NORTH ATLANTIC TREATY ORGANISATION
HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

REQUEST FOR PROPOSAL

RFP-ACT-SACT-26-02

Capability Development Management Support (CDMS)

Part B
Amendment Five

LC#	POSITION TITLE	PRIMARY LOCATION	NUMBER OF CANDIDATES
10	FULL STACK DEVELOPER	ON-SITE	3
12	DEVSECOPS ENGINEER	ON-SITE	1
22	SENIOR CONTRACTOR SUPPORT TO ACT OFFICE OF INTERNAL AUDIT	ON-SITE	1
32	CYBERSPACE CONCEPT DEVELOPER & VALIDATOR	ON-SITE	1
33	CYBERSPACE WARFARE DEVELOPMENT ENGINEER	ON-SITE	1
39	SUPPORT TO THE ACT SECURITY CIS ACCREDITATION AUTHORITY	ON-SITE	1
~~41~~	~~SUPPORT TO THE ACT MISSION SECURITY COORDINATOR~~	~~ON-SITE~~	~~1~~
42	CONTRACTOR SUPPORT TO CAPABILITY LIFECYCLE AI/ML ENGINEER	ON-SITE	1
43	SUPPORT FOR BUSINESS ANALYSIS AND REQUIREMENT MANAGEMENT	ON-SITE	1
44	CONTRACTOR SUPPORT TO ANALYTICS SPECIALIST – CAPABILITY LIFECYCLE (ENGINEERING)	ON-SITE	1
45	CONTRACTOR SUPPORT TO CAPDEV QUALITY MANAGEMENT BRANCH, QUALITY ASSURANCE ANALYST	ON-SITE	2
46	NATO DIGITAL BACKBONE SYSTEMS ANALYST (AKA COMMAND NETWORK SYSTEMS ANALYST)	ON-SITE	1
47	NUCLEAR CONSULTATION COMMAND & CONTROL (NC3) COORDINATION SUPPORT SECRETARIAT	ON-SITE	1
48	PROTOCOL SPECIALIST	ON-SITE	1
49	ICS DATA ANALYSTS	ON-SITE	1

BIDDING INSTRUCTIONS

1. General

a. This is a **Firm Fixed Price Level of Effort** contract in accordance with the HQ SACT General Terms and Conditions;

b. HQ SACT General Terms and Conditions Dated **January 2026** are applicable to this procurement and can be located on the ACT Website at; **WWW.ACT.NATO.INT/CONTRACTING** under Contractor Information.

c. Contract Award is contingent upon funding availability; Partial bidding is allowed.

2. Classification

This Request for proposal (FFP) is a NATO UNCLASSIFIED document.

3. Definitions

a. The “Prospective Bidder” shall refer to the entity that has indicated thereon its intention without commitment, to participate in this RFP.

b. The term “Bidder” shall refer to the bidding entity that has completed a bid in response to this RFP.

c. The term “Contractor” shall refer to the bidding entity to whom the contract is awarded.

d. The term “Contracting Officer” designates the official who executes this RFP on behalf of HQ SACT.

e. “Contracting Officer`s Technical Representative” or “COTR” is the official who is appointed for the purpose of determining compliance of the successful bid, per the technical specifications.

f. The term “HQ SACT” shall refer to Headquarters Supreme Allied Commander Transformation.

g. The term “ACT” shall refer to Allied Command Transformation.

h. The term “NATO” shall refer to the North Atlantic Treaty Organization.

i. The term “days” as used in this RFP shall, unless otherwise stated, be interpreted as meaning calendar days.

4. Eligibility

a. This RFP is open to governmental or commercial entities:

b. Established in a North Atlantic Treaty Organization Alliance member nation.

c. Working in the required field of study and legally authorised to operate in the country and countries in which this contract is to be performed, at the time of bidding. Has performed the desired past performance including size, cost and scope, as described in this RFP.

d. All proposed key personnel on this requirement must be citizens of a NATO member nation.

e. **For on-site contractors wherein a security clearance is required, the Contractor Company must hold a Facilities Security Clearance (FSC) at NATO or National SECRET or above IAW AC/35-D/2003-REV5 and ACT D 070-001.**

1) If the bidder does not have an active FSC at the time of bidding and/or there is a national process that precludes issuing an FSC until award, the bidder may indicate this within the proposal in lieu of providing the FSC information.
2) If the bidder is successful, however, any contract award shall be on a provisional basis and final award will not be approved until the NSA/DSA has provided an assurance that the bidder has been granted an FSC at the required level.
3) The bidder is not expected to manage any materials at the facility during the bidding period or project delivery in this case.
4) **Bidders are requested to investigate national FSC procedures and advise the anticipated approval timeline within the proposal**.

5. Duration of Contract

a. The contract awarded shall be effective upon date of award.

b. Period of Performance: **Refer to Annex A for Period of Performance for each Labor category.**

c. Option periods shall be exercised at the sole discretion of the HQ SACT Contracting Officer, based on satisfactory work performance, availability of funding, and ongoing evolving requirements.

6. Exemption of Taxes

In accordance with the agreements (Article VIII of the Paris Protocol dated, 28 August 1952) goods and services under this contract are exempt from taxes, duties and similar charges.

7. Amendment or Cancellation

a. HQ SACT reserves the right to amend or delete any one or more of the terms, conditions or provisions of the RFP prior to the date set for bid closing. A solicitation amendment or amendments shall announce such action.

b. HQ SACT reserves the right to cancel, at any time, this RFP either partially or in its entirety. No legal liability on the part of HQ SACT shall be considered for recovery of costs in connection to bid preparation. All efforts undertaken by any bidder shall be done considering and accepting, that no costs shall be recovered from HQ SACT. If this RFP is cancelled, any/all received bids shall be returned unopened, per the bidder's request.

8. Bidder Clarifications

a. Prospective Bidders should seek clarification at their earliest convenience. Any explanation regarding the meaning or interpretation of this RFP, terms, clause, provision or specifications, shall be requested in writing, from the Contracting Officer. All Contracting Officers listed on this RFP must receive such requests via email for clarification no later than **18 February 26.**

b. In lieu of a bidder's conference, HQ SACT invites bidders to submit technical and contractual questions not later than **18 February 26.**

c. Information in response to all inquiries / requests for clarification to a prospective bidder shall be furnished to all prospective bidders at the following link: http://www.act.nato.int/contracting as a Question-and-Answer addendum. All such addendums and any necessary solicitation amendments shall be incorporated into this RFP. Verbal Interpretations shall not be binding.

9. Bid Closing Date

Bids shall be received at HQ SACT, Purchasing and Contracting Office, no later than **1 April 2026, 0900 hours, Eastern Standard Time, Norfolk, Virginia, USA.** No bids shall be accepted after this date and time. **No hard copy proposals will be accepted.** Please see Proposal Submission (paragraph 12) for more details.

EXCEPTION TO CLOSING FOR THE FOLLOWING LABOR CATERGORIES

LC22 - SENIOR CONTRACTOR SUPPORT TO ACT OFFICE OF INTERNAL AUDIT
LC39 – SUPPORT TO THE ACT SECURITY CIS ACCREDITATION AUTHORITY
LC49 - ICS DATA ANALYSTS

will have a separate closing date of **13 April 2026 0900 hours, Eastern Standard Time, Norfolk, VA, USA**. No bids shall be accepted after this date and time. No hard copy proposals will be accepted. Please see Proposal Submission (paragraph 12) for more details.

10. Bid Validity

a. Bids shall remain valid for a period of one hundred and twenty days (120) from the applicable closing date set forth within this RFP. HQ SACT reserves the right to request an extension of validity. Bidder shall be entitled to either grant or deny this extension of validity. HQ SACT shall automatically consider a denial to extend the validity as a withdrawal of the bid.

b. **HQ SACT will not accept supplier proposals prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to chatbots, such as Chat Generative Pre-Trained Transformer (Chat GPT), or other language generating tools. HQ SACT reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at HQ SACT's sole discretion, and HQ SACT reserves the right to take further steps in such cases as appropriate.**

11. Content of Proposal

The proposal shall consist of two (2) separate documents (Technical / Price) sent via e-mail as per the instructions. No hard copy proposals will be accepted. The E-mailed documents shall be received no later than **1 April 2026, 0900 hours, (LC 22/39/49 13 April 2026 0900 hours) Eastern Standard Time, Norfolk, Virginia, USA.**

The company description portion of its technical proposal shall be limited to 10 pages.

In accordance with HQ SACT General Terms and Conditions – Companies must request approval – in advance of submission – before proposing a candidate currently serving on another HQ SACT contract. Failure to do so will result in non-review of the candidate. Requests will be considered on a case-by-case basis giving consideration to impact on HQ SACT priorities.

Companies are encouraged to coordinate with HQ SACT Contracting Officer on submission of previous NATO contractors to ensure successful past performance.

a. **Technical Proposal shall be a Signed PDF document and contain:**

1) A table of contents for the entire proposal (See Enclosure #1):

2) The bidder's full name, address, Point of Contacts, Telephone, Fax number; Internet site;

3) Compliance statement (See Enclosure#2);

4) Past performance (See Enclosure #3);

5) List of key personnel;

6) Provision of technical volumes;

7) Compliance matrix (See Annex B to Statement of Work).

8) FSC Information (See Enclosure #6)

b. **Price Proposal shall be submitted as an Excel Spreadsheet and:**

1) **Shall be in U.S. Dollar Currency.** Contractor may request payment post award in alternate currency based on agreed conversion rate.

2) Prices shall be on a **Firm Fixed Price Basis** and include any relevant discount schedule.

3) Price proposal may be provided as supplemental PDF document if excel workbook cannot be signed – but should be submitted together with the excel workbook.

12. Proposal Submission

a. Proposals shall be separate e-mail submissions to:

Technical proposal: **hqsact.techproposal@nato.int**

Price proposal: **hqsact.priceproposal@nato.int**

b. E-mail subjects shall include the solicitation information along with company name (for example: RFP -ACT-SACT-26-02_Tech_ABC Inc. / RFP -ACT- SACT-26-02_Price_ABC Inc.). Allow sufficient time in sending your submission should you encounter e-mail size challenges.

c. No verbal bids or verbal modifications or telephonic bids shall be considered.

d. It is the ultimate responsibility of a prospective bidder prior to submission that all proposal submissions are reviewed to ensure they meet the technical, contractual and administrative specifications and that offers meet the limitations and expressed conditions.

13. Late Proposals

a. It is solely the bidder`s responsibility that every effort is made to ensure that the proposal reaches HQ SACT prior to the established closing date and time. No late bids shall be considered.

b. **A delay in an e-mail exchange due to server or size restrictions does not constitute a delay by NATO.**

14. Bid Withdrawal

A bidder may withdraw their bid up to the date and time specified for bid closing. Such a withdrawal must be completed in writing with attention to the HQ SACT Contracting Officer.

A bid withdraw will be annotated on the Contract Award Report.

15. Bid Evaluation

a. The evaluation of bids and determination as to the responsiveness and technical adequacy or technical compliance, of the products or services requested, shall be the responsibility of HQ SACT. Such determinations shall be consistent with the evaluation criteria specified in the RFP. HQ SACT is not responsible for any content that is not clearly identified in any proposal package.

b. HQ SACT reserves the right conduct pre-award discussions with proposed key personnel to accurately assess identified technical competencies. Discussions will be limited to scope of this RFP and the evaluation criteria identified.

c. Proposals shall be evaluated and awarded taking into consideration of the following factors:

1) Successful administrative submission of bid packages as requested in paragraph 11 and as listed in this RFP.

2) Successful determination of compliance. (Compliant/non-compliant).

3) Technical factors / pricing factors rated the following:
Technical / Price = 70/30 (Best Value)

DEVIATIONS FROM THIS TECHNICAL /PRICE FACTOR WILL BE ADDRESSED IN THE INDIVIDUAL LABOR CATEGORIES IF APPLICABLE.

4) The overall proposed hourly rates and the total hours indicated in the solicitation will be the basis of the Price Evaluation.

5) Technical clarifications as determined may be conducted.

6) Acceptance of HQ SACT General Terms and Conditions.

16. Proposal Clarifications

During the entire evaluation process HQ SACT reserves the right to discuss any bid clarify what is offered, interpret language within the bid, to resolve in potential areas of concern.

17. Award

a. HQ SACT intends to award a firm fixed price level of effort contract(s) to the Offeror(s) whose proposal(s) represents the Best Value offer to NATO. Partial awards are authorized.

b. HQ SACT will collect information from references provided by the Offeror regarding its past performance. Contractors must provide authorization to contact references.

c. HQ SACT reserves the right to negotiate minor deviations to the listed General Terms and Conditions to this RFP.

18. Surge Capability:

A surge capability requirement is included to have a contract vehicle in place should emerging circumstances require a quick and temporary increase in contractor support (LOE or Deliverable) to meet new requirements within the scope of the existing Statement of Work. The Supplier shall be prepared to provide support services per labour category described above. The contractor shall be prepared to evaluate requirements and submit a price proposal for any new in scope requirement for consideration by HQ SACT. Surge proposals will be evaluated by the Contracting Officer for fair and reasonable pricing and should be developed based upon the same pricing structure as the original contract proposal. The rate for surge effort shall not exceed the base/option year rate. Surge requirements will be incorporated by formal contract modification. Requests for pricing are made on a non-committal basis and do not constitute a formal commitment by HQ SACT to contract for additional work; supplier will not be reimbursed costs for preparing price proposals or other related expenses in response to a surge request. HQ SACT surge efforts will not exceed 50% of the annual contract value or 50% of the cumulative contract value. Requests to surge from other organizations outside of HQ SACT are not counted against the HQ SACT when calculating the surge tolerances

19. Disputes

Disputes will be settled between the bidder and the Contracting Officer by mutual agreement through negotiation, while respecting and observing NATO regulations and policies.

