. At the end of the project, the Contractor shall provide the final version of all artefacts (regardless of format) created during the execution of all TV&V activities.

1.14.2. ~~Test Waivers~~

~~1.14.2.1. The Contractor may request a Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. The Purchaser, after review of test waivers and analysis of their impact, reserves the right to require test and certification of the modified equipment at no cost to the Purchaser. The Purchaser has the right to reject any test Waiver.~~

~~1.14.2.2. The Contractor shall record and log all waiver requests along with their resolution submitted for the Purchaser's approval.~~

1.15. Test Defect Categorization

The Contractor shall use the Purchasers' categorization nomenclature for all defects and non-compliances.

Should a failure be identified during a TV&V event/activity, a defect shall be recorded ~~in the Agency's' test management and defect management systems~~and documented. Once the event has concluded, the defect shall be reviewed during the event review meeting to agree on the severity, priority and category. The event test report shall then report the disposition of all defects recorded during the event and the defect management system shall be updated accordingly.

Classification shall follow the definitions in Table 3 - Definitions for Defect Categorization:

Attributes	Definition
Severity	The severity of a defect is the degree of impact that the failure has on the development or operation of a component, a system or a user function. The severity shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached, the Purchaser's PM will set the severity.
Priority	The priority of a defect defines the order in which defects shall be resolved. The priority of the defect shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached, the Purchase's PM will set the priority.
Category	The type of observation identified during the execution of a test case.

Table 3 - Definitions for Defect Categorization

1.15.1. Severity

According to their severity, defects shall be classified as one of the following in Table 4 - Classification of defects based on severity:

Severity	Definition
Critical	The failure of testing of a requirement. The failure results in the termination of the complete system or one or more component of the system. The failure causes extensive corruption of data. The failed function is unusable and there is no acceptable alternative

Severity	Definition
	method to achieve the required results
Major	A significant failure that causes severely impaired functions but does not prevent operational processing. Applies to conditions under which the complete system or one or more component of the system are partially inoperative, but are still usable by the users. A work around may be available, but it may require manual intervention. Examples: * Absence of expected modules/ object or Unit * failure of business operational process that affects a large group of users * complete failure of a module
Moderate	The failure does not result in the termination and all functions are available but causes the system to produce incorrect, incomplete or inconsistent results. When resources are available and budgeted, should be resolved.
Minor	The failure does not result in termination and does not damage the functioning of the system. The desired results can be easily obtained by working around the failure.
Cosmetic	The failure is related to the look and feel of the application, typos in a document or user interfaces (amongst others), and not part of the immediate usability or contractual requirements. The failure does not adversely affect the overall system operation.

Table 4 - Classification of defects based on severity

1.15.2. Priority

According to their priority, defects shall be classified as one of the following in Table 5 - Priority Classes for Defect Classification:

Priority	Description
Urgent	The defect shall be resolved as soon as possible. Required to complete independent verification and validation activities.
Medium	The defect shall be resolved in the normal course of development activities. It can wait until a new build or version is created.
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.

Table 5 - Priority Classes for Defect Classification

1.15.3. Category

According to their category, defects shall be classified with one of the values defined in Table 6 - Defects Categories:

Category	Description
Defect	An imperfection or deficiency in a work product where it does not meet its requirements or specifications. This category of defect could drive to the creation a Class II (Product Correction) Engineering Change Proposal (ECP).
Enhancement	This type of defect is used to record an Improvement to the product baseline. This category of defect would typically drive to the creation of a Class I (Product enhancement) ECP.
Document	This category is used to record defects encountered in the system documentation (test cases, test procedures, RTM, test plan, manuals, design, procedures…).
Clarification	This category is used to record deficiencies encountered during the test execution, which must be clarified.
Waiver	This category is used to record when a waiver is required to address a specific observation or defects.

Table 6 - Defects Categories

Annex A ~~Verification Methods~~

~~A.1. Verification Methods~~

1 ~~This annex aims to provide further details about the possible verification methods for Requirements expressed in this and other associated documents. The definitions are based on ISO/IEC/IEEE 29148 (*6.6.9*).~~

A.1.1 ~~Test~~

~~A.1.1.1. Definition: an action by which the operability, supportability, or performance capability of an item is quantitatively verified when subjected to controlled conditions that are real or simulated. These verifications often use special test equipment or instrumentation to obtain very accurate quantitative data for analysis.~~

~~A.1.1.2. This method is used when it is possible to make direct or indirect measurement of a specific numerical parameter to verify compliance with a stated requirement. Actual measured values are recorded, and pass/fail is determined by comparing the measured value with the specified value. Input data and results are provided in the test procedures.~~

~~A.1.1.3. Controlled condition, configurations, and inputs are used in order to observe the response. Results are quantified and analyzed. This method can be used where user interaction is involved and when computations with input data are necessary.~~

~~A.1.1.4. Two basic test approaches are black box and white box testing.~~

- ~~In black box testing, the inner structure and design of the test object is unknown or not considered and the test cases are derived from the specification.~~
- ~~White box techniques are based in the knowledge of the inner structure of the test object, require that the source code were available and flow-oriented test cases will be identified.~~

~~A.1.1.5. In practice, these approaches are used to complement each other because they tend to detect different classes of errors. Black box techniques are useful for finding incorrect or missing functions, interface errors, errors in data structure, performance errors and initialization and termination errors. Black box techniques miss many other errors because they ignore important properties of items that are due to design and implementation factors and incomplete requirement descriptions. White box testing focuses on such errors.~~

A.1.2 ~~**Demonstration**~~

~~A.1.2.1. Definition: a qualitative exhibition of functional performance, usually accomplished with no or minimal instrumentation or test equipment. Demonstration uses a set of test activities with system stimuli selected by the supplier to show that system or system element response to stimuli is suitable or to show that operators can perform their allocated functions when using the system. Observations are made and compared with predetermined responses. Demonstration may be appropriate when requirements or specifications are given in statistical terms (e.g., mean time to repair, average power consumption, etc.).~~

~~A.1.2.2. This method is used to demonstrate a capability to be provided by the requirement.~~

~~A.1.2.3. Test procedures and their test cases will contain test steps which define specifically the inputs and pre-conditions necessary for verification of the subject requirement.~~

~~A.1.2.4. The system receives messages, as defined in the test description and provided by the test environment, to potentially include a tool to check the inputs for correctness.~~

~~A.1.2.5. Demonstrations may occur during verification of a SUT (System Under Test) at any development stage.~~

~~A.1.2.6. Pass/fail criteria are simple yes/no indications of functional performance since no quantitative values are specified.~~