20. Proposed Candidates

If successful, contractor company must notify HQ SACT of any special accommodations or requirements of its personnel for on-site support.

21. Communications

All communication related to this RFP, between a prospective bidder and HQ SACT shall only be through the nominated HQ SACT Contracting Officer. Designated contracting staff shall assist the HQ SACT Contracting Officer in the administrative process. There shall be no contact with other HQ SACT personnel regarding this RFP. Such adherence shall ensure Fair and Open Competition with equal consideration and competitive footing leverage to all interested parties.

22. Points of Contact

(PLEASE INCLUDE ALL BELOW ON ALL CORRESPONDENCE)

Tonya Bonilla, ACT Contracting Officer, 757-747-3575; Tonya.bonilla@nato.int
Louise Syms, ACT Contract Specialist, 757-747-3788; Louise.syms@nato.int

Enclosure 1: Proposal Content / Checklist

PROPOSAL CONTENT / CHECKLIST

Table of Contents

☐ Bidder's name, address, POC, Contact numbers, email address.

☐ Compliance Statement.

☐ Past Performance (including References).

☐ List of Key Personnel.

☐ Technical Proposal.

☐ Price Proposal (Excel worksheet – Enclosure 4 - provides mandatory price proposal format)

Enclosure 2: Compliance Statement

COMPLIANCE STATEMENT TO SEALED BID RFP-ACT-SACT-26-02

It is hereby stated that our company has read and understands all documentation issued as part of this RFP. Our company proposal submitted in response to the referenced solicitation is fully compliant with the provisions of this RFP and the intended contract with the following exception(s); such exemptions are considered non-substantial to the HQ SACT solicitation provisions issued.

Clause	Description of Minor Deviation
----------	----------
----------	----------

(If applicable, add another page)

Company:_____

Signature:

Name &Title:_____ Date: _____

Company Bid Reference: _____

Bidder's proposal must be based on full compliance with the terms, conditions and requirements of the RFP and all future clarifications and/or amendments. The bidder may offer variations in specific implementation and operational details provided that the functional and performance requirements are fully satisfied. In case of conflict between the compliance statement and the detailed evidence or explanation furnished, the detailed evidence/comments shall take precedence/priority for the actual determination of compliance. Minor or non-substantial deviations may be accepted. Substantial changes shall be considered non- responsive.

Enclosure 3: Past Performance Information Form

(Company is required to submit minimum of one. Company should be clear how **both the company and candidate meet the requirements of past performance.** Reference to a contract must include a detailed description of the work performed relevant to the requirements outlined in the SOW. Generic or Vague references to the contract awarded without clear connection to work performed will be disqualified)

(a) Contracting Entity:

(b) Contract No:

(c) Type of Contract (Firm Fixed Price, IDIQ, Requirements):

(d) Title of Contract:

(e) Description of Work Performance and Relevance to Current Acquisition (Type of facility, capacity, estimated patronage, summary of staff used):

(f) Contract Dollar Amount:

(g) Period of Performance:

(h) Name, Address, Fax and Telephone No. of Reference:

(i) Indicate Whether Reference Acted as Prime or Sub-contractor:

(j) Comments regarding compliance with contract terms and conditions:

(k) Complete Contact Information for client:

(l) Permission to contact client for reference: Yes / No

Name/Signature of Authorized Company Official: _____
_____

This Enclosure is designed to assist the respective company provide HQ SACT with all necessary documents/information required. For clarification, please refer to bidding instructions in part 1 of subject solicitation.

Enclosure 4: Mandatory Price Proposal Excel Spreadsheet

Pricing shall be submitted using the excel workbook provided. Bidders may elect to submit a second PDF proposal for pricing **if the excel workbook is provided as well.**
Proposals not submitted in the proper format will not be considered.

Formulas have been added for convenience; however, it is the company's responsibility to ensure that the formulas are correctly reflecting your expected bid proposal value.

Enclosure 5: Security Aspects Letter

HQ Supreme Allied Commander Transformation
Purchasing and Contracting Section
Office of Budget and Finance
Norfolk, Virginia | USA

27 January 2026

From: HQ SUPREME ALLIED COMMANDER
TRANSFORMATION HEAD OF CONTRACTS
7857 Blandy Road, Suite 100
Norfolk, VA 23551-2490

Subject: RFP-ACT-SACT-26-02 NATO SECURITY ASPECTS LETTER

Reference: A) AC/35-D/2003-REV5 – Directive on Classified Project and Industrial Security

To whom it may concern,

In the performance of subject contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the National Security Agency/Defense Counterintelligence Security Agency (NSA/DCSA) of the nation in which the work is performed or in the contracts involving NATO RESTRICTED (NR) information only as established in the Contract Security Clause.

All classified information and material shall be protected in accordance with the requirements established by the NSA/DCSA of the nation in which the work is performed or in the case of NR information or above as may also be established in the Contract Security Clause.

In particular, the Contractor shall:

Appoint an officer to be responsible for supervising and directing security measures in relation to the Request for Proposals (RFP), contract or sub-contract;

Submit in due time to the NSA/DCSA the personal particulars of the person the contractor wishes to employ on the project with his/her Personnel Security Clearance (PSC) at the required level where NATO CONFIDENTIAL (NC) and above is involved;

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

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

Supply the NSA/DCSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information;

Maintain a record of 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;

Deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DCSA or in the case of NR information as determined by the need-to-know;

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;

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;

Report to Security Officer and to the appropriate NSA/DCSA 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/DCSA, such as reports on holdings of NATO classified information or materiel;

Obtain written authorisation of programme/project office and NSA/DCSA 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 by contract;

Undertake not to utilise, other than for the specific purpose of the bid, contract or sub-contract, without the written permission of the programme/project office or the prime Contractor, any NATO classified information supplied, and return to the 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 my direct; and

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

Any person taking part in the performance of work of classified parts of which are to be safeguarded, must possess the appropriate NATO security clearance issued by his NSA/DCSA. 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 in involved.

Unless specifically authorised to do so by the 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.

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.

No Communication and Information Systems (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 the Contract Security Clause (Annex 4) of reference A).

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.

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.

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.

The Contractor shall be required to acknowledge receipt of an accompanying Security Aspects Letter (SAL) or Program security Instruction (PSI) that is made part of the applicable contract bidding documents 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 Contract Security Clause and specifically that any company CIS used to handle or process NR classified information or above has been appropriately security accredited.

TONYA BONILLA
HQ SACT Contracting Officer

CONTRACTOR ACKNOWLEDGEMENT

The Contractor acknowledges receipt of this Security Aspects Letter that is made part of the applicable contracts and confirm that it understands and will comply with the security aspects defined. The Contractor further acknowledges that it will comply with the provisions of the Contract Security Clause, specifically any contractor CIS used to handle or process NR classified information has been appropriately security accredited.

Company:

_____

Contractor’s Facility:

_____

Security Officer’s Name (print):

_____

Security Officer’s Signature:

_____

Date:

_____

Enclosure 6 Facilities Security Clearance Details

Facilities Security Clearance Information

Please initial appropriate boxes

This information will be used to seek validation from the appropriate NSA/DSA – Self Certification will not be accepted.

	I confirm that [company name] holds a Facilities Security Clearance at the appropriate level.
	I confirm that the proposed candidate is an employee of [company name] and therefore is covered under [Company Name} FSC

Facilities Security Officer (FSO)

Name:

Title:

E-mail Address:

Phone Number:

Company NSA/DSA [nation]

	I confirm that the proposed candidate is a subcontractor of [company name] working for [Sub-Contractor Company Name] and that the subcontractor holds a Facilities Security Clearance at the appropriate level.

Subcontractor Company Facilities Security Officer (FSO)

Name:

Title:

E-mail Address:

Phone Number:

Company NSA/DSA [nation]

ANNEX A: STATEMENT OF WORK (SOW) FOR CAPABILITY DEVELOPMENT MANAGEMENT SUPPORT (CDMS)

Background

In recent years, NATO nations have launched a variety of innovation-focused initiatives in the military domain to leverage the unprecedented pace of technological development, much of it driven by the commercial sector. NATO responded by establishing a senior-level Innovation Board chaired by the Deputy Secretary General, which confirmed Allied Command Transformation's (ACT) role to "…play the leading role for innovation in NATO." ACT has since adapted its structures and processes to align with the ambitions of NATO nations and ensure innovation is delivered at speed and scale.

To deliver on this mandate, ACT has adopted Agile DevSecOps principles, emphasizing rapid, iterative delivery cycles and user-driven development. Many capability development efforts are software-intensive, while others integrate hardware and software into larger systems and services. Modern continuous integration and delivery toolsets are applied to ensure transparency, traceability, and responsiveness, allowing solutions to be developed, fielded, and refined quickly while remaining aligned with operational requirements.

The growing demand for digital solutions has led to an expanding backlog of projects requiring sustained contractor support. Contractors are embedded within ACT's cross-functional teams, working alongside staff in product-centric development efforts. These teams deliver Minimum Viable Products (MVPs) through rapid development cycles while simultaneously exploring emerging technologies that combine hardware and software integration. This dual-track approach ensures NATO can meet immediate operational needs while also experimenting with novel solutions that strengthen long-term capabilities.

To sustain and expand this capability, HQ SACT is seeking contractor support across multiple labor categories, including Solution Architects, DevSecOps Engineers, Full-Stack Developers, UI/UX Designers, Security Professionals, Acquisition and Contracting Specialists, Product Managers, Systems Engineers, Network Engineers, and Service Desk Operators. Contractors will be integrated into ACT teams under the guidance of the Contracting Officer's Technical Representative (COTR), working within an Agile DevSecOps framework to deliver user-centric, operationally relevant solutions at speed.

The contractor may be required, at the direction of the COTR, to undertake official travel in support of ACT, both within and outside NATO boundaries, for a maximum of 30 days per year or as otherwise agreed.

While no security clearance is required for remote contractors for the contract award, the contracting authority reserves the right to require an appropriate clearance at any point during contract execution. In such cases, reasonable processing times for the issuance of the clearance will be accepted and taken into account.

LABOR CATEGORY 10: FULL-STACK DEVELOPER

Location: Norfolk, VA, USA (On-site)

Number of Candidates: Three (3) personnel required

Period of Performance:

Base Period: Award – 31 December 2026 with four potential 12 – month options, 1 January 2027 – 31 December 2027, 1 January 2028 – 31 December 2028, 1 January 2029 – 31 December 2029, 1 January 2030 – 31 December 2030

Tasking

1. Build containerized application tools following the 12-Factor App methodology, Test Driven Development (TDD), and Extreme Programming (XP).
2. Develop products as part of a balanced agile team (Product Manager, Product Owner, UI/UX Designer, and Data Scientists as applicable).
3. Design and implement REST APIs and microservices architecture.
4. Develop full-stack solutions using modern JavaScript, Python, and/or Java frameworks.
5. Perform front-end development (e.g., React, Angular) and back-end development (e.g., Node.js, Django/Flask, SpringBoot).
6. Conduct database design and programming (e.g., MySQL, PostgreSQL, MongoDB).
7. Deploy containerized applications using Docker, Kubernetes, or OpenShift.
8. Work in a collaborative, pair programming environment as needed.
9. Rapidly learn and apply new programming languages, frameworks, and tools.
10. Support the creation of sustainable DevSecOps pipelines and agile delivery practices.

Essential Qualifications

1. Minimum 4 years of experience in full-stack development using JavaScript, Python, or Java.
2. Minimum 4 years of experience in front-end development (React, Angular, etc.) and/or back-end development (Node.js, Django/Flask, SpringBoot, etc.).
3. Minimum 4 years of experience in database design/programming (MySQL, PostgreSQL, etc.).
4. Experience in REST API design and development.
5. Experience with Test Driven Development (TDD).
6. Experience in Microservices Architecture.
7. Experience deploying containerized applications with Docker, Kubernetes, or OpenShift.
8. Experience working in collaborative, agile teams.
9. Experience delivering iterative releases in an Agile/DevSecOps environment.
10. Fluent in English (oral and written) at SLP 3333 or equivalent.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 10: FULL-STACK DEVELOPER (ON-SITE)

Each candidate must have a separate compliance matrix.

Item	Compliant	Non-Compliant
Minimum of one past performance citation within the last seven years to show successful completion of similar work.		
Fluent in English both written and oral.		
Active NATO or National SECRET (or higher) security clearance.		
Minimum of **50 Points** in the Subject Matter Expert Criteria.		
Proposed key personnel citizen of NATO member nation.		