A.1.3 ~~**Inspection**~~

~~A.1.3.1. *Definition: an examination of the item against applicable documentation to confirm compliance with requirements. Inspection is used to verify properties best determined by examination and observation (e.g., - paint colour, weight, etc.). Inspection is generally non-destructive and typically includes the use of sight, hearing, smell, touch, and taste; simple physical manipulation; mechanical and electrical gauging; and measurement.*~~

~~A.1.3.2. *Products subject to inspection:*~~

- ~~Software to determinate whether physical quality lists are met. Software logic inspections are conducted on selected Test Cases;~~
- ~~Hardware products (including server rooms, racks, cabling…) to determinate whether physical quality lists are met. It may require moving, turning, or partially disassembling the item to aid visual access, but does not require operation of the item;~~
- ~~Documentation, for example design, operational manuals or other project documentation including test plans and test cases.~~

~~A.1.3.3. *The pass/fail criteria are simple accept/reject indications and shall be based on the visual inspection results or information content of the documentation.*~~

A.1.3.4. *Inspection is conducted by experts in product design (i.e., software designers, hardware designers, test team members), who are not directly related to the development of the product being inspected.*

A.1.4 **Analysis**

A.1.4.1. Definition: Use of analytical data or simulations under defined conditions to show theoretical compliance. Used where testing to realistic conditions cannot be achieved or is not cost-effective. Analysis (including simulation) may be used when such means establish that the appropriate requirement, specification, or derived requirement is met by the proposed solution. Analysis may also be based on 'similarity' by reviewing a similar item's prior verification and confirming that its verification status can legitimately be transferred to the present system element. Similarity can only be used if the items are similar in design, manufacture, and use; equivalent or more stringent verification specifications were used for the similar system element; and the intended operational environment is identical to or less rigorous then the similar system element.

A.1.4.2. Pass/fail criteria are objective and based on the analytical/simulation/analysis results versus the stated requirements and associated tolerances.

A. Test data: Analysis of test data is used where a specified parameter cannot be measured directly. Selected parameters are measured and analysed to determine whether the specified parameter is met.
B. Simulation: Evaluation of a simulation model's outputs is used to determine compliance with specific parameters when there is no other practical technique to show specification compliance.
C. Documentation: The design and manufacturing documentation is evaluated by qualified personnel to ascertain, by analytical methods, if a specification parameter is met.

EXHIBIT 9

SECURITY ACCREDITATION

1 SECURITY ACCREDITATION

1.1 Security Accreditation Requirements

1.1.1. ACPV needs to achieve security accreditation in order to be granted the authorization for operational use at [NS]~~ or [NR].~~ Therefore, the security accreditation process established for the Enterprise ACPV Communications and Information System (CIS) by the Purchaser Security Accreditation Authority (SAA) shall be followed.

1.1.2. The contractor shall be clearly informed by the Purchaser about the final decision at which classification level the ACPV will operate.

1.1.2.1. The accreditation process documentation, requirements and deliverables regardless of the classification decision are the same, only the security requirements of the ACPV might change.

1.1.3. The Contractor shall respect any established security accreditation processes in the NATO Enterprise. The Purchaser shall provide the required coordination, ensure all relevant Security Accreditation Authorities are informed, and clearly state the accreditation process requirements to the Contractor. The NATO Enterprise is defined in ~~reference 6.2.12~~ AC/322-D(2015)0014-REV4 (INV) dated 04 July 2023.

1.1.4. The ACPV CIS will connect or interconnect with NATO CIS from different NATO Enterprise stakeholders. The Contractor shall provide clear description which data sources/systems are required to be interconnected to for the ACPV to achieve required results.

1.1.5. The Contractor from the perspective that any connection or interconnection shall be revealed and acknowledged by the respective security accreditation authorities shall respect the existing security accreditations for all the CIS in the ACPV scope.

1.1.6. The contractor shall prepare the accreditation documentation and add the required deliverables to the PMS. In case of the gradual implementation of the CIS across multiple sites or data sources, the accreditation deliverables shall represent that fact as well.

1.1.7. The Purchaser security accreditation authority shall facilitate the coordination with respective security accreditation authorities over the NATO Enterprise.

1.1.7.1 The primary objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the ACPV. This includes ensuring that the ACPV conforms to NATO Security Policies and Directives identified in Section 6.2 of Part 6 and in the ACPV-specific Security Accreditation Documentation Set (SADS) (see section 1.4).

1.1.7.2 The security accreditation is to be issued to the Purchaser by the Purchaser SAA, hereinafter referred to as the SAA, for the ACPV to store, process and transmit NATO information in its operational environment.

1.1.7.3 The Purchaser Accreditation Support Office (ASO) will facilitate the coordination of the security accreditation process with the SAA. For some activities, the ASO may delegate the authority to other members of the Purchaser and this fact will be always communicated to the Contractor.

1.1.7.4 Roles and Responsibilities in the security accreditation process are described at the end of this chapter.

1.1.8. The Contractor shall follow the a structured security accreditation of ACPV process based on the high level requirements established in the Management Directive on CIS Security (Reference 6.2.3) as detailed in this section and in the Security Accreditation Plan (SAP). Deviations from this structured process shall be always documented and can only be authorized by the SAA.

1.1.9. Security accreditation process for the ACPV shall be strictly followed by the contractor and encompass overall development, production and implementation of the ACPV.

1.1.10. Security accreditation for ACPV shall be achieved before the system is transitioned to the operational live-environment, unless the SAA will require that some security related activities to be conducted in the operational live-environment.

1.1.11. The Contractor shall recognize the NATO Security Policies and supporting Directives identified in the references under Section 6.2 of Part 6 and any other guidance provided by the Purchaser, in order to take into account all related requirements in the resulting ACPV technical solution design and installation thereof.

1.1.12. The Contractor shall take into account the NATO CIS security requirements identified in the PWS Exhibit 11 – Technical Solution Design for the implementation and support of security domains in the NATO environment.

1.1.13. The Contractor shall ensure the ACPV architecture is configured, deployed, tested and operated in compliance with the security requirements as specified in the Security Accreditation Documentation Set (e.g. SRA, SSRS, CSRS, STVP and SecOPs).

1.1.14. The Contractor shall ensure that all the security countermeasures, as detailed and accepted by the Purchaser in the Security Risk Assessment (SRA), System-Specific Security Requirement Statement (SSRS), Community Security Requirement Statement (CSRS), System Interconnection Security Requirement Statement (SISRS), Security Operating Procedures (SecOPs) and other relevant accreditation documents, have been installed and configured for all delivered ACPV elements.

1.1.15. The Contractor shall ensure through security testing that security measures (e.g. personnel security, physical security, security of information, CIS security controls, security of the classified projects and industrial security), including security baselines identified in the respective SRA, SSRS, CSRS, SISRS and SecOPs have been properly implemented in accordance with the requirements of the SAA.