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience.** **Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result in disqualification.**	**Page/Paragraph/Line Reference**	**Score 100 Points**
1. Experience in developing innovative digital products in a NATO or National defense institution	Every 1 year = 2 points (max **12 points**)		
2. Full-stack development (JS/Python/Java)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
3. Modern Front-End Frameworks (React/Angular)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
4. Modern Back-End Frameworks (Node.js, Spring Boot, Django/Flask)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
5. REST API / GraphQL / gRPC	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
6. Microservices Architecture + Cloud-Native Principles	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
7. Containers & Orchestration (Docker, Kubernetes, OpenShift)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
8. CI/CD + DevSecOps (pipelines, security integration)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		

9. Test Driven Development + Automation Frameworks	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
10. Database Systems (SQL + NoSQL, streaming/Kafka, etc.)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
11. Experience delivering iterative releases in an Agile/DevSecOps environment	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
12. Balanced team and pair programming	<4 yrs: 1 point 4-6 yrs: 2 points 7–9 yrs: 3 points 10+ yrs: **4 points**		
13. 4-year university degree in relevant field (computer science/systems engineering)	Relevant CS/Engineering degree = **4 points** Otherwise = 0 points		

LABOR CATEGORY 12: DEVSECOPS ENGINEER

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One (1) candidate required

Period of Performance:

Base Period: Award – 31 December 2026 with four potential 12 – month options, 1 January 2027 – 31 December 2027, 1 January 2028 – 31 December 2028, 1 January 2029 – 31 December 2029, 1 January 2030 – 31 December 2030

Tasking

1. Deploy and operate containerized services using orchestration frameworks to ensure scalability and resilience.
2. Automate infrastructure through Infrastructure as Code (IaC) to provide consistent and repeatable environments.
3. Deploy and monitor workloads in cloud environments (AWS, Azure, Google Cloud, VMware, OpenStack).
4. Implement site reliability engineering (SRE) and observability practices to ensure resilience, monitoring, logging, metrics, and distributed tracing.
5. Support high-throughput and service-oriented architectures, ensuring resilient and scalable deployments.
6. Deliver incremental capabilities in Agile and DevSecOps environments following frameworks such as Scrum, SAFe, or Kanban.
7. Design and manage secure networking and service meshes (TLS, Istio, Linkerd, API gateways) to ensure encrypted and reliable service-to-service communication.
8. Apply zero-trust principles and compliance automation to enforce security policies and validate system compliance.
9. Manage identity and access using secure methods for secrets, tokens, certificates, and least privilege access control.

Essential Qualifications

1. Minimum 4 years of experience with containerization and orchestration (Docker, Kubernetes, OpenShift).
2. Minimum 4 years of experience in designing and maintaining CI/CD pipelines with automated testing and security validation.
3. Experience with Infrastructure as Code (Terraform, Ansible, Helm, Pulumi).
4. Experience deploying and securing workloads in hybrid/public cloud environments (AWS, Azure, Google Cloud, VMware, OpenStack).
5. Experience implementing site reliability engineering and observability practices (Prometheus, Grafana, ELK/Loki, OpenTelemetry).
6. Experience implementing scalable, resilient, high-throughput systems and service-oriented architecture.
7. Experience delivering capabilities in Agile/DevSecOps environments (Scrum, SAFe, Kanban).

8. Experience designing and managing secure networking and service mesh (TLS, Istio, Linkerd, API gateways).
9. Experience applying zero-trust principles and compliance automation (OPA, Kyverno, SBOM, CIS benchmarks).
10. Experience managing secrets and access policies using modern IAM solutions (Vault, AWS KMS, Azure Key Vault, RBAC/ABAC).
11. Fluent in English (oral and written).

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (including other citizenships):

Best Value Criteria for LABOR CATEGORY12: DEVSECOPS ENGINEER (ON -SITE)

Item	Compliant	Non-Compliant
Minimum of one past performance citation within the last seven years to show successful completion of similar work.		
Fluent in English both written and oral.		
Active NATO or National SECRET (or higher) security clearance.		
Minimum of 50 Points in the Subject Matter Expert Criteria.		
Proposed key personnel citizen of NATO member nation.		

Subject Matter Expert Criteria (100 pts possible)

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience.** **Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result in disqualification.**	**Page/Paragraph/Line Reference**	**Score 100 Points**
1. Experience in developing and adapting a DevSecOps platform to allow Agile and innovative development in a NATO or National defense institution	Every 1 year = 2 points (max **12 points**)		
2. Designing, operating, and securing containerized workloads at scale (Docker, Kubernetes, OpenShift)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
3. Designing and maintaining pipelines with integrated automated testing and security validation (Jenkins, GitLab, GitHub Actions, PyTest, Selenium, SAST/DAST)	<4 yrs: 1 point 4–6 yrs: 3–6 points 7–9 yrs: 7–9 points 10+ yrs: **10 points**		
4. Deploying and managing environments using automated, testable IaC tools (Terraform, Ansible, Helm, Pulumi)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
5. Running and securing workloads in hybrid/public cloud environments (AWS, Azure, Google Cloud, VMware, OpenStack)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
6. Ensuring resilience and operational visibility through monitoring, logging, metrics,	<4 yrs: 1 point 4–6 yrs: 2–4 points		

and distributed tracing (Prometheus, Grafana, ELK/Loki, OpenTelemetry)	7–9 yrs: 5–7 points 10+ yrs: **8 points**		
7. IaaS. Implementing scalable, resilient, high-throughput systems and service-oriented architectures (SOA, distributed systems, performance tuning)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
8. Delivering incremental capabilities using Agile and DevSecOps practices (Scrum, SAFe, Kanban)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
9. Designing and managing secure networking and encrypted service-to-service communication (TLS, Istio, Linkerd, API gateways)	<4 yrs: 1 point 4–6 yrs: 3–6 points 7–9 yrs: 7–9 points 10+ yrs: **10 points**		
10. Applying zero-trust principles and policy-as-code to enforce compliance automatically (OPA, Kyverno, SBOM, CIS benchmarks)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
11. Managing secrets, certificates, and access policies to enforce least privilege (Vault, AWS KMS, Azure Key Vault, RBAC/ABAC)	<4 yrs: 1 point 4–6 yrs: 2–4 points 7–9 yrs: 5–7 points 10+ yrs: **8 points**		
12. Relevant Degree in Computer Science, Engineering, or related discipline	Yes = **4 points** No = 0 points		

LABOR CATEGORY 22: SENIOR CONTRACTOR SUPPORT TO ACT OFFICE OF INTERNAL AUDIT – HQ SACT

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: Award – 31 December 2026, Option Period One: 1 January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028, Option Period Three: 1 January 2029 – 31 December 2029, Option Period Four: 1 January 2030 – 31 December 2030.

Taskings:

1. Conducts compliance and integrity audits, inspections, reviews, and audit tests in accordance with international auditing standards, and ACT audit policies and procedures. Reviews protocols and advises ACT leadership on regulations and policies.

2. Assess and evaluate ACT's compliance with applicable laws and regulations. This involves conducting detailed reviews of travel activities (travel plans, travel approvals, travel claims, etc.).

3. Analyze, consolidate, and update the ACT audit universe (requires significant spreadsheet analysis) to reflect the actual activities undertaken, in Travel, Finance, programmes of work, and Human Resources. Reconciliation and joining of branch information and plans will be necessary to provide organizational overview, branch review, and deep dive audits and inspections where necessary.

4. Determine the effectiveness of management response to previous audit recommendations, internal control risk and compliance with applicable NATO and ACT financial policies. Support senior leadership in their daily decision-making relating to emerging travel non-compliance and ACT's implementation of NATO's and ACT's anti-fraud and corruption strategies and directives.

5. Respond to potentially serious or irregular compliance issues and violations, and consults with management on appropriate responses.

6. Support to other audit activities approved in ACT's annual Risk Based Audit Plan covering all aspects of the ACT audit universe.

7. Analyze internal audit processes and update ACT internal audit manuals to adapt to agile auditing of areas that rapidly changes within the yearly planning cycle.

8. Develop and conduct audit risk assessment of ACT resource management activities to continue risk-based auditing and identify risk areas. When needed, update internal audit methodology to reflect the right risk assessments and audit universe.

9. Review the execution, implementation, status and effectiveness of ACT's travel management and risk management process; report on the status and effectiveness of risk registers and advise on all governance issues arising from these reviews.

10. To undertake ad-hoc analyses and studies if relevant as tasked by the Chief of Staff and ACT Head of Internal Audit.

Essential Qualifications

1. University Degree in accounting, finance, business administration or related discipline and 4 years function related experience, or Higher Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 5 years post related and 4 years function related experience.
2. 6 or more years of experience performing compliance, integrity, and/or forensic auditing.
3. 4 or more years of experience in travel management (and associated Internal Controls) and/or auditing travel management (planning, requisitions, claim liquidation, etc.) in a large organization.
4. Experience in retrieving, compiling, structuring, statistical and non-statistical sampling, and analyzing large data sets of financial and travel information.
5. Experience with Accounting software and Microsoft office, particularly Excel, PowerPoint and Word applications.
6. Hold a recognized professional fraud examiner (CFE) and/or professional accounting (CPA, CMA, etc.) qualification.
7. Proven forensic accounting or forensic investigation experience.
8. Proven ability to communicate clearly and persuasively, both orally and in writing to senior management (specialist and non-specialist audiences).
9. Without conflicts of interest with any ACT staff.

Annex B
Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Best Value Criteria for LABOR CATEGORY 22 SENIOR CONTRACTOR SUPPORT TO OFFICE OF INTERNAL AUDIT – HQ SACT

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Note: Each candidate within this category must have their own compliance matrix.

Item	Compliant	Non-Compliant
Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
No conflicts of interest with any ACT staff.		
Minimum of **70 Points** in the Subject Matter Expert Criteria		

Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item **PLEASE ENSURE TOTAL PTS EQUAL 100**	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience.** **Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification.** **ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1. University Degree in accounting, finance, business administration, or related discipline and 4 years function related experience, or Higher Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 5 years post related and 4 years function related experience.	Non-Compliant in Education or years of experience: 0 points High School With 5 Years Post Related Experience & 4 Years Function Related Experience: 10 Point Bachelor's Degree With 4 Years Function Related Experience: 20 points Bachelor's Degree With 4+ Years Function Related Experience: 30 points		
1. 6 or more years of experience performing compliance, integrity, and/or forensic auditing.	Less than 6 years (0 Points) 6 years (10 Points) 6+ years (20 points)		

2.	4 or more years of experience in travel management (and associated internal controls) and/or auditing travel management (planning, requisitions, claim liquidation, etc.) in a large organization.	Less than 4 years (0 Points) 4 or more years travel management experience (10 Points) 4 or more years travel management audit experience (10 Points) 4 or more years of both (20 points)		
3.	Experience in retrieving, compiling, structuring, statistical and non-statistical sampling, and analysing large datasets of financial and travel information.	Yes (5 Points) No (0 Points)		
4.	Experience with accounting software and Microsoft Office, particularly Excel, PowerPoint and Word applications.	Yes (2.5 Points) No (0 Points)		
5.	Hold a recognized professional fraud examiner (CFE) and/or professional accounting (CPA, CMA, etc.) qualification.	Professional fraud examiner qualification (5 Points) Professional accounting qualification (10 points) Both of above (15 points) No (0 Points)		
6.	Proven forensic accounting or forensic investigation experience.	Yes (5 Points) No (1 Points)		
7.	Proven ability to communicate clearly and persuasively, both orally and in writing, to senior management (specialist and non-specialist audiences).	Yes (2.5 Points) No (0 Points)		

LABOR CATEGORY 32: CYBERSPACE CONCEPT DEVELOPER AND VALIDATOR (ONE CANDIDATE)

Location : Norfolk, VA, USA (On-site)

Number of Candidates: One candidate.

Period of Performance: Base Period: Award – 31 December 2026, Option Period One: 1 January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028, Option Period Three: 1 January 2029 – 31 December 2029, Option Period Four: 1 January 2030 – 31 December 2030.

Taskings:

1. Based on NATO operational needs, literature review, high-level direction and guidance (notably stemming from ACT's Warfare Development Agenda), and guidance from ACT Cyberspace Technical Director, **identify cyberspace operation capability concepts to be developed**.
   [For information: Building on previous efforts on Cyberspace Situational Awareness (CySA), follow-on capability concepts are expected to be developed in the area of decision-support and Cyberspace Command and Control (CyC2), to name a few.]
2. **Develop the identified cyberspace operation capability concepts**, by conducting all the necessary activities, including, but not limited to, initial research, input collection, concept aim/scope definition, concept drafting, submission, and approval.
3. **Build and maintain Communities of Interest** (NATO organizations, Nations, Industry, Academia) dedicated to the development and implementation of cyberspace operation concepts, in close coordination with the Technical Director and ACT Cyberspace Federation & Partnership SME.
4. **Contribute to experimentation and validation efforts** related to the cyberspace operation concepts (feasibility analysis, experiment design and preparation, assessment, etc.), under the guidance of the Technical Director.
5. **Develop (as lead or contributor) relevant engineering products/artefacts** to support cyberspace capability development and implementation. This includes capability requirements identification and definition across all DOTMLPFI[1] aspects, Analyses of Alternatives, architecture development, Information Exchange Requirements definition, operational evaluation/validation, and interoperability assessment.
6. **Support and contribute to other warfare development activities** related to concept implementation and engineering (feasibility studies, foresight analysis, technical and operational analysis, experimentation campaigns, etc.).
7. **Inform, organize and participate** in meetings, workshops, conferences and other events, and travel to attend those, as needed, generally within NATO's boundaries for up to 20 days per year.
8. **Perform additional tasks**, related to the contract, as required by the COTR.

[1] Doctrine, organization, training, material, leadership and education, personnel, facilities, interoperability.

Essential Qualifications

Note: Hands-on experience in system engineering activities, including definition, implementation and engineering of operational/military concepts throughout the complete capability life cycle, is essential. In general, management experience, team leading, participation and/or contribution to the above activities will not suffice to qualify.