1.1.16. The Contractor shall ensure that verification is carried out on the request of the SAA and typically supported by appropriate results of security testing conducted based upon agreed Security Test and Verification Plan (STVP) which is to cover all security requirements identified and approved in form of in the respective SSRS, CSRS and SISRS.

1.1.15.1. The Purchaser system security requirements implementation and tests effectiveness will be verified by the independent security audit unless decided otherwise by the SAA.

1.1.17. Within the Security Accreditation Document Set (SADS), the Contractor shall ensure that it presents to the Purchaser, all required documents listed in the section 1.4.

1.1.18. Contractor shall recognize that Purchaser SAA might require additional documents for the successful accreditation of ACPV especially after the interconnections of ACPV will be confirmed by the SAA.

1.1.19. The Contractor shall provide all the required documents to the Purchaser. The Contractor shall not deliver any documents directly to the SAA unless directed by the Purchaser. The Purchaser will conduct the coordination with the SAA.

1.1.20. The SAA may provide advice and instructions to the Contractor on any security implication or any proposed change based on the findings and results of the assessments and/or security test results. The Contractor shall consider the advice, instructions and guidance from the SAA. The Contractor shall take action(s) to follow, carry out the necessary work and to implement the advice, instructions and guidance given by the SAA.

1.1.21. The Contractor shall ensure that full support is provided to the Purchaser in order to achieve security accreditation for ACPV and shall adhere to the timelines and sequence of the required deliverables as specified by the Purchaser (see section 1.2).

1.1.22. The Contractor shall ensure that in the support of producing the deliverables the Contractor shall closely engage directly with representatives of the Purchaser ASO and/or the SAA (through the Purchaser) in order to discuss particular security-related requirements but also to clarify and/or enhance the documentation to be provided as part of the SADS.

1.1.23. The Contractor shall ensure that they conveyed security meetings and workshops that shall be attended by the Contractor and by representatives of the Purchaser. Location of the meetings and workshops will be defined by the Purchaser and will typically take place at a facility located in the Purchaser. The Contractor may be invited to provide briefings and/or technical expertise for meeting(s) with the SAA.

1.2 Security Accreditation Process

1.2.1. The achievement of security accreditation for ACPV depends on development and SAA approval of necessary Security Accreditation Documentation Set (SADS).

1.2.2. The Contractor shall produce, complement and manage SADS in order for the approval of the Purchaser SAA to consider ACPV for accreditation as per section 1.4.

1.2.3. All the documents in the SADS shall be approved by the SAA to be accepted as the part of the required deliverables.

1.2.4. If acceptance requires multiple rounds of comments and amendments, the Contractors shall comply with the requests of the Purchaser and/or the SAA until the approval process is completed.

1.2.5. In case of any potential timeline issues resulting in the unforeseen extension of the approval process of the accreditation documentation, the Contractor shall inform immediately the Purchaser.

1.2.6. The SADS shall be developed in parallel to appropriate project deliverables related with the ACPV architecture as depicted in the points below.

1.2.7. CIS Description, Security Risk Assessment and System-specific Security Requirements Statement and Community Security Requirement Statement shall be developed by the Contractor. The review process of those documents will follow the accreditation timelines after the Contractor will make the documents available to the Purchaser.

1.2.8. CIS Description, SRA, CSRS and SSRS shall be approved by the SAA.

1.2.9. Initial versions of SecOPs, Security Test and verification Plan (STVP) and System Interconnection Security Requirement Statement (SISRS) shall be developed and released by the Contractor.

1.2.10. Final versions of SecOPs, STVP and SISRS shall be developed and released by the Contractor not later than 4 weeks prior to the start the initial security testing.

1.2.11. SecOPs, STVP shall be approved by the SAA before commencing initial security testing.

1.2.12. SISRS shall be approved by the SAA before interconnection to another CIS is to take place as depicted in the CIS Description and required by Security Accreditation Plan (SAP).

1.2.13. Some SADS documents (especially SecOPs) might require further updates as recommended by the Contractor and/or Purchaser based on the observations and lessons learned gathered during security tests and/or service acceptance tests. New versions of every security-related documentation shall be approved by the SAA.

1.2.14. The Contractor shall conduct security testing in accordance with SAA approved STVP.

1.2.15.1. The Purchaser might be required to conduct some STVP related

testing in support of the security accreditation process. This is applicable for all tests, which Contractor will not be able to accomplish successfully.

1.2.15. The instances of security testing shall be conducted in support of the accreditation process of the ACPV and they will be communicated to the Contractor after the approval of the STVP.

1.2.16. The security testing shall be conducted as per populated at the later stage table.

1.2.17. Table 1-1 Sample of the Instances of ACPV Security Testing

Test Instance	When	Where	Scope	Responsibility
Location A				
Initial security testing				The Contractor
Main security testing				The Contractor
Supplementary security testing				The Purchaser
Additional security testing				The Purchaser

1.2.18. The overall purpose of each security testing instance is depicted in the Table 1-2 below:

Table 1-2 Description of Security Testing Instances

Test Instance	Description / Purpose
Initial security testing	To verify compliance to identified CIS security requirements (as per STVP). Scope of the testing might be limited as system is not yet fully configured and/or connected to other CIS, which might be required to support full testing of the specific Security Requirements. Example of the security requirement to be tested: Existence of required TEMPEST certificates[3], deployment of generic NCSC security settings.
Main security testing	To verify implementation of all those CIS security requirements and associated security mechanisms which were either not able to be verified during initial security testing (for example all tests which would require interconnection in order to be executed) or where not successfully completed during initial security testing.
Supplementary security testing	To verify the overall compliance with SSRS. If approved by the Purchaser and / or the SAA this instance might be also used to verify implementation of CIS security requirements, which were not successfully completed during initial and/or main security testing.

[3] Should the technical solution involve provision of CIS equipment (hardware), the contractor shall be required to provide TEMPEST A, B or C certificates for the equipment provided as part of the technical solution depending on the environment where the equipment will be located. Reference Part 6 para 6.2.39.

Test Instance	Description / Purpose
Additional security testing	To verify implementation of all those CIS security requirements and associated security mechanisms which were not successfully completed during supplementary security tests sessions. The understanding is that none or only very limited amount of security tests should be tested during additional security testing.

1.2.19. The Contractor shall develop STVR after each instance of security testing identified in the Table 1-1 Sample of the Instances of ACPV Security Testing where responsibility is identified as for the Contractor.

1.2.20. The Contractor shall develop a separate STVR for each ACPV component, location or any other testing functional block agreed with the Purchaser SAA.