1. Master's degree in engineering, systems engineering or computer science. A bachelor's degree and 5 years of recent experience in system engineering, capability concept development and implementation in a military context will be considered in lieu of a master's degree.
2. Proven recent (at least three within the last five years) post-degree hands-on experience in authoring cyberspace concepts, specifications, architectures, functional analysis, designs, preferably in the area of military information and cyber systems. Experience at the level of management, overseeing, participating or supporting shall not be accounted for.
3. Post-degree education in CIS security and cyber defence disciplines, as Certified Information Systems Security Professional (CISSP), GIAC Security Expert or ISACA Certified Information Security Manager (CISM).
4. Post-degree hands-on experience in architecture drafting, preferably using NATO Architectural Framework (NAF) or similar standard (e.g. TOGAF).
5. Demonstrated experience in planning, coordinating and executing workshops for various stakeholders including governmental agencies, academia and industry.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 32: CYBERSPACE CONCEPT DEVELOPER AND VALIDATOR

Each candidate within this category must have their own compliance matrix.

Item	Compliant	Non-Compliant
Minimum of one past performance citations within the last five years to show that he/she has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of **70 Points** in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item	Range Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT	Page, Paragraph and Line Number referencing where candidates meet the criteria and how.	Score (100 pts possible).
1. Master's degree in engineering, systems engineering or computer science. A bachelor's degree and 5 years of recent experience in system engineering, capability concept development and implementation in a military context will be considered in lieu of a master's degree.	• No degree: 0 points • Bachelor's degree only: 1-5 points • Bachelor's degree and 5 years of recent experience in system engineering in military context: 6-10 points • Master's degree: **11-15 points**		
2. Professional cyberspace-related certification in CIS security and cyber defence disciplines, as Certified Information Systems Security Professional (CISSP), GIAC Security Expert or ISACA Certified Information Security Manager (CISM).	• No post-degree training: 1 point • Two or more cyber security certificates below CISSP/GSE or CISM: 5 points • CISSP / GSE or CISM: **15 points**.		
3. Proven recent (at least three within the last five years) post-degree hands-on experience in authoring cyberspace concepts, specifications, architectures, functional analysis, designs, preferably in the area of military information and cyber systems. Experience at the level of management,	• No experience: 1 point. • Less than 5 years, 2-3 points. • Five or more years in areas other than military cyber, 5-15 points. • Five or more years in military cyber concepts, **16-20 points**		

overseeing, participating supporting or using shall not be accounted for			
4. Proven experience (at least three within the last seven years) experience in the design, development, management and/or expert level operation of military systems, preferably in the areas of: • Operational Command and Control (C2). • Tactical Command and Control (C2). • Situational awareness (domain awareness and recognized/common operational pictures). • Operational planning. • Tactical planning.	• No experience: 0 points. Otherwise add scoring for the technologies below, for a maximum of **25 points:** • Operational C2: 6 points. • Tactical C2: 4 points. • Situational awareness: 8 points • Operational planning: 4 points • Tactical planning: 3 points		
5. Participation of 5 or more years (during the last seven) in large (20+ people) program teams, preferably related to the development of military cyberspace capabilities, in two or more of the following roles: main concept developer, concept development team management, systems engineering (requirements, architectures, design), military software development, lead community of interest building, planning and	• Less than two roles: 1 point. Otherwise add scoring for the roles below, for a maximum of **25 points:** • Main concept developer: 8 points • Concept development team management: 2 points • Systems engineering: 3 points • military software development: 4 points • lead community of interest building: 4 points		

coordination of large multinational events.	• Planning and coordination of large multinational events: 4 points		

LABOR CATEGORY 33: CYBERSPACE WARFARE DEVELOPMENT ENGINEER (ONE CANDIDATE)

Location : Norfolk, VA, USA (On-site)

Number of Candidates: One candidate.

Period of Performance: Base Period: Award – 31 December 2026, Option Period One: 1 January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028, Option Period Three: 1 January 2029 – 31 December 2029, Option Period Four: 1 January 2030 – 31 December 2030.

Taskings:

1. Based on NATO operational needs, requirements, literature review, and high-level direction and guidance from ACT Programme Director, **develop, describe and document cyber capabilities**, including:
    a. Develop, analyse, validate, complete and enhance **capability requirements**, departing from operational requirements, to translate them into specifications for the capability description.
    b. Develop or support the development and documentation of **capability architectures**.
    c. Develop or support the development of **capability specifications**, including functional and non-functional specifications.
    d. Develop or support the development of **implementation plans**, including analysis of scope, timelines, cost and risk.
2. **Build and maintain Communities of Interest** (NATO organizations, Nations, Industry, Academia) dedicated to the development and implementation of cyberspace capabilities, in close coordination with the Technical Director and ACT Cyberspace Federation & Partnership SME.
3. Use those Communities of Interest to develop and **validate the products** resulting from tasking 1, above.
4. **Support and contribute to other capability development activities,** including feasibility studies, foresight analysis, technical and operational analysis, experimentation campaigns, etc.
5. **Inform, organize and participate** in meetings, workshops, conferences and other events, and travel to attend those, as needed, generally within NATO's boundaries for up to 20 days per year.
6. **Perform additional tasks**, related to the contract, as required by the COTR.

Essential Qualifications

Note: Hands-on experience in system engineering activities, including definition, implementation and engineering of complex cyber defence and/or cyberspace capabilities is essential. In general, management experience, team leading, participation and/or contribution to the above activities will not suffice to qualify.

1. Master's degree in engineering, systems engineering or computer science. A bachelor's degree and 5 years of recent experience in system engineering, capability development and implementation in a military context will be considered in lieu of a master's degree.

2. Proven recent (at least three within the last five years) post-degree hands-on experience in authoring specifications, architectures, functional analysis and designs, preferably in the area of military information and cyber systems. Experience at the level of management, overseeing, participating or supporting shall not be accounted for.

3. Post-degree education in CIS security and cyber defence disciplines, as Certified Information Systems Security Professional (CISSP), GIAC Security Expert or ISACA Certified Information Security Manager (CISM).

4. Post-degree hands-on experience in architecture drafting, preferably using NATO Architectural Framework (NAF) or similar standard (e.g. TOGAF).

5. Expert-level certification at the level of Programme Management Professional (PMP), AXELOS Management of Successful Programmes (MSP) or Project Professional Qualification (PPQ).

6. Demonstrated experience in planning, coordinating and executing workshops for various stakeholders including governmental agencies, academia and industry.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & Nation):

Best Value Criteria for LABOR CATEGORY 33: CYBERSPACE WARFARE DEVELOPMENT ENGINEER (ONE CANDIDATE)

Note: Each candidate within this category must have their own compliance matrix.

Item	Compliant	Non-Compliant
Minimum of one past performance citations within the last five years to show that he/she has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of **70 Points** in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

	Range **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1. Master's degree in engineering, systems engineering or computer science. A bachelor's degree and 5 years of recent experience in system engineering, capability development and implementation in a military context will be considered in lieu of a master's degree.	• No degree: 0 points • Bachelor's degree only:2- 5 points • Bachelor's degree and 5 years of recent experience in system engineering in military context: 6-10 points • Master's degree: **11-15 points**		
2. Professional cyberspace-related certification in CIS security and cyber defence disciplines, as Certified Information Systems Security Professional (CISSP), GIAC Security Expert or ISACA Certified Information Security Manager (CISM).	• No post-degree training: 1 point • Two or more cyber security certificates below CISSP/GSE or CISM: 2-4 points • CISSP / GSE or CISM: **5-10 points**.		
3. Proven recent (at least five within the last ten years) post-degree hands-on experience in authoring specifications, architectures, functional analysis and designs, preferably in the area of military information and cyber systems (Experience at the level of management, overseeing, participating, supporting or	• No experience: 0 points. • Less than 5 years, 1-3 points. • Five or more years in areas other than military cyber, 4-5 points. • Five or more years in military/cyber areas, **6-10 points**.		

using shall not be accounted for).			
4. Post-degree hands-on experience in architecture development, preferably using NATO Architectural Framework (NAF) or similar standard (e.g. TOGAF), and preferably applied to military/NATO systems. Experience at the level of management, overseeing, participating, supporting or using shall not be accounted for.	• No experience: 1 point. • Less than 3 years: 2 points. • 3 years or more without NAF/TOGAF or in applications other than military/NATO: 3-5 points. • 3 years or more with NAF/TOGAF and applied to military/NATO systems: **6-10 points.**		
5. Post-degree hands-on experience (team management, oversight, contribution, support or use will not suffice) in the development/coding of large software systems (> $50M and > 100,000 lines of code) preferably for cyberspace operations capabilities (including cyber situational awareness, cyber-Command and Control, Cyber Threat Intelligence), including rapid prototyping and Minimum Viable Product (MVP) development.	• No experience: 0 points. • Less than three years in small non-cyber projects: 1-5 points • 3 years or more in large non-cyber projects: 6-10 points • Less than 3 years in small, non-cyber projects: 11-15 points. • 3 years or more in small cyber projects: 16-20 points • 3 years or more in large, cyber projects: **21-25 points.**		
6. Hands-on experience, at the level of developer and programmer (team manager, architect, contributor, support, user community, etc. will not suffice) of complex tools and applications using the following technologies (do not score on technologies for abilities are less than at the “expert” level): a. DevSecOps b. Cloud services (Azure, AWS, etc.) c. Containers (Docker, Kubernets) and Virtual	• Less than two technologies at expert level: 1 point. Otherwise add scoring for the technologies below, for a maximum of **20 points**: • Experience in DevSecOps: 4 points • Experience in Cloud services: 2 points • Experience in Containers: 2 points		

Machines (VMware, Hyper-V, etc.) d. Development environments (GitHub / GitLab, VS, etc.) e. Programming languages (Python, Java, etc.) f. Databases and Data Lakes (AWS S3, SQL, etc.) g. AI for development / AI coding / Vibe coding (Cursor, Replit, GitHub Copilot, Lovable, etc.)	• Experience in Development environments: 2 points • Experience in Programming languages: 2 points • Experience in Databases and Data Lakes: 2 points • Experience in AI for development / AI coding / Vibe coding: 6 points		
7. Participation of 5 or more years (during the last 7) in large program teams, preferably related to the development of military cyberspace capabilities, in two or more of the following roles: a. engineering team management b. systems engineering (requirements, architectures, design) c. product development d. planning and coordination of large multinational events	• Less than two roles: 1 point. Otherwise add scoring for the roles below, for a maximum of **10 points**: • Engineering team management: 4 points • Systems engineering: 2 points • Product development: 2 points • Planning and coordination of large multinational events: 2 points.		

LABOR CATEGORY 39: SUPPORT TO THE ACT SECURITY CIS ACCREDITATION AUTHORITY

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: Contract Award – 31 December 2026, Option Period One: 1 January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028, Option Period Three: 1 January 2029 – 31 December 2029

The Communication and Information System (CIS) Security Section within AOS provides support to the ACT Security Accreditation Authority. Due to an increase in the number of CIS required to undergo security accreditation, the CIS Section does not have the capacity to provide timely security accreditation support to all CIS in ACT. Further ACT, as a whole, has 60 currently operational systems or applications that have failed to become accredited previously due to these manning constraints. This violates requirements set forth in Security Committee's Guidelines for Security Accreditation of CIS (AC/35-D/1021-REV3), HQ SACT Internal Security Instruction for CIS (HQ SACT DIR 70-6), and the Security Accreditation Strategy for ACT Managed and Operated CIS (AOS TT-0660) and presents a major security risk. Thus, temporary staffing is required to work the backlog of accreditation.

Taskings:

A. Maintain records of the progress of a CIS through NATO security accreditation processes and the application of NATO security regulations.
B. review of security accreditation documentation for CIS and make recommendations for approval. Security accreditation documentation includes the CIS Description, Risk Assessment Results, System-Specific Security Requirements Statement, Security Operating Procedures, Security Test & Validation Plan, Security Test & Validation Results, Incident Reports, etc.
C. Ensure that verification activities are properly executed, to confirm that the agreed security measures have been implemented
D. Provide support and guidance to CIS developers and service providers. Note that some developers and service providers are based in Europe.
E. Contribute to updates of the statement of the security risk for ACT CIS
F. Liaising with other roles in the Security Accreditation process
G. Representing the ACT SAA in NATO Enterprise meetings, either in person or via VTC.

Essential Qualifications

1. 3 or 4 year university degree or equivalent national academic qualification in computer science, network security, cyber-security or related field.
2. Certification in CIS security or cyber defence disciplines provided by a recognised certification scheme, as a Certified Information Systems Security Professional

(CISSP), GIAC Security Expert or ISACA Certified Information Security Manager (CISM).

3. At least 5 years demonstrated experience in CIS security, CIS development or CIS service delivery
4. Within the 5 years' experience above, at least 3 years of demonstrated experience working in or in direct support of a national, international or multi-national CIS security accreditation, certification or similar field
5. Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.
6. Active NATO or National SECRET (or higher) security clearance issued by the industrial security authority of a NATO member nation
7. Valid NATO Nation passport with no travel restrictions to NATO nations
8. Minimum of 70 Points in the Subject Matter Expert Criteria
9. Writing - Ability to prepare written documentation to transfer technical information about concepts, situations, products, services, or results to audiences with varying levels of technical knowledge. Thorough understanding of grammar, sentence structure, and intended audiences to the process of reviewing, editing, or constructively critiquing a document, publication, or message.
10. Communication - Skill in clearly and effectively conveying information verbally to senior leadership. Ability to deliver clear, effective communication and ability to take responsibility for understanding others. Ability to ask appropriate questions.
11. Computer Skills - Has the knowledge and ability to use computers and related technology efficiently. Proficient in Microsoft Office products (e.g. Word, PowerPoint, Excel, Access, Project, MS Teams, and SharePoint)

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Best Value Criteria for LABOR CATEGORY 39

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Item	Compliant	Non-Compliant
Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Contractor Company holds Facilities Security Clearance at NATO or National SECRET or Higher		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of **70 Points** in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item	Range Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT	Page, Paragraph and Line Number referencing where candidates meet the criteria and how.	Score (100 pts possible)
1. 3 or 4 year university degree or equivalent national academic qualification in computer science, network security, cyber-security or related field.	Degree in directly related field – 20 points Degree in numeric discipline (e.g. engineering, physics, statistics, mathematics) – 15 points No degree / non-numeric discipline – 0 points		
2. Certification in CIS security or cyber defence disciplines provided by a recognised certification scheme, as a Certified Information Systems Security Professional (CISSP), GIAC Security Expert or ISACA Certified Information Security Manager (CISM), or equivalent COMPTIA certification.	5 points per relevant certification, up to a maximum of 25		
3. At least 5 years demonstrated experience in CIS security, CIS development or CIS service delivery.	Less than 5 years – 0 points 5 years or more – 5 to 20 points		
4. Within the 5 years' experience above, at least 3 years of demonstrated experience working in or	3 years of experience working as an accreditor / certifier: 20 to 35 points		

in direct support of a national, international or multi-national CIS security accreditation, certification or similar field.	3 years of demonstrated experience with an accreditor / certifier to achieve security accreditation of a CIS: 5 to 25 points Less than three years' experience in security accreditation: 1 points		

LABOR CATEGORY 41: SUPPORT TO THE ACT MISSION SECURITY COORDINATOR

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: 1 September 2026 – 31 December 2026, Option Period One: January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028

Background Information:

The Headquarters Allied Command Transformation (HQ SACT), under the ACT Office of Security (AOS), plays a central role in NATO's transformation process, ensuring the security of personnel, assets, and sensitive information. The Force Protection (FP) team is tasked with ensuring the safety and security of HQ SACT staff during external events and missions, both within NATO's areas of responsibility and internationally. This includes both Diamond Events (high-profile engagements) and regular official travel

The Force Protection (FP) team is responsible for the safety and security of HQ SACT Staff during external events and missions. The FP Staff Officer performs the planning, coordination, and execution of all Diamond events within the Host Nation (HN) and abroad, and security coordination of all missions of SACT HQ personnel. A Mission Security Coordinator should be identified to organize and carry out the safety and security responsibilities of all travel duties of HQ SACT personnel as well as support the Section during external event.

A Mission Security Coordinator is essential to the FP section for the successful monitor, consultation and debriefing of the HQ SACT personnel that is travelling for duty reasons all over the world. Coordination with external security advisory agencies to helping HQ SACT protect its assets, employees, and events outside the United States is the main duty of the Mission Security Coordinator. In addition, supporting the organization and management of Diamond events with local actors (businesses, law enforcement agencies, organizations, etc.), which supports the generation of critical threat and risk assessment is requested. This post will be instrumental and unique in providing dedicated attention to security and safety matters that may arise to those travelling personnel and attendees of events.

Tasking:

This contract provides technical support to the ACT Mission Security

Coordinator. Specific responsibilities include

1. Analyse reports from the ACT travel database (FINs) to identify high-risk destinations and critical travel locations for HQ SACT personnel.

2. ~~Collect and analyze security information from multiple sources, including open-source intelligence (OSINT), classified reports, and local security advisories, to assess risks and threats in advance of travel.~~

3. ~~Provide comprehensive security briefings to HQ SACT travelers, offering specific advice on security protocols, local risks, and mitigation strategies tailored to individual missions and events.~~

4. ~~Develop security plans for high-risk events and missions, ensuring that all travel and event operations comply with NATO's security policies and procedures.~~

5. ~~Perform regular risk assessments and security audits to identify vulnerabilities at planned event sites and provide recommendations for risk mitigation.~~

6. ~~Lead site surveys to assess potential vulnerabilities at event venues, developing actionable security reports, and risk mitigation strategies based on findings.~~

7. ~~Examine attendee lists for non-NATO participants and evaluate counterintelligence (CI) risks, identifying individuals or groups who may pose a security threat to NATO personnel or operations.~~

8. ~~Prepare security briefs for top leaders/management approval; format to be coordinated with FP Staff Officer and FP Assistant.~~

9. ~~Be present at the host venues during events to assist Delegate Assistance Centres/Registration and Check in Desks, to provide security assistance and oversight.~~

10. ~~Coordinate security efforts for Diamond Events and external missions with local authorities, law enforcement, and intelligence agencies. This includes managing security logistics, site assessments, and emergency response protocols~~

11. ~~Assist in the on-site security management of events by providing oversight at Delegate Assistance Centres, registration desks, and check-in points, ensuring that security protocols are followed, and that personnel are appropriately safeguarded.~~

12. ~~Prepare after-action reports (AARs) and post-event analyses, identify key security challenges, and document security protocols for future reference.~~

13. ~~Work with the FP team to generate lessons learned products and historical security documents, ensuring that insights gained during events and missions are used to improve future planning and risk management strategies.~~

14. ~~Ensure compliance with NATO's documentation standards for all security-related reports and briefings, ensuring that all security incidents and lessons are formally recorded.~~

15. ~~Provide briefings and consultations to internal NATO stakeholders at all levels, including FP officers, NATO Command leadership, and event planners, regarding security requirements, risk management, and operational priorities.~~

16. Collaborate with local agencies and international organizations to ensure security policies and procedures are harmonized with NATO's requirements for personnel safety.

Essential Qualifications:

1. A minimum of 5 years' experience in security administration, risk management, criminology, public administration, or industrial security administration. Experience must include specific responsibility for planning, coordination, and execution of security operations for high-profile events, international travel, or multinational operations
2. At least 3 years' experience in planning, managing, and executing security measures for major events involving VIPs, senior leadership, or large-scale international operations. This should include experience in conducting risk assessments, site security surveys, and coordination with local law enforcement, intelligence agencies, and emergency responders.
3. Possession of a recognized certification in Risk Management (e.g., PMP, CRMP, or equivalent) or another relevant security-related qualification. Additional certifications in counterterrorism or crisis management will be considered an asset.
4. Demonstrated ability to collect, analyze, and interpret security-related data from open-source intelligence (OSINT) and other classified or unclassified sources. Demonstrated ability to develop comprehensive security briefings, risk assessments, and incident reports for both senior leadership and operational teams i.
5. Demonstrated ability to engage effectively with stakeholders at all levels, including senior leadership, internal teams, external security agencies, and local law enforcement. This includes providing briefings, coordinating security measures, and ensuring effective communication during mission execution.
6. Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.
7. Must possess an active NATO SECRET (or higher) security clearance issued by a NATO member nation's industrial security authority. Clearance must be maintained throughout the period of performance.
8. Advanced proficiency in Microsoft Office Suite (Word, Excel, PowerPoint), security databases, and collaborative tools (e.g., SharePoint, Teams). Ability to utilize online resources for open-source intelligence gathering and use various digital platforms for planning, coordination, and reporting.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below to ascertain whether the individuals have adequate qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 41: SUPPORT TO THE ACT MISSION SECURITY COORDINATOR

Item	**Compliant**	**Non-Compliant**
Minimum of one past performance citation within the last seven years to show that it has successfully completed work that is similar or **directly traceable to the requirements outlined in the Statement of Work**		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		

Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of 60 Points in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience.** **Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1.Education and training in Risk Management;	No education or training – 1 point Basic introduction to risk management (e.g. Risk management foundation) – 2 to 15 points Advanced training in risk management (e.g. Risk management practitioner) – 16 to **25 points**		

2.At least 2 years' experience in security administration, criminology, public administration, industrial security administration, law or related discipline for specific task related skills	<2 years – 0 points (NON-COMPLIANT) 2-5 years – up to 15 points >5 years – 16 to **25 points**		
3. At least 1 years' experience in planning and managing security for major events;	<1 year – 0 points 1-2 years – 1-5 points 2-5 years – 6-15 points >5 years – 16-**20 points**		
4.Ability to collect and analyse security information from open sources and deliver detailed security briefings to the travellers	Yes - 1-**15 points** No - 0 points (NON-COMPLIANT)		
5.Ability to engage with stakeholders at all levels, both in briefing and during execution of events	Yes - 1-**15 points** No- 0 points (NON-COMPLIANT)		

LABOR CATEGORY 42: CONTRACTOR SUPPORT TO CAPABILITY LIFECYCLE AI/ML ENGINEER

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: 1 July 2026 – 31 December 2026, with 4 potential 12-month option periods; 1 January – 31 December 2027, 1 January – 31 December 2028, 1 January – 31 December 2029, 1 January – 31 December 2030.

Background Information:

1. Deputy Chief of Staff Capability Development (DCOS CAPDEV) acts as the Supreme Allied Commander Transformation's Director for guidance, direction and co-ordination of the activities and resources of the Capability Development Directorate. CAPDEV is responsible to:

a. Identify and prioritize Alliance capability development from short to long term, ensuring coherence between all capabilities within the CAPDEV portfolio.
b. Lead the determination of required capabilities and prioritization of shortfalls to inform the delivery of materiel and non-materiel solutions across the Doctrine, Organisation, Training, Material, and Leadership, Personnel, Facilities and Interoperability (DOTMLPFI) lines of effort to enable a holistic approach to capability development, ensuring improved interoperability, deployability and sustainability of Alliance Forces.

2. The future Capability Development Directorate will include enduring functionality to effectively plan and manage coherent through life capability development, aligned to NATO's strategic intent and priorities. The CAPDEV Data and Analytics Office (DAO) is responsible to DCOS for managing the data and platform operations for Capability Lifecycle, Requirements, and P3M data as well as providing analytics as service and enabling self-service analytics for CAPDEV decision makers.

3. As part of ongoing organisational functional reviews, CAPDEV is in the process of implementing measures for improved capability development planning and management, including the way it collects, manages, analyses and reports on capability development and delivery information, both legacy and current.

Taskings — Capability Lifecycle AI/ML Engineer

1. **AI/ML Model Development**: Design, develop, train, and deploy machine learning models to support forecasting, risk identification, readiness assessment, and decision support across the capability lifecycle.
2. **Advanced Analytics Integration**: Integrate AI/ML models into enterprise analytics workflows, dashboards, and reporting solutions to enable operational use by analysts and decision-makers.
3. **Data Preparation and Feature Engineering**: Develop and maintain data preparation pipelines, feature engineering processes, and training datasets in coordination with data engineering teams to ensure model accuracy, robustness, and traceability.

4. **Cloud-Based AI/ML Engineering**: Implement and operate AI/ML solutions within approved cloud environments, including model training, deployment, and orchestration using secure, scalable architectures.
5. **Model Lifecycle Management**: Establish and execute model validation, performance monitoring, retraining, and version control processes to ensure sustained accuracy and operational relevance of deployed models.
6. **Responsible AI Practices**: Apply responsible and explainable AI principles, including transparency, bias awareness, and interpretability, appropriate to defence and decision-support contexts.
7. **Automation and Optimization**: Identify and implement opportunities to automate analytic workflows, model execution, and data processing to improve efficiency and reduce manual intervention.
8. **Prototyping and Experimentation**: Design and deliver proof-of-concept and prototype AI/ML solutions, including exploration of emerging techniques (e.g., large language models or incremental learning), aligned with DAO priorities.
9. **Performance and Scalability Optimization**: Optimize AI/ML pipelines and supporting infrastructure to ensure reliable performance under operational workloads and evolving data volumes.
10. **Technical Documentation**: Produce and maintain comprehensive technical documentation describing AI/ML models, data dependencies, assumptions, limitations, and operational integration points.
11. **Stakeholder Engagement**: Collaborate with analysts, engineers, and stakeholders to translate operational requirements into AI/ML solutions and explain analytic outputs to technical and non-technical audiences.
12. **Knowledge Transfer**: Deliver knowledge transfer, mentoring, and technical guidance to DAO personnel to support long-term sustainment of AI/ML capabilities.
13. **Security and Compliance**: Ensure AI/ML development and deployment comply with NATO and organizational security, data protection, and classification handling requirements.
14. **Capability Lifecycle Support**: Apply AI/ML expertise to support requirements-based planning, capability development, delivery monitoring, and performance assessment activities.
15. **Continuous Improvement**: Identify opportunities to enhance AI/ML methods, tooling, and practices in alignment with DAO's Decision Advantage objectives.
16. **Technical Support**: Provide ongoing technical support and troubleshooting for AI/ML models, pipelines, and integrated analytic solutions.
17. **Additional Tasks**: Perform additional tasks as required by the COTR in scope of this labor category.

Essential Qualifications:

1. 8+ years of progressive professional experience in data science, advanced analytics, and/or machine learning engineering, including experience delivering operational analytics or decision-support solutions in complex enterprise environments.
2. Demonstrated expertise in machine learning and statistical modeling, including development, training, validation, and deployment of models supporting forecasting, risk analysis, performance assessment, or decision support across business or capability lifecycles.