1.2.21. The STVR shall be made available to the Purchaser within 1 week after completion of the relevant security test event.

1.2.22. The STVR developed for the initial security testing for specific ACPV component, location or any other testing functional block agreed with the Purchaser SAA, shall be further amended during main security testing, supplementary and additional security testing.

1.2.23. All identified CIS security related deficiencies documented in STVR under Contractor responsibility shall be either fixed by the Contractor or waived by the Purchaser before the specific element of ACPV would be handed over to the Purchaser.

1.2.24. In order to test specific ACPV elements, before use in the final operational environment or to enable some specific activities (e.g. Independent Verification and Validation, Security Testing in accordance with Security Test and Verification Plan (STVP), SIT, etc.) the Contractor shall provide Approval for Testing (AfT) Request. The Contractor shall release the AfT Request not later than 10 working days prior to each test activity requiring AfT.

1.2.25. The AfT requirement pertains to any test where access to the life NATO system or operational data is required.

1.2.26. AfT request(s) are subject to SAA review (through the Purchaser). If approved, the SAA will issue official AfT.

1.2.27. Successful STVRs will be one of the conditions for the SAA to grant AfT or (Interim) Security Accreditation (I(SA)).

1.2.28. The AfT requests are to be supported by the relevant STVRs.

1.2.29. Type 3 Security Audit (Vulnerability Assessment) will be performed by the Purchaser as required by the SAA. All identified CIS security related deficiencies documented in Type 3 Security Audit Report under Contractor responsibility shall be either fixed by the Contractor or waived by the Purchaser SAA.

1.2.30. The result of the accreditation process shall be the Security Accreditation (SA).

1.2.31. If the achievement of the full Security Accreditation is not possible and SAA will issue only the Interim Security Accreditation (ISA), the Contractor is to coordinate with the Purchaser whether the ISA can be considered as the acceptable process outcome.

1.2.32. By exception and for pressing operational deployment the CIS Operational Authority (CISOA) may issue an Interim Authorization to Operate (iATO). The iATO has no impact on the ongoing accreditation process and shall not be considered a part of the process but rather the temporary mitigation. It is the Purchaser's decision if the iATO will be requested for ACPV.

1.2.33. The iATO is not the desired outcome of the ACPV accreditation process. The Purchaser reserves the right to decide whether the conditions justify accepting this as the outcome of the accreditation process.

1.2.34. Considering the fact the ACPV might not be delivered to all locations at the same time, the security accreditation statement might be amended few times to reflect addition of each element separately.

1.2.35. Final security accreditation for the entire ACPV CIS shall be achieved before Service Acceptance.

1.2.36. All above activities and associated expected timelines are depicted in the Purchaser developed Security Accreditation Plan (SAP). It will detail how accreditation shall be achieved for ACPV.

1.3 Security Risk Assessment

1.3.1. The Security Risk Assessment is the crucial part of the accreditation process.

1.3.2. The Security risk assessment is the process of identifying security risks, i.e. the threats and vulnerabilities to the CIS, determining their magnitude and identifying areas needing countermeasures. Security risk assessment serves to identify the risks that exist, identify the current security posture of the CIS in respect to handling information, and then assemble the information necessary for the selection of effective security countermeasures, based upon NATO Security Policy and supporting Directives and Guidance.

1.3.3. Objective of the SRA is to define the security objectives of confidentiality, availability and integrity/authenticity of the designed ACPV systems according/in tandem to the particular services to be provided by the resulting ACPV system, the values of the traffic and information stored and transported over the system, and the nature and levels of the particular threats being identified.

1.3.4. The Security risk assessment contributes to the decision on which security measures are required, and how the apportionment between technical and alternative security measures can be achieved. It shall produce an unbiased assessment of the residual risk.

1.3.5. The Contractor shall conduct an ACPV Security Risk Assessment (SRA) based on the information provided in the CIS Description document. SRA is to be approved by the Purchaser SAA.

1.3.6. The Contractor shall conduct an SRA in accordance with AC/35-D/1017 (references found in PWS Part 6).

1.3.7. The Contractor shall use the SRA application PILAR 2021.1 version minimum or any newer version approved by the Purchaser (and utilizing MAGERIT methodology) with the NATO profile.

1.3.8. The Contractor shall made request to the Purchaser to access the NATO PILAR application and specify the number of required licenses. The Purchaser will provide the license purchasing details.

1.3.9. It is not allowed to use any other version of the PILAR as NATO version differs from the one that can be obtained commercially.

1.3.10. The application will be available on the NATO NR AIS (REACH).

1.3.11. The Purchaser will provide to the Contractor the detailed user guide, required introductory training and guidance how to model risk in ACPV in accordance with recommendations from the NATO Security Risk Assessment Group (NSRAG).

1.3.12. The Contractor shall organize SRA workshop(s) at the Purchaser facility. Respective Purchaser's Subject Matter Experts (SMEs) shall be invited to support proper assessment. It has been anticipated that at least 5 (five) up to 10 (ten) days SRA workshops will be required.

1.3.13. The ACPV SRA process shall include the following stages:

1.3.13.1. Identification of the scope and objective of the security risk assessment (which shall be agreed with the Purchaser SAA and possibly with national SAAs);

1.3.13.2. Use of the AC/322-D/0048-REV3 Technical and Implementation Directive on CIS Security (Reference 6.2.7) as the source of controls for the SRA (already incorporated in the PILAR);

1.3.13.3. Completing Project Data part in the PILAR including proper identification of the security domains for ACPV system;

1.3.13.4. Determination of the essential, physical, personnel and information assets which contribute to the fulfilment of the mission of the ACPV;

1.3.13.5. Determination of the value of the identified assets against the following impacts: disclosure, modification, unavailability and destruction;

1.3.13.6. Establishment of the Logical and Physical Zones for ACPV SRA;

1.3.13.7. Identification of the threats and vulnerabilities to the risk environment and their level;

1.3.13.8. Identification and valuation of the existing countermeasures in the risk treatment;

1.3.13.9. Determination of the necessary countermeasures and a comparison with existing measures; identifying and valuating those countermeasures, which are already installed, and identifying those countermeasures, which are recommended. SRA valuation shall be substantiated with comments related to the particular valuation of controls.

1.3.14. Based on the results of the SRA, the Contractor shall identify areas of the ACPV System and service that require safeguards and countermeasures to comply with NATO Security Policy and supporting Directives. The decision on specific security mechanisms shall be based on evidence(s) and results produced by the Security Risk Assessment Report.

1.3.15. Where the implementation of the security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components, the Contractor shall evaluate and process and embody the change within the technical and financial scope of this Contract. ~~In this instance, no Engineering Change Proposal (ECP) shall be generated.~~ The relevant security accreditation documentation shall be amended to reflect this modification of the design.

1.3.16. Where the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, the Contractor shall raise an ECP.

1.4 Security ACCREDITATION Documentation Set

1.4.1. The complete Security Accreditation Documentation Set (SADS), also known as the Security Related Documentation (SRD), which encompass the entire ACPV CIS shall consist of the following documents:

1.4.1.1. Initial CIS Description (iCISD);

1.4.1.2. CIS Description;

1.4.1.3. Security Accreditation Plan (SAP);

1.4.1.4. Security Risk Assessment (SRA) Report;

1.4.1.5. System Specific Security Requirement Statement (SSRS);

1.4.1.6. Community Security Requirement Statement (CSRS) (if required);

1.4.1.7. System Interconnection Security Requirement Statement (SISRS);

1.4.1.8. Security Operating Procedures (SecOPs);

1.4.1.9. Security Test and Verification Plan (STVP);

1.4.1.10. Security Test and Verification Report (STVR),

1.4.2. The Contractor shall produce, complement and manage the SADS in support of the accreditation process, these are deliverables in English language:

1.4.2.1. Security Accreditation Plan (SAP)

1.4.2.2. Initial CIS Description (iCISD)

1.4.2.3. CIS Description (CISD);

1.4.2.4. Security Risk Assessment (SRA) Report;

1.4.2.5. System Specific Security Requirement Statement (SSRS);

1.4.2.6. Community Security Requirement Statement (CSRS) (if required)

1.4.2.7. Generic System Interconnection Security Requirement Statement (SISRS);

1.4.2.8. Security Operating Procedures (SecOPs);

1.4.2.9. Security Test and Verification Plan (STVP);

1.4.2.10. Security Test and Verification Report (STVR)

1.4.3. Only SAA is authorized to approve the security accreditation documents. The Contractor should expect a number of review rounds per document before it will be approved.

1.4.4. SAA has three (3) months review cycle. The Contractor in the respective PIP and PMP shall consider this.

1.4.5. Once approved all the changes shall seek the standard approval process.

1.4.6. The Contractor shall produce required security related documentation or inputs to these documents using templates, provided by the Purchaser, as listed in the Table 2-1. These templates will be provided after CA.

1.4.7. The Contractor shall ensure that the all documents being part of SADS are standalone documents.

1.4.1 Security Accreditation Plan (SAP)

1.4.1.1. The Security Accreditation Plan (SAP) describes the steps to be taken to achieve security accreditation for Project ACPV.

1.4.1.2. The SAP for ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.1.3. This SAP will be made available to the Purchaser ~~not later than 2 weeks after CA~~ in accordance with Part 7 Exhibit 2 and Exhibit 6.

1.4.1.4. The Contractor shall strictly adhere to the security accreditation activities described in the SAP as approved by the SAA. All activities related with the security accreditation process identified in SAP shall be included in the respective Project Implementation Plan (PIP), Project Master Schedule (PMS) and in the Project Management Plan (PMP).

1.4.1.5. The Contractor shall update SAP regarding schedule of security accreditation based on the information available in the PMS.

1.4.1.6. Changes required by the Purchaser to be incorporated into the SAP shall be addressed by the Contractor and provided to the Purchaser who will coordinate this with SAA.

1.4.1.7. Any other changes required by the Contractor to be incorporated into the SAP shall be addressed by the Contractor and provided to the Purchaser who will (if accept the changes from the overall contractual obligation) coordinate this with SAA.

1.4.2 Initial CIS Description

1.4.2.1. The initial CIS Description will provide a framework for the development of the CIS Description and will be created by the Contractor.

1.4.2.2. Initial CISD will provide for the commencing of the accreditation process and

will be delivered to the Purchaser's SAA at the early stage of the accreditation process.

1.4.2.3. The Initial CISD ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.2.4. The Contractor shall make the iCISD available to the Purchaser not later than 2 weeks after CA.

1.4.3 CIS Description

1.4.3.1. Together with the input for the SAP, the initial CIS Description that will convert into the CIS Description for ACPV is the first document in support to security accreditation process to be developed after CA.

1.4.3.2. The CISD for ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.3.3. The Contractor shall ensure that the CIS Description is developed in the early a part of the project planning, this shall be further enhanced as the project develops; however, any changes to the CIS Description that may affect the security posture of the system shall be finalized prior to the Security Risk Assessment (SRA) compilation.

1.4.3.4. The CIS Description document shall at a minimum include the following information:

1.4.3.4.1. Detailed technical description showing the main components and the high level as well as detailed information flows, and how these are protected, inclusive of any data flow from leveraged networks/infrastructure (if any);

1.4.3.4.2. Description of all internal and external connections of the system including interconnections to other CIS;

1.4.3.4.3. List of hardware and software components used;

1.4.3.4.4. Overview of the security mechanism, which are going to be implemented in the ACPV and all its components.

1.4.3.5. The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall update the CIS Description document as many times as necessary in order to obtain SAA approval.

1.4.3.6. The Contractor shall maintain and keep the CIS Description document up to date throughout the project.

1.4.4 Security Risk Assessment Report

1.4.4.1. The Contractor shall use the NATO template "SRA Report (PILAR) Template", as listed in the Table 2-1, to document the results of the SRA and shall be approved by the SAA (through the Purchaser).

1.4.4.2. The Contractor shall develop annexes to the SRA executed in NATO PILAR tool. These annexes shall address risks not covered in the NATO PILAR, including risks related to modern CIS technologies and ACPV specific risks, which cannot be addressed in NATO PILAR tool due to its limitations.

1.4.4.3. The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct update of the SRA Report as many times as necessary in order to obtain SAA approval.

1.4.4.4. The Contractor shall maintain and keep the SRA Report up to date throughout the project.

1.4.5 Systems-Specific Security Requirement Statement

1.4.5.1. The System-specific Security Requirement Statement (SSRS) is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met.

1.4.5.2. The SSRS specifies how security is to be achieved and maintained.

1.4.5.3. The SSRS for the ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.5.4. The Contractor shall ensure the SSRS is formulated at the earliest stage of the project and shall be further developed and enhanced as the project develops.

1.4.5.5. The Contractor's developed SSRS shall:

1.4.5.5.1. To be aligned to the SRA content;

1.4.5.5.2. Describe the minimum levels of security deemed necessary to countermeasure the risk(s) identified in a risk assessment;

1.4.5.5.3. Specify details how to particular countermeasure has been implemented.

1.4.5.5.4. Have an unique identifier for each security requirement;

1.4.5.5.5. Indicate mandatory and recommended Security Measures as in Reference 6.2.7.

1.4.5.6. The SSRS shall also take into consideration parameters covering the operational environment such as the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation and other Purchaser's specific requirements.