3. Demonstrated experience designing and operating automated data pipelines, including ETL/ELT workflows, feature engineering, and data transformation processes to support analytics and AI/ML workloads.
4. Demonstrated professional experience with cloud-based analytics and AI/ML platforms, including deployment and operation of models and data pipelines in secure, scalable cloud environments.
5. Bachelor's degree in Data Science, Computer Science, Mathematics, Engineering, Statistics, or a related quantitative discipline.
6. Demonstrated experience integrating AI/ML solutions into enterprise analytics tools, dashboards, or reporting platforms to support operational use by analysts and decision-makers.
7. Demonstrated experience with model lifecycle management, including performance monitoring, retraining strategies, version control, documentation, and optimization for production environments.
8. Demonstrated experience working within governed or regulated environments, including adherence to data governance, security, and compliance requirements relevant to defence, security, or other highly regulated domains.
9. Demonstrated ability to collaborate across multidisciplinary teams, including analysts, data engineers, platform engineers, and system administrators, to deliver interoperable, production-ready analytics solutions.
10. Demonstrated ability to communicate complex analytical and AI/ML concepts clearly to both technical and non-technical stakeholders, supporting effective adoption and operational use of delivered solutions. Demonstrated minimum NATO or National SECRET clearance with the appropriate national authority for the duration of the contract.
11. Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.
12. Demonstrable proficiency in effective oral and written communication, including briefing and coordinating with business stakeholders.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 42: CONTRACTOR SUPPORT TO CAPABILITY LIFECYCLE AI/ML ENGINEER

	Item	**Compliant**	**Non-Compliant**
1	Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
2	Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
4	Active NATO or National SECRET (or higher) security clearance		
5	Valid NATO Nation passport with no travel restrictions to NATO nations		
6	Proficiency in the use of the Microsoft Office Tool suite and collaborative software		

7	Minimum of 60 Points in the Subject Matter Expert Criteria		
8	**Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)**		

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification.** **ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1. 8+ years of progressive professional experience in data science and/or machine learning engineering, with at least 5 years within the last 8 years of demonstrated experience designing, developing, and deploying AI/ML models that directly support forecasting, risk analysis, performance assessment, or decision support in enterprise or defense-related environments.	8+ years progressive experience AND 5+ recent years of exact matching experience – 20 points 6–7 years progressive experience AND 3–4 recent years of exact matching experience – 12 points 4–5 years progressive experience AND 1–2 recent years of partial matching experience – 6 points Less than 4 years of relevant experience – 2 points		
2. 8+ years of progressive professional experience, with at least 5 years within the last 8 years of demonstrated experience deploying AI/ML models into production environments, including	8+ years progressive experience AND 5+ recent years of exact matching experience – 20 points 6–7 years progressive experience AND 3–4 recent		

monitoring, retraining, version control, and lifecycle management within secure, regulated, or governed contexts.	years of exact matching experience – 12 points 4–5 years progressive experience AND 1–2 recent years of partial matching experience – 6 points Prototype-only or limited operational experience – 2 points		
3. 6+ years of progressive professional experience, with at least 3 years within the last 6 years of demonstrated experience designing and operating automated data pipelines (ETL/ELT), feature engineering processes, and data preparation workflows that directly support analytics and AI/ML workloads.	6+ years progressive experience AND 3+ recent years of exact matching experience – 15 points 4–5 years progressive experience AND 2 recent years of exact matching experience – 9 points 3–4 years progressive experience AND 1 year of partial matching experience – 5 points Less than 3 years of relevant experience – 2 points		
4. 6+ years of progressive professional experience, with at least 3 years within the last 6 years of demonstrated experience implementing analytics and AI/ML solutions using modern cloud platforms in secure or enterprise environments.	6+ years progressive experience AND 3+ recent years of exact matching experience – 15 points 4–5 years progressive experience AND 2 recent years of exact matching experience – 9 points 3–4 years progressive experience AND 1 year of partial matching experience – 5 points Less than 3 years of relevant cloud experience – 2 points		

5. 5+ years of progressive professional experience, with at least 2 years within the last 5 years of demonstrated experience integrating AI/ML outputs into analytics platforms, dashboards, or reporting tools used operationally by analysts or decision-makers.	5+ years progressive experience AND 2+ recent years of exact matching experience – 10 points 3–4 years progressive experience AND 1 recent year of exact matching experience – 6 points 2–3 years progressive experience with partial matching integration experience – 3 points No demonstrated operational integration experience – 1 point		
6. 5+ years of progressive professional experience, with at least 2 years within the last 5 years of demonstrated experience applying responsible AI practices, model governance, documentation, explainability, validation, and compliance appropriate to enterprise or defense decision-support environments.	5+ years progressive experience AND 2+ recent years of exact matching experience – 10 points 3–4 years progressive experience AND 1 recent year of exact matching experience – 6 points 2–3 years progressive experience with partial matching experience – 3 points No demonstrated governance or responsible AI experience – 1 point		
7. A University in Degree Computer Science, Information Systems, or related field.	Relevant Masters or Bachelors (5 Points) Non-Related Masters/Bachelors or Relevant Associates Degree or International Equivalent (3 Points) No (1 Point)		

8. Demonstrable proficiency in effective oral and written communication, including briefing and coordinating with business stakeholders.	Yes (5 Points) Some (3 Points) No (1 Points)		

LABOR CATEGORY 43: SUPPORT FOR BUSINESS ANALYSIS AND REQUIREMENT MANAGEMENT

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: 1 July 2026 – 31 December 2026, with four potential 12-month option periods: 1 January – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028, Option Period Three: 1 January 2029 – 31 December 2029, Option Period Four: 1 January 2030 – 31 December 2030.

Background

The contractor will provide specialized support to the Requirements and Architecture Management Branch by performing business analysis and formal solicitation, documentation, validation, and management of requirements for NATO Capability Development programmes. The tasks executed by the contractor will contribute to the coherence, quality, and traceability of architectures and requirements, while supporting NATO capability development and strategic objectives.

Taskings

1. Support or lead the formal elicitation, capture, and documentation of capability requirements based on operational and regulatory needs.
2. Collaborate with stakeholders across NATO Enterprise to identify and document regulatory requirements and operational constraints that impact capability development.
3. Perform detailed analysis and evaluation of identified requirements to ensure clarity, completeness, consistency, and alignment with capability programme objectives.
4. Maintain version-controlled requirements repositories, ensuring thorough documentation and traceability throughout the requirements lifecycle.
5. Document trade-offs and prioritize functional, non-functional, and regulatory requirements to ensure programme goals are met effectively and efficiently.
6. Ensure consistency between requirements and existing strategic-level enterprise architectures, as well as alignment with agreed reference frameworks.
7. Ensure coherence and optimization of requirements across ACT capability development programmes.
8. Facilitate formal requirements validation processes involving stakeholders to ensure requirements meet operational needs and standards.
9. Provide recommendations for resolving conflicts and deconflicting requirements during the validation process.
10. Implement quality assurance measures to ensure high standards in requirements documentation, including completeness, accuracy, and consistency.
11. Monitor and analyse gaps, overlaps, and dependencies related to capability requirements across programmes.
12. Support the Branch Head CR and travel to meetings and conferences both within and outside NATO’s boundaries for up to 30 days per year.
13. Perform additional tasks as required by the COTR related to the labour category.

Essential Qualifications At least five (5) years in the last ten (10) of demonstrable hands-on experience in business analysis and requirements management, using professional requirements documentation and management tools (e.g. Sparx Enterprise Architect, Aris, Jira, DOORS, Jama Connect), in accordance with industry standards and best practices (e.g. International Requirements Engineering Board, Scaled Agile Framework, Business Analysis Body of Knowledge).

- Certification or formal training with demonstratable proficiency in one or more industry in requirements management and business analysis methodologies like IREB, SAFe, IIBA or comparable.

- Demonstrable ability to present requirement sets, business processes and architectures in an easy understandable and accessible way to non-technical audiences, from end users to senior decision makers and approval boards.

- Demonstrated minimum NATO or National SECRET clearance with the appropriate national authority for the duration of the contract.

- Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading, and Writing) or equivalent.

- Demonstrable proficiency in effective oral and written communication, including briefing and coordinating with business stakeholders.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified
elow to ascertain whether the individuals have adequately qualifications to be considered compliant. HQ SACT
reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LC 43 SUPPORT FOR BUSINESS ANALYSIS AND REQUIREMENT MANAGEMENT

Item	**Compliant**	**Non-Compliant**
Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading, and Writing) or equivalent.		
Demonstrable proficiency in effective oral and written communication, including briefing and coordinating with business stakeholders.		
Minimum of **70 Points** in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification.** **ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1. Demonstrated at least 5 years (out the last ten) of hands-on experience in business analysis and requirements management, using professional requirements documentation and management tools (e.g. Sparx Enterprise Architect, Aris, Jira, DOORS, Jama Connect), in accordance with industry standards and best practices (e.g. International Requirements Engineering Board, Scaled Agile Framework, Business Analysis Body of Knowledge).	No demonstrable hands-on experience in business analysis and requirements management: 0 points No demonstrable proficiency with professional tools:0 points Less than 5 years: 0 points 5 – 10 years (at least 5 in the last 10): 1-50 points More than 10 years (at least 5 in the last 10): **51-65 points**		
2. Certification or formal training with demonstratable proficiency in one or more industry in requirements management and business analysis methodologies like IREB, SAFe, IIBA or comparable.	Certified for less than 2 years: 1-5 points Certified for at least 2 years: **6-15 points**		

3. Demonstrable ability to present requirement sets, business processes and architectures in an easy understandable and accessible way to non-technical audiences, from end users to senior decision makers and approval boards.	No demonstrable experience: 0 points Less than 5 years of experience: 1-10 points At least 5 years of demonstrable experience: **11-20 points**		

LABOR CATEGORY 44: CONTRACTOR SUPPORT TO ANALYTICS SPECIALIST – CAPABILITY LIFECYCLE (ENGINEERING)

Location: Norfolk, VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: 1 July 2026 – 31 December 2026, with 4 potential 12-month option periods.

Background Information:

1. Deputy Chief of Staff Capability Development (DCOS CAPDEV) acts as the Supreme Allied Commander Transformation's Director for guidance, direction and co-ordination of the activities and resources of the Capability Development Directorate. CAPDEV is responsible to:

a. Identify and prioritize Alliance capability development from short to long term, ensuring coherence between all capabilities within the CAPDEV portfolio.

b. Lead the determination of required capabilities and prioritization of shortfalls to inform the delivery of materiel and non-materiel solutions across the Doctrine, Organisation, Training, Material, and Leadership, Personnel, Facilities and Interoperability (DOTMLPFI) lines of effort to enable a holistic approach to capability development, ensuring improved interoperability, deployability and sustainability of Alliance Forces.

2. The future Capability Development Directorate will include enduring functionality to effectively plan and manage coherent through life capability development, aligned to NATO's strategic intent and priorities. The CAPDEV Data and Analytics Office (DAO) is responsible to DCOS for managing the data and platform operations for Capability Lifecycle, Requirements, and P3M data as well as providing analytics as service and enabling self-service analytics for CAPDEV decision makers.

3. As part of ongoing organisational functional reviews, CAPDEV is in the process of implementing measures for improved capability development planning and management, including the way it collects, manages, analyses and reports on capability development and delivery information, both legacy and current.

Taskings — Analytics Specialist – Capability Lifecycle (Engineering).

1. **Requirements Analytics and Engineering Insight**: Design, develop, and maintain analytic products that provide visibility into requirements definition, maturity, completeness, and alignment across the capability lifecycle.
2. **Requirements Capture and Decomposition Support**: Support the analysis, decomposition, and structuring of complex system and capability requirements to enable effective analytics, traceability, and decision support.
3. **Requirements Traceability and Linkage Analysis**: Develop analytics and reports that assess traceability between requirements, architectures, capabilities, verification artifacts, and delivery outcomes across engineering repositories.
4. **Engineering Data Integration and Interoperability**: Integrate requirements and engineering data from multiple authoritative sources to enable unified analysis, reporting, and cross-domain insight.

5. **Configuration and Change Management Analytics**: Support configuration management and change control activities by developing analytics that track requirement baselines, version history, change impacts, and configuration status.
6. **Engineering Performance Metrics**: Define, calculate, and maintain metrics that measure requirements quality, engineering progress, technical risk, and delivery readiness.
7. **Business Intelligence Development (Engineering Focus)**: Develop, customize, and maintain dashboards, reports, and visualizations that communicate engineering status, risks, and trends to technical and non-technical stakeholders.
8. **Cross-System Engineering Reporting**: Integrate and correlate engineering data with programmatic, schedule, and risk data to support holistic capability lifecycle analysis.
9. **Data Quality and Validation**: Perform validation, consistency checks, and quality assurance activities on engineering and requirements data to ensure accuracy and reliability of analytic outputs.
10. **Decision Support for Engineering Reviews**: Produce analytic products that support requirements reviews, design trade-off analyses, technical governance forums, and capability assurance activities.
11. **Stakeholder Engagement**: Collaborate with engineers, architects, analysts, program managers, and international stakeholders to capture analytic requirements and translate them into actionable engineering-focused analytics.
12. **Process Improvement and Automation**: Identify opportunities to streamline and automate engineering analytics, reporting, and data preparation workflows to improve efficiency and reduce manual effort.
13. **Tool and Workflow Support**: Support the configuration and effective use of analytics tools and engineering workflows to ensure adoption and consistent use across stakeholders.
14. **Documentation**: Develop and maintain documentation describing analytic logic, data sources, assumptions, and limitations for engineering-focused analytics and reports.
15. **User Training and Knowledge Transfer**: Deliver training sessions, user guides, and ad hoc support to ensure effective adoption and interpretation of engineering analytics products.
16. **Capability Lifecycle Engineering Support**: Apply analytics expertise to support requirements-based planning, capability development, verification, validation, and delivery assurance activities.
17. **Technical Support**: Provide ongoing analytic support and troubleshooting for engineering-focused analytics, reports, and dashboards.
18. **Additional Tasks**: Perform additional tasks as required by the COTR related to this labor category.