1.4.5.7. The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct update of SSRS document as many times as necessary in order to obtain SAA approval.

1.4.5.8. The Contractor shall maintain and keep the SSRS up to date throughout the project.

1.4.6 Community Security Requirement Statement

1.4.6.1. The Contractor shall develop (if required) a Community Security Requirement Statement (CSRS) in order to address the security aspects of the community of CISs.

1.4.6.2. The CSRS for ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.6.3. The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct update of CSRS document as many times as necessary in order to obtain SAA approval.

1.4.6.4. The Contractor shall maintain and keep the CSRS up to date throughout the project.

1.4.7 System Interconnection Security Requirement Statement

1.4.7.1. The Contractor shall develop a System Interconnection Security Requirement Statement (SISRS) in order to cover security requirements for the interoperability of ACPV with other CIS to achieve the required goal of the ACPV. The SISRS shall cover all identified external connections to ACPV and be aligned to the interconnections listed in the CISD.

1.4.7.2. The SISRS for ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.7.3. The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct update of SISRS document as many times as necessary in order to obtain SAA approval.

1.4.7.4. The Contractor shall maintain and keep the SISRS up to date throughout the project.

1.4.8 Security Operating Procedures

1.4.8.1. Security Operating Procedures (SecOPs) are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel.

1.4.8.2. ACPV SecOPs shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.8.3. ACPV SecOPs shall contain separate chapters for personnel performing security management as well as administrative functions (e.g. Core Administrators, Local Administrators, CIS Security Officer, and Local

CIS Security Officers) and ACPV users[4].

1.4.8.4. ACPV SecOPs, as a minimum, shall include the following sections:

1.4.8.4.1 Administration and organization of security, including points of contact;

1.4.8.4.2 Personnel security, physical security, security of information;

1.4.8.4.3 CIS Security;

1.4.8.4.4 Incident and emergency procedures;

1.4.8.4.5 Configuration management;

1.4.8.4.6 Acceptable use policy.

1.4.8.5. ACPV SecOPs shall also cover all security requirements identified in the SRA and SSRS, which are not fully fulfilled by technical countermeasures. For example, following security procedures should be addressed (not exhaustive list):

1.4.8.5.1 System configuration and maintenance;

1.4.8.5.2 System backup;

1.4.8.5.3 System recovery, etc.

1.4.8.6. The Contractor shall take into account any comments from the Purchaser and SAA (provided to the Contractor through the Purchaser) and shall conduct update of ACPV SecOPs document as many times as necessary in order to obtain SAA approval.

1.4.8.7. The Contractor shall maintain and keep ACPV SecOPs up to date throughout the project.

1.4.9 Security Test and Verification Plan

1.4.9.1 The Security Test and Verification Plan (STVP) is a description of the security testing and verification of the CIS Security measures to be implemented for the ACPV.

1.4.9.2 The STVP for the ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.9.3 The STVP shall describe in detail:

1.4.9.3.1 tests which will demonstrate compliance with the security requirements for the ACPV identified in the respective SRA, SSRS, generic SISRS and SecOPs;

1.4.9.3.2 a complete and detailed sequence of steps that shall be followed to prove that the security mechanisms designed into ACPV enforce the security requirements identified in the

[4] If required separate SecOPs for different groups of users or locations might be developed.

SSRS.

1.4.9.3.3 Location of the test to be conducted.

1.4.9.4 The Contractor shall ensure that for each security test the following details are identified:

1.4.9.4.1 System element under test;

1.4.9.4.2 The countermeasure and its expected implementation details as per SSRS;

1.4.9.4.3 The objective of the security test

1.4.9.4.4 An outline description of the security test procedure;

1.4.9.4.5 Planned location of the test. STVP shall also distinguish between test to be conducted locally (on-site) or centrally (from DC) and tests to be executed in support of deployable elements;

1.4.9.4.6 Required verification method (i.e. Inspection, Analysis, Demonstration, Test);

1.4.9.4.7 A description of the execution of the security test (too include technical instructions how to conduct the test);

1.4.9.4.8 The pass criteria for the security test.

1.4.9.5 The Contractor shall ensure that every security test is cross-referenced to the corresponding security requirements from the ACPV SSRS (identified by the unique identifier).

1.4.9.6 The Contractor shall ensure all security requirements from the ACPV SSRS are planned for testing.

1.4.9.7 The Contractor shall also develop, provide and maintain the initial and any updated Security Implementation Verification Procedures (SIVP) for ACPV as part of the STVP.

1.4.9.8 These procedures shall consist of a set of software scripts and inspection procedures that shall allow a CIS Security Officer to verify that all components of the ACPV have been installed and configured property and comply with the SSRS and SecOPs.

1.4.9.9 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct update of STVP document as many times as necessary in order to obtain SAA approval.

1.4.9.10 The Contractor shall maintain and keep the STVP up to date throughout the project.

1.4.10 Security Accreditation Test and verification report

1.4.10.1. The Security Test and Verification Report (STVR) is a description of the results for the every instance of security testing conducted based on STVP.

1.4.10.2. The Contractor shall conduct security testing, producing the necessary Security Test and Verification Reports (STVR) based on the approved Security Test and Validation Plan (STVP).

1.4.10.3. The Subject Matter Expert (SME) designated by the Purchaser will witness execution of STVP. The SME will countersign respective STVR(s).

1.4.10.4. The Contractor shall develop the ACPV STVR for every instance of security testing conducted based on STVP.

1.4.10.5. The STVRs for the ACPV shall be developed by the Contractor based on Purchaser's provided template, as listed in the Table 2-1, and shall be approved by the SAA (through the Purchaser).

1.4.10.6. The Contractor shall, for each security test, identify the following within the STVR:

1.4.10.6.1 Test ID;

1.4.10.6.2 An outline description of the security test;

1.4.10.6.3 A detailed test case to support the test objective and outlined description;

1.4.10.6.4 The location of the conducted test;

1.4.10.6.5 The pass criteria for the security test;

1.4.10.6.6 The results of the security tests;

1.4.10.6.7 Test status (e.g. in progress, passed, failed);

1.4.10.6.8 Test completion (in per cent);

1.4.10.6.9 Failure severity (e.g. critical, high, medium, low, none);

1.4.10.6.10 Test date;

1.4.10.6.11 Any info about who conducted the test;

1.4.10.6.12 An information about who witness the test.

1.4.10.7. STVR shall contain overall test summary details:

1.4.10.7.1 Identification of the element under tests;

1.4.10.7.2 Tests starting date;

1.4.10.7.3 Tests finishing date;

1.4.10.7.4 Amount of all tests to be conducted;

1.4.10.7.5 Amount of tests executed;

1.4.10.7.6 Tests passed;

1.4.10.7.7 Tests failed;

1.4.10.7.8 Tests still in progress;

1.4.10.7.9 Amount of findings with clear distinguish of their severity (e.g. critical, high, medium, low, none).

1.4.10.8. The Contractor shall take into account any comments from the Purchaser and/or the SAA (provided to the Contractor through the Purchaser) and shall conduct update of STVR (this might require some security tests to be re-conducted) as many times as necessary in order to obtain SAA approval.