Essential Qualifications:

1. 8+ years of progressive professional experience in requirements engineering systems analysis, engineering analytics, or related disciplines supporting complex technical systems within defence, security, or similarly regulated environments.
2. Demonstrated expertise in requirements lifecycle management, including requirements capture, decomposition, traceability, validation, and verification across the capability lifecycle using enterprise requirements or lifecycle management tools.

3. Demonstrated experience developing analytics, metrics, and visualizations that provide insight into requirements status, maturity, risk, and alignment to support engineering decision-making and technical governance.
4. Bachelor's degree in Engineering, Computer Science, Information Systems, Mathematics, or a related technical discipline, or equivalent professional experience.
5. Demonstrated experience integrating engineering and requirements data from multiple authoritative sources to support cross-system analysis, traceability, and reporting in enterprise environments.
6. Demonstrated experience supporting configuration management and change control activities, including baselining, version control, impact analysis, and compliance with organizational, NATO, or DoD standards.
7. Demonstrated experience supporting full systems or software development lifecycle (SDLC) activities, including requirements analysis, system design, testing, verification, and deployment.
8. Demonstrated proficiency in data analysis and reporting, including use of business intelligence or analytics tools to translate engineering data into actionable insight for technical and non-technical stakeholders.
9. Demonstrated professional experience operating within secure or classified environments, including adherence to security classification handling, data protection, and access control requirements.
10. Demonstrated ability to collaborate across multidisciplinary and international teams, including engineers, architects, program managers, and stakeholders, to translate engineering data into decision-support products.
11. Demonstrated minimum NATO or National SECRET clearance with the appropriate national authority for the duration of the contract.
12. Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.
13. Demonstrable proficiency in effective oral and written communication, including briefing and coordinating with business stakeholders.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 44: CONTRACTOR SUPPORT TO ANALYTICS SPECIALIST – CAPABILITY LIFECYCLE (ENGINEERING).

	Item	Compliant	Non-Compliant
1	Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
2	Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
3	Contractor candidate holds active NATO or National SECRET (or higher) security clearance		
4	Valid NATO Nation passport with no travel restrictions to NATO nations		
5	Proficiency in the use of the Microsoft Office Tool suite and collaborative software		

6	Minimum of 60 Points in the Subject Matter Expert Criteria		
7	**Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)**		

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1. 8+ years of progressive professional experience (with at least 5 years within the last 8 years of demonstrated experience) supporting requirements engineering, analysis, traceability, and lifecycle management for complex systems in defense, security, or similarly regulated environments.	8+ years progressive experience AND 5+ recent years of exact matching experience – 13-**20 points** 6–7 years progressive experience AND 3–4 recent years of exact matching experience – 7-12 points 4–5 years progressive experience AND 1–2 recent years of partial matching experience –3- 6 points Less than 4 years of relevant experience –1- 2 points		
2. 8+ years of progressive professional experience (with at least 5 years within the last 8 years of demonstrated experience) performing requirements traceability,	8+ years progressive experience AND 5+ recent years of exact matching experience – **20 points** 6–7 years progressive experience AND 3–4 recent		

baselining, configuration management, and change impact analysis across engineering repositories.	years of exact matching experience – 12 points 4–5 years progressive experience AND 1–2 recent years of partial matching experience – 6 points Limited or indirect experience – 2 points		
3. 6+ years of progressive professional experience (with at least 3 years within the last 6 years of demonstrated experience) developing analytics, metrics, dashboards, or reports that provide insight into engineering status, risk, maturity, or readiness.	6+ years progressive experience AND 3+ recent years of exact matching experience – **10-15 points** 4–5 years progressive experience AND 2 recent years of exact matching experience – 6-9 points 3–4 years progressive experience AND 1 year of partial matching experience – 3-5 points Less than 3 years of relevant experience – 1-2 points		
4. 6+ years of progressive professional experience (with at least 3 years within the last 6 years of demonstrated experience) integrating engineering or requirements data across multiple systems to enable unified analysis, traceability, and reporting.	6+ years progressive experience AND 3+ recent years of exact matching experience – **10-15 points** 4–5 years progressive experience AND 2 recent years of exact matching experience – 6-9 points 3–4 years progressive experience AND 1 year of partial matching experience –3- 5 points Limited or indirect integration experience –1- 2 points		
5. 5+ years of progressive professional experience (with at least 2 years within the last 5 years of demonstrated experience) producing analytic outputs that support	5+ years progressive experience AND 2+ recent years of exact matching experience – **7-10 points**		

engineering reviews, requirements prioritization, design trade-offs, or technical governance.	3–4 years progressive experience AND 1 recent year of exact matching experience – 4-6 points 2–3 years progressive experience with partial matching experience – 2-3 points No demonstrated decision-support experience – 1 point		
6. 5+ years of progressive professional experience (with at least 2 years within the last 5 years of demonstrated experience) supporting full system or software development lifecycle activities, including requirements analysis, verification, validation, testing, or audit/compliance support.	5+ years progressive experience AND 2+ recent years of exact matching experience – **7-10 points** 3–4 years progressive experience AND 1 recent year of exact matching experience – 4-6 points 2–3 years progressive experience with partial matching experience – 2-3 points No demonstrated SDLC experience – 1 point		
7. University in Degree Computer Science, Information Systems, or related field.	Relevant Masters or Bachelors **(5 Points)** Non-Related Masters/Bachelors or Relevant associate's degree or International Equivalent (3 Points) No (1 Point)		
8. Demonstrable proficiency in effective oral and written communication, including briefing and coordinating with business stakeholders.	Yes **(5 Points)** Some (3 Points) No (1 Points)		

LABOR CATEGORY 45 : CONTRACTOR SUPPORT TO CAPDEV QUALITY MANAGEMENT BRANCH, QUALITY ASSURANCE ANALYST

Location: Norfolk, VA, USA (On-site)

Number of Candidates: Two Candidates

Period of Performance: Base Period: 1 July 2026 – 31 December 2026, Option Period One: 1 January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028, Option Period Three: 1 January 2029 – 31 December 2029, Option Period Four: 1 January 2030 – 31 December 2030.

Background

1. DCOS Capability Development (CAPDEV) acts as the Supreme Allied Commander Transformation's Director for guidance, direction and co-ordination of the activities and resources of the Capability Development Directorate. CAPDEV is responsible to:

a. Identify and prioritize Alliance capability shortfalls from short to long term, along a continuum of holistic capability development.

b. Lead the determination of required capabilities and prioritization of shortfalls to inform the delivery of materiel and non-materiel solutions across the Doctrine, Organization, Training, Materiel, and Leadership, Personnel, Facilities and Interoperability (DOTMLPFI) lines of effort to enable a holistic approach to capability development, ensuring improved interoperability, deployability and sustainability of Alliance Forces.

2 The CAPDEV Quality Management Branch (QMB) provides a capability development quality assurance process and is responsible for developing and managing the CAPDEV Quality Management System (QMS) providing independent risk based assurance of capability development processes to ensure that outputs, products and services meet customer expectations, and comply with NATO Policies and Standards whilst ensuring that Portfolio, Programme, Project Management best practices and standards are implemented throughout the capability lifecycle. The QMB:

a. Conducts independent Quality Assurance and audit of processes, functions and activities, and quality control of outputs for compliance with agreed quality criteria and metrics or authorized exception processes.

b. Supports Capability and Programme Directors by performing independent, assessments of performance (cost, schedule, scope, performance and risk) against agreed tolerances.

c. Produces risk-based quality reports and quantified improvement opportunities: leveraging process metrics to forecast benefits and efficiencies

d. Identifies and ensures resolution of Corrective and Preventative Actions (CPA) to manage risk and remediate issues, defects and deficiencies identified during audit and assurance reviews. Supports the identification and capture of programmatic and capability risks, on behalf of the accountable risk owners, to develop actionable recommendations and potential response activities.

e. Leverages metrics and KPIs for external benchmarking of performance against comparable organizations and within and between internal teams.

f. Fosters a culture of quality and Continuous Process Improvement through monitoring, measurement, and analysis and supports process owners in implementation of Continuous Process Improvement activities to improve quality of output, to increase the maturity of internal processes and to prevent issues, defects and deficiencies.

g. Supports CUR/UR and other acquisition processes to ensure quality and consistency across NATO requirements management and NATO life cycle management (LCM) processes

h. Supports Business Analysts and Capabilities' Programme Directors to maintain the quality of capability requirements and traceability throughout the lifecycle of the capability.

i. Ensures that capabilities requirements are developed to NATO Standards across all Doctrine, Organization, Training, Materiel, Leadership, Process, Facilities and Interoperability (DOTMLPFI) lines of development and that dependencies with other capabilities are identified and managed.

Tasking

1. Provide independent quality assurance of information, management products and processes, and quality reports for CAPDEV leadership.

2. Provide quality assurance expertise in support of HQ SACT's programme management and requirements engineering and specifically in support of Requirements Managers undertaking the Identification, elicitation, capture, analysis, evaluation, integration and maintenance of high-quality capability (business) requirements.

3. Support the ongoing development, and maintenance of the requirements repository and requirements related information and the achievement and maintenance of the organization's requirements and quality expectations.

4. Support the development and maintenance of processes relating to capability development and delivery. Contribute to the development of directives and standard operating procedures that relate to capability development and delivery including requirements development and management and the ACT Requirements Repository.

5. Contributes to organizational continual process improvement activities.

6. Participate in workshops, seminars, conferences and meetings in support of the activities above.

7. Perform additional tasks as required by the COTR related to the labour category.

Essential Qualifications:

1. A University Degree in engineering, management, information systems, accounting, economics, finance, business administration, public administration, operations research, programme and project management or related disciplines.

2. Five years' experience in the last 10 in the field of quality assurance including requirements for engineering processes.

3. Demonstrated minimum NATO or National SECRET clearance with the appropriate national authority for the duration of the contract.

4. Nationality of one of the NATO Countries.

5. Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.

6. Demonstrable recent (i.e. in the last 5 years) experience working in support of processes that were formally certified in accordance with the ISO 9001 standard.

7. Experience with IBM Rational Engineering Lifecycle Management (ELM), DOORS Next or equivalent tool for quality assurance and requirements engineering including personal use of quality assurance tools for evidence-based quality reporting.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequate qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 45 (QMB): CONTRACTOR SUPPORT TO CAPDEV QUALITY MANAGEMENT BRANCH QUALITY ASSURANCE ANALYST

Note: Each candidate within this category must have his/her own compliance matrix.

Item	**Compliant**	**Non-Compliant**
Demonstrated minimum NATO or National SECRET clearance with the appropriate national authority for the duration of the contract.		
Nationality of one of the NATO Countries.		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
~~Demonstrable recent (i.e. in the last 5 years) experience in quality assurance including requirements engineering processes~~		
~~Demonstrable recent (i.e. in the last 5 years) experience working in support of processes that were formally certified in accordance with the ISO 9001 standard.~~		
~~Experience of quality assurance leveraging functionality within IBM ELM, Rational DOORS Next or equivalent tool.~~		
Minimum of **75 Points** in the Subject Matter Expert Criteria.		

BEST VALUE CRITERIA MATRIX

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT.**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible)**
1. A University Degree in engineering, management, information systems, accounting, economics, finance, business administration, public administration, operations research, programme and project management or related disciplines.	Yes **(5 Points)** No (1 Points)		
2. Five years' experience in the last 10 in the field of quality assurance including requirements engineering processes.	5 years in the last 6 years): (**41-50 Points)** 5 years in the last 8 years): (31-40 Points) 5 years in the last 10 years: Yes (2-30 Points) No (1 Point)		

3. Demonstrable recent (i.e. in the last 5 years) experience conducting quality assurance of processes that were formally certified in accordance with the ISO 9001 standard or equivalent.	Yes: 1-5 years: (2-5 points) 6-10 years: (6-10 points) >10 years: **(11-15 points)** No (1 Point)		
4. Experience using quality assurance functionality with IBM ELM. Rational DOORS Next or equivalent.	1-2 years: (1-10 points) 3-4 years: (11-20 points) >5 years: **(21-30 points)** No (1 Points)		

LABOR CATEGORY 46: NATO DIGITAL BACKBONE SYSTEMS ANALYST (COMMAND NETWORK SYSTEMS ANALYST)

Location: Norfolk VA, USA (On-site)

Number of Candidates: One Candidate

Period of Performance: Base Period: 01 July 2026 – 30 Dec 2026 with 3 potential 12-month option periods, 5 Jan 2027 – 30 Dec 2027, 5 Jan 2028 – 30 Dec 2028, 5 Jan 2029 – 30 Dec 2029

Background Information:

The NATO Digital Backbone (NDBB) is a critical asset for the overall NATO Digital Transformation and is a prerequisite for the execution of Multi-Domain Operations.

The NDBB is a strategic and operational level command network connecting the NATO Command Structure and NATO Force Structure as well as non-military actors to provide synchronization.

The NATO Command Network Project was part of the Cross-Domain Command WDI and started in 2022 and with an aim to implement it by 2035. The NATO Command Information Systems Initiative has transitioned into supporting the development of the NATO Digital Backbone.

The Digital Backbone is a strategic deliverable under the Digital Transformation Implementation Strategy. The definition of the Digital Backbone is to connect sensor, decision makers and effectors. The digital backbone is architecturally referenced in the NDBB and Data Centric Reference Architecture (RA). The NDBB is described as the layer underpinning the data management and data exploitation mechanisms. The collection of the capabilities and services to realize the Digital Backbone are independent useful systems that till now have been treated as distinct entities providing unique set of outcomes and operational benefits. The intent of the NDBB initiative is to create a whole that is greater than the sum of the individual capabilities/services. The approach to address the creation of a NATO Digital Backbone will require planning, analyze organizing, and integrating the existing and new system changes into a system of system capability that generates outcomes and operational benefits greater than the sum of individual parts. NATO Digital Transformation is an endeavour to transform the Alliance towards a secure data-enabled organisation. It addresses the operational needs to securely move data vertically from the strategic to the tactical level, and horizontally across the Land, Maritime, Air, Cyber and Space domains.

The work will include the management, revision and execution of the NATO Digital Backbone Capability Programming Strategy. The CPS will also include the need to include interoperability, emerging and disruptive technology, non-material (e.g. facilities) and other capability development aspects. New operational requirements will also need to be incorporated into the CPS planning. The contractor will support the completion of all these activities.

Tasking:

1. Contract personnel shall provide products and support services to the CIS Branch in support of the main NATO Command Information Systems Initiative (NDBB) activity to provide enterprise architecture support for the following tasks:

2. Conduct activities through direction from the CIS Branch lead for the NATO Command Information Systems Initiative (NDBB).

3. Plan and facilitate the conduct of NATO Command Information Systems Initiative (NDBB) workshop with stakeholders in NATO HQ, ACO, NCI Agency and others in Europe with the purpose of implementing a cohesive NATO Digital Backbone aligned to operational requirements statements. Provide briefings, engage in discussions, and facilitate working sessions.

4. Development and incorporation of coherent capability requirements across all NDBB related efforts through work with the Planning, Requirements and Execution Division Branches.

5. Facilitate/support ACO in the development of high-level requirements (e.g. operational requirements) for the NDBB that support multi-domain operations using work from Conceptual, operational requirements, architectural, and high-level guidance. Must be able to communicate the overall intent of the NDBB to guide the further development of new operational requirements.

6. Support ACT's contributions to standing network initiatives that may result in updates to existing NDBB programming and CPS, the execution of an implementation plan, or the development of ACT management products (e.g. capability programme plan) associated with the NDBB.

7. Consult with Enterprise Architecture, conceptual working groups, FMN gap analysis, programme directors, project managers within ACT and in other organizations Germane to the NATO Command Information Systems Initiative (NDBB) to accomplish the aforementioned tasks.

8. Consult as appropriate with project/programme managers, operational users, business architects, system engineers, and other key stakeholders, within NATO Commands and Agencies to obtain the information necessary for analysis, to develop the outcomes needed to support the Digital Transformation through NDBB.

9. Support the updating of ACT programme management dashboards and SharePoint sites consistent with HQ SACT guidance. This includes updating programme plans, risk registers, and documentation repositories.

10. Develop presentations and information papers in order to provide updates on the NATO Command Information Systems Initiative (NDBB) to stakeholder groups and for use by COTR for further dissemination to leadership.

11. Participates in planning, executing and reporting on NDBB related exercises and experimentation.

12. Other duties as assigned by the COTR are NCISI/NDBB related.

Essential Qualifications:

1. Demonstrable experience (4 years or more) in CIS capability integration, systems engineering, Project Management, CIS requirements or equivalent.

2. University degree level education (bachelor and/or master) in a relevant field (Computer Science, Engineering, Information Sciences and Technology, Mathematics, Business Management etc.).

3. Demonstrated Ability to participate effectively in high-level discussions, workshops, etc. and prepare professional, high-quality documents and briefings for review.

4. Knowledge and experience (3 years) of project management techniques.

5. Demonstrable experience (3 years or more) in conducting studies and providing coherent papers explaining study results and recommendations.

6. Knowledge of NATO, its organizational structure. Previous experience working in

   a. defence environment or technical development organizations.

7. Familiarity and knowledge of the specific area of communications-information systems such as data centres, cloud computing, communications, and application services.

Annex B

Requirements Matrix

Contractors' technical proposals will be assessed on the qualifications of both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below to ascertain whether the individuals have adequate qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 46: NATO DIGITAL BACKBONE SYSTEMS ANALYST (COMMAND NETWORK SYSTEMS ANALYST)

Item	**Compliant**	**Non-Compliant**
Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of 50 Points in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

	Range **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 pts possible**
1. Demonstrable experience (4 years or more) in CIS capability integration, systems engineering, Project Management, CIS requirements or equivalent.	Yes – 2-**10 Points** No - 1 Points		
2. University degree level education (bachelor and/or master) in a relevant field (Computer Science, Engineering, Information Sciences and Technology, Mathematics, Business Management etc.).	Yes – 2-**15 Points** No - 1 Points		
3. Demonstrated Ability to participate effectively in technical and programmatic discussions, workshops, etc. and prepare professional, high-quality documents and briefings for review.	Yes – 2-**20 Points** No - 1 Points		
4. Knowledge and experience (3 years) of project management techniques.	Yes – 2-**20 Points** No - 1 Points		

5. Demonstrable experience (3 years or more) in conducting studies and providing coherent papers explaining study results and recommendations.	Yes – 2-**10 Points** No - 1 Points		
6. Knowledge of NATO, its organizational structure. Previous experience working in a defence environment or technical development organizations.	Yes – 2-**10 Points** No - 1 Points		
7. Familiarity and knowledge of the specific area of communications-information systems such as data centers, cloud computing, communications, and application services	Yes – 2-**15 Points** No - 1 Points		

LABOUR CATEGORY 47: NUCLEAR CONSULTATION COMMAND & CONTROL (NC3) COORDINATION SUPPORT SECRETARIAT

Location: Norfolk, VA USA (On-Site)

Number of Candidates: One Candidate

Period of Performance: Base Period: Award – 31 December 2026 with four potential 12 – month options, 1 January 2027 – 31 December 2027, 1 January 2028 – 31 December 2028, 1 January 2029 – 31 December 2029, 1 January 2030 – 31 December 2030

Background Information:

Nuclear Consultation, Command and Control (NC3) Modernisation programme is the largest programme in the Common Funded Capability Development portfolio. NC3 modernization has been identified by the Military Committee as a Key Requirement Area (KRA) for NATO 2030 with tens of billions of Euros of planned investment. It is also one of the most complex programmes, that requires a sound orchestration across the Host Nations and the variety of Implementing entities involved to coordinate delivery, life-cycle management, and in-service operations of NC3 services and equipment.

NC3 workload has progressively increased with the approval of the CPP #1 and CPP #1 addendum in 2024 and 2025. The iCMO is orchestrating the delivery of 50+ project proposals within the next 18 months, together with another CPP next year.

The coordination of support for the Secretariat function is a key element in maintaining a comprehensive knowledge over the planning and execution of all Programmes and Projects. This position manages collaborative tools and data SharePoint of the Programme to enable full and timely accessibility to the Management and Governance documents, and ensuring effective collaboration
among multiple stakeholders. This position contributes directly to the Communication and engagement efforts performed by the Branch.

Tasking:

1. Support the NC3 Programme Director (PD) in maintaining comprehensive knowledge over the planning and execution of all Programmes and Projects (Configuration/administration of key Programme documents).
2. Support the Branch by assisting in stakeholder engagement and communications regarding all key engagements with ACO, Nations, and NATO HQ, helping to liaise and facilitate information flow/exchange with appropriate counterparts throughout the Alliance
3. Support cross-functional management regarding the NC3 programme and ACT processes and procedures
4. IKM - coordinate and manage an effective and efficient iCMO IKM (Share Point, EDMS, TRANSNET, mailboxes) to enable full and timely accessibility to all relevant Management and Governance documents
5. Enable induction of new iCMO staff members (course/training coordination, IT account/access/equipment coordination).

6. Support management and coordination of programme-related meetings.
7. Support Tasker Tracker requirements.
8. Support engagement & communication to the broader NATO NC3 Community of interest.
9. Support the creation of MS-Office products for internal and external reporting.
10. Other administrative tasks as required by the programme Director.

Essential Qualifications:

1. An associate degree or higher.
2. Demonstrable working knowledge/experience in administration and management (IKM, event organization and coordination, human resource management, or equivalent).
3. Demonstrable working knowledge/ experience in multinational/ international organizations or defense and security-related organizations.
4. Experience in management/coordination in a Portfolio, Programme and Project Management environment.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 47: NUCLEAR CONSULTATION COMMAND & CONTROL (NC3) COORDINATION SUPPORT SECRETARIAT

Item	Compliant	Non-Compliant
Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent. / or native English speaker.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of **70 Points** in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item	Range Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW - not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification.	Page, Paragraph and Line Number referencing where candidates meet the criteria and how.	Score (100 pts possible)
1. An associate degree or higher	No Degree: 0 points Associate degree: 0-4 points Associate degree & experience (minimum 2 yrs.): 5-8 points bachelor's degree: 9-12 Points Bachelor's Degree & experience (minimum 2 yrs.): 13-16 points Master's Degree: 17-20 points Master's Degree & experience (minimum 2 yrs.): 21- 25 points		
2. Demonstrable working knowledge/experience in administration and management (IKM, event organization and coordination, human resource management or equivalent).	No experience: 0 points Less than 1 year: 0-5 points 1-3 years: 6-15 points More than 3 years: 16-25 points		
3. Demonstrable working knowledge/ experience in multinational/ international organizations or defense and security-related organizations. Increased value based on experience working within NATO.	No experience: 0 points Less than 1 year: 0-3 points 1-2 years: 4-6 points More than 2 years: 7-15 points Experience working within NATO (at least 1 year): 0-15 additional points		

4. Experience in management/coordination in a Portfolio, Programme and Project Management environment. Increased value based on experience involved in a NATO common-funded (CFCDGM) pogramme.	Experience in a P3 management environment: 0-5 points Experience involved in a NATO CFCDGM programme (at least 1 year): 0-15 additional points		

LABOR CATEGORY 48: PROTOCOL SPECIALIST

Number of Candidates: One Candidate

Location : Norfolk, VA, USA (On-site)

Period of Performance:

Base Period: Contract Award – 31 December 2026 with four option periods, 1 January – 31 December 2027, 1 January – 31 December 2028, 1 January – 31 December 2029, 1 January – 31 December 2030.

Taskings:

The Contractor shall perform under the direction of the COTR the following duties that include, but are not limited to:

1. Acting as focal liaison point with Local Authorities.

2. Developing and maintaining the VIP database.

3. Planning, preparing, and executing all conferences, exercises, seminars, ceremonies, and VIP visits to HQ SACT.

4. Personally meeting and escorting visitors and dignitaries (as required) on their arrival and accompanying them through various phases of their visits.

5. Preparing and executing an effective and comprehensive DV programme. Responsible for creating schedules of events, including briefing arrangements, luncheons, ship and base tours, accommodations, transportation, and all details.

6. Providing advice and training on matters relating to the customs and regulations governing diplomatic formality, precedence, and etiquette.

7. Supporting the execution of numerous National Day Flag Raising Ceremonies, including coordination of Marine Corps and Band support, guests of honour, gifts, and various other details.

8. Maintaining alphabetical biography books of NATO officials and all DVs.

9. Serve as SME on all matters regarding protocol planning software applications inside the Protocol Branch and for events in support of HQ SACT mission requirements.

Essential Qualifications

1. Experience in the following:

a. Experience in an international military or governmental agency protocol environment.
b. Experience on major joint or international military staff that includes planning of high-level events such as: Conferences, Exercises, Seminars, Ceremonies and high-level visits (Preferably within NATO).
c. Familiarity with NATO Protocol standards.
d. Excellent organizational and communication skills.
e. Experience in managing complex schedules.
f. Experience in Management of electronic registration using Cvent.
g. Experience in Management of protocol software i.e. SocialTables.
h. Experience in Management of electronic seating plan drawing tools i.e. Autocad.
i. Experience on Database managing tools (Microsoft Access).

2. College degree or similar national academic qualification is required. 5 years of equivalent military or professional experience in a protocol or similar environment can be used as a substitute(s) for a university degree.

3. External of NATO Protocol Course Certificate desired, NOT essential.

Other Considerations

1. Ability to work independently, proactively, and resourcefully on several tasks at one time with minimum supervision.

2. Present a mature, professional appearance; interact well with others in international environment.

3. Advanced knowledge of word processing, spreadsheet, project management, and graphics software.

4. Protocol Officer Course or equivalent formal training.

5. Portfolio, Programme and Project management (P3) course is desirable.

6. Previous experience working with Flag/General Officers or equivalent is desirable.

7. Foreign Language proficiency, particularly French is desirable.

8. Fluent in English (written and Oral).

9. Ability to work outside of normal working hours to include weekends and evenings, often on short notice; and frequent travel.

10. Attendance at the NATO Protocol Course, NATO School of Oberammergau is mandatory in the first six months. Tuition and travel shall be provided and therefore not included in the bid price.

Instructions for Submitting Video Interview to DropBox

INSTRUCTIONS FOR SUBMITTING VIDEO

1. All interested bidders are required to submit a video. In the first part present themselves and why do they think they are the best choice for the place two (2) minutes. In the second part answering the three (3) questions below four (4) minutes.

2. Responses to each of the questions should be clear, concise. Video interview submission should not exceed longer than six (6) minutes in length.

3. Interviewees should treat this interview in a similar fashion as one that you would apply for in person in a business setting. Candidates should present themselves in a professional manner.

4. Video files should be sent in the mpeg/mpg4 format. File names shall be labelled: Company Name.First Name.Last Name.Position. Example: AcmeIndustries.John.Smith.ProtocolSpecialist.mp4

a. 5. Files shall be sent to the following address: https://www.dropbox.com/request/S3NvvmUdAuNqCHmcsupC

6. Please email the contracting officers listed