1.4.11 Approval For Testing

1.4.11.1. The Approval for Testing (AfT) request(s) for the ACPV shall be developed by the Contractor based on template provided by the Purchaser, as listed in the Table 2-1.

1.4.11.2. Approval for Testing request(s) shall be provided to the SAA (through the Purchaser) and shall contain at least the following information:

1.4.11.2.1 References to the existing Security Related Documentation for ACPV;

1.4.11.2.2 Objective of the tests;

1.4.11.2.3 Outline description of the ACPV components under tests (to include high level diagram);

1.4.11.2.4 Sites involved in testing;

1.4.11.2.5 Timeframe for testing;

1.4.11.2.6 Brief description of test activities planned to be conducted during test period.

1.4.11.3. The Contractor shall provide together with AfT request(s) accreditation related documentation being part of SADS even in the incomplete state if that would be required by the SAA to grant AfT.

1.4.11.4. The Purchaser will coordinate all AfT request(s) with the SAA. Provided that required prerequisite deliverables are available, AfT request(s) shall be provided minimum 14 working days prior to the testing itself to allow the Purchaser for the sufficient coordination with the SAA. Planning for the AfT shall consider all the required prerequisites delivery and approval e.g. Security Test and Verification Plan (STVP).

1.4.12 Security Defects Log

1.4.12.1 The Contractor shall present a plan to the Purchaser, for the Contractor's resolution of defect log entries associated with risks preventing ACPV accreditation.

1.4.12.2 The Contractor shall resolve all defects identified by the Purchaser within this plan, prior to the service acceptance.

1.5 Security Related Responsibilities

1.5.1. Table 1-3 below summarizes responsibilities related to the development of each security document given at section 1.4 above, required for security accreditation process.

1.5.2. The column “Baseline/Guidance” lists available templates, relevant NATO Security Directives and Guidance, and similar documentation.

1.5.3. The Contractor shall undertake the work identified in the column ‘Contractor Responsibility’ in Table 1-3 .

Table 1-3 - Security Accreditation Related Responsibilities

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall :)	Purchaser Responsibility
SAP	SAP Template	• Develop SAP • Update the SAP • Ensure that the SAP is a part of the Project Implementation Plan (PIP) • Deliver its input with all activities related to the security accreditation identified in the respective Project Implementation Plan (PIP) and in the Project Management Plan (PMP) • Deliver updates of the timelines	• Provide applicable documents, templates and guidance to the Contractor • Review changes • Coordination with the SAA
Initial CIS Description	CIS Description Template	• Develop Initial CISD	• Provide applicable documents, templates and guidance to the Contractor • Review changes • Coordination with the SAA
CIS Description	CIS Description Template	• Based on the design adjust it to the CIS Description template focusing on CIS security aspects • Develop CIS Description	• Provide SRA Template • Provide guidance to the Contractor • Review • Coordination with the

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall :)	Purchaser Responsibility
		• Maintain CIS Description during project duration and inform about updates.	SAA
SRA	[AC/35-D/1015] [AC/35-D/1017] Tool for formal SRA: NATO PILAR SRA Report Template	• Conduct SRA • Provide the inputs to the SRA per system design • Provide assets identification • Provide safeguards (technical and organizational measures – information security) identification and valuation • Develop SRA Report	• Provide SRA Template • Provide guidance to the Contractor • Review • Support Contractor in conducting SRA • Review • Coordination with the SAA
SSRS	[AC/35-D/1015] SSRS Template	• Develop SSRS • Provide technical input to SSRS	• Provide SSRS Template to the Contractor • Indicate SSRS sections to be completed by the Contractor • Provide guidance to the Contractor • Review • Coordination with the SAA
CSRS	CSRS Template	• Develop CSRS • Provide technical input to CSRS	• Provide CSRS Template to the Contractor • Indicate CSRS sections to be completed by the Contractor • Provide guidance to the Contractor

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall :)	Purchaser Responsibility
			• Review • Coordination with the SAA
SISRS	SISRS Template	• Develop SISRS • Provide technical input to SSRS	• Provide SISRS Template to the Contractor • Indicate SISRS sections to be completed by the Contractor • Provide guidance to the Contractor • Review • Coordination with the SAA
SecOPs	[AC/35-D/1014] SecOPs Template	• Develop SecOPs for users and system administrators	• Provide SecOPs Template to the Contractor • Indicate SecOPs Sections to be completed by the Contractor • Provide input if required • Provide guidance to the Contractor • Review • Coordination with the SAA
STVP	[AC/35-D/2005] STVP template	• Develop STVP • Develop detailed STVP test procedures	• Provide template and guidance to the Contractor • Review

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall :)	Purchaser Responsibility
			• Coordination with the SAA
STVR	[AC/35-D/2005] STVP template	• Execute STVP • Record the results of testing • Create and complete STVR	• Provide template and guidance to the Contractor • Review results of testing • Execute the tests that were not accomplished by the contractor. • Coordination with the SAA • Witness the testing conducted by the Contractor

2 REFERENCES

A.1.1 NATO SECURITY REFERENCES

A.1.1.1. The Contractor shall refer to the NATO Security Policies, Directives, Guidance and Instructions contained in Part 6 of this PWS. The list provides only general set of references and information that is more detailed might be required for the proper technical implementation of the security solutions. Required additional regulations can be provided on request should the industrial security requirements will be fulfilled.

A.2 NATO SECURITY TEMPLATES

A.2.1. The Contractor shall use the NATO Templates listed in Table 2-1.

Table 2-1 – NATO Security Templates (to be provided after Contract Award)

#	Full document Name and Reference
1	Security Accreditation Plan Template, version 4.0, dated 08 July 2016
2	CIS Description Template, version 2.1, dated 10 August 2018
3	Security Risk Assessment (SRA) Report (NATO PILAR) Template, version 1.0, dated January 2013
4	System Security Requirements Statement (SSRS) Template, version 5.0, dated 15 June 2021

#	Full document Name and Reference
5	System Interconnection Security Requirements Statement (SISRS) Template, version 1.0, dated 17 October 2014
6	Abbreviated System Interconnection Security Requirements Statement (A-SISRS) Template, version 1.0, dated 19 September 2017
7	Secure AIS Generic SecOPs, version 1.0 dated 20.06.2015
8	Generic Security Test & Verification Plan, version 2.0, dated 15 December 2021
9	Electronic Security Environment Conformance Statement (ESECS) Template, dated 05.02.2018
10	Approval for Testing Request Template, dated 23.01.2017
11	Community Security Requirement Statement template_V5.0_NU dated 22.02.2022

EXHIBIT 10

TRAINING

[This Exhibit shall provide the requirement for design and delivery of Users' training. This training programme/planning shall explain how to exploit all the functions and full performance of the delivered services. It shall cover:

1. *the approach to the training programme and in particular what and how many what Use Cases are initially will be considered, how the list / content of the use cases will be refined during implementation and how the relevant training contents will be built*
2. *the approach to the documentation of the use cases, representation and formal language*
3. *the overall training programme, structuring the learning objects in specific learning paths (e.g. standard users, advanced users and decision makers roles etc.) .*
4. *the training methodology, standards and templates, with particular emphasis to the training documentation format and contents, its reuse and continuous update following any change to the ACPV services, dataset, security domains and underpinning IT assets.]*

1.9 Training:

1.9.1 In the implementation stage the Contractor shall further develop the training plan providing all the Use Cases, the relevant documentation, planning, execution and reporting of the training programme.

1.9.2 The training shall be based either on the pre-production environment or on simulated environment encompassing all the Contractor's defined and Purchaser's accepted Use Cases for the ACPV services.

1.9.3 The contractor shall be fully responsible for the Operation and Maintenance (including administration) of the HW/SW solution defined and implemented to deliver the ACPV services.

1.9.4 The Purchaser will have full access to the training material and ACPV service documentation, without limitations to extract, modify, reproduce or destroy part or full contents with the primary scope of re-using the material for future training session or for internalization of the ACPV services.

1.9.5 ~~The Contractor shall deliver a full training programme including Training Needs Analysis (TNA), planning, preparation/design, delivery/execution and assessment of the training activities.~~

1.9.6 ~~The training programme shall cover all user training relevant to the new service.~~

1.9.7 ~~In addition to the above, the Contractor shall deliver one (1) Train-the-Trainer (TtT) training session for each new service component or service feature delivered during the duration of the contract.~~

1.9.8 ~~The Contractor shall deliver each training session up to a maximum of 10~~

~~trainees (per session).~~

1.9.9 ~~The Contractor shall deliver the training considering a 50/50 percent blend of classroom and hands-on training or propose any alternative training method for discussion and concurrence with the Purchaser (at no additional cost).~~

1.9.10 ~~In preparation of the training activities, the contractor shall deliver a draft Training Needs Analysis (TNA) and a final version in accordance with the Purchaser provided AI 16.31.11 – Requirements for the Preparation of TNA Reports.~~

1.9.11 ~~The Contractor shall deliver a draft Training Plan (including the TP-POAP, ref. 1.9.13) with the PIP and a final Training Plan at CDR including the resolution of all the comments provided by the purchaser on the draft version.~~

1.9.12 ~~The Training Plan shall describe in detail the training programme that the Contractor will implement including the proposed duration for each session, sequence of the sessions, daily planning and any other information deemed important for the correct planning and execution of the trainings.~~

1.9.13 ~~The Contractor shall develop and deliver the Training Plan (TRNP) in accordance with the Purchaser provided Agency Instructions:~~

- ~~AI 16.31.04 – Requirements for the preparation of TRNP~~
- ~~AI 16.31.04 Annex A – Training POAP (Plan On A Page)~~
- ~~AI 16.31.04 Annex B – Training Feedback Form~~
- ~~AI 16.31.04 Annex C – Training Evaluation Report Form~~

1.9.14 ~~The Contractor's proposed duration of the trainings shall be accepted by the Purchaser and be adequate to the content, complexity and required knowledge to be transferred to the trainees in accordance with the requirements of this PWS and the result of the TNA required above. .~~

1.9.15 ~~The Contractor shall propose to the purchaser the formats and templates for the training data and material at CDR.~~

1.9.16 ~~Upon review of the proposed format and templates for the training data and material, the purchaser will provide comments (if any) or acceptance within four (4) working weeks from the reception of Purchaser's proposed format and templates for the training data and material.~~

1.9.17 ~~In case of comments of the purchaser, the Contractor shall provide an amended version of the format and templates for training not later than two (2) working weeks from the reception of Purchaser's comments.~~

1.9.18 ~~The Contractor shall prepare/design the training data and material on the basis of the performance levels and requirements defined in this PWS.~~

1.9.19 ~~The training data and material shall be delivered to the PM not later than eight (8) working weeks before the expected training for Purchaser review and acceptance before training start.~~

1.9.20 ~~Upon review of the training data and material, the purchaser will provide~~

~~comments (if any) or acceptance within four (4) working weeks.~~

1.9.21 ~~In case of comments of the purchaser, the Contractor shall provide an amended version of the training data and material not later than two (2) working weeks from the reception of Purchaser's comments.~~

1.9.22 ~~The Contractor shall be responsible for the timely provision on the training site/location of the following training data and material for each trainee:~~

- ~~trainee guidebook;~~
- ~~Training material, properly structured and organized, including (but not limited to) video/audio material, drawings and procedures, slides/presentations, COTS documentation etc.;~~
- ~~Final training test questionnaire;~~
- ~~Completion certificates (upon successful completion of the final test).~~

1.9.23 ~~The Contractor shall be responsible for the instructor material and tools (instructor's guidebook, laptop, portable projector etc.).~~

1.9.24 ~~The Contractor shall be fully responsible for the quality, content, completeness and correctness of the training material and shall implement the modifications, corrections and improvements required by the Purchaser to achieve acceptance and deliver the training accordingly.~~

1.9.25 ~~The training and training material shall be delivered in simplified English language and the instructor shall be fluent in English or proficient and certified in English language (STANAG 6001 level 4333 at least).~~

1.9.26 ~~Any training session/course shall be delivered by an instructor with a minimum of two (2) years' experience of the product/system/capability involved.~~

EXHIBIT 11

TECHNICAL SOLUTION DESIGN

[This Exhibit shall be developed according to the collaborative discussions during the sprints of the dynamic sourcing process. The Contractor shall provide a technical solution design with sufficient level of detail to ensure the overall IT coherence and understand the architecture of the solution, its interfaces with the NATO systems and support the security accreditation process.

This TSD is an initial deliverable based on Contractor assumptions that would be refined and finalized as part of the service design phase.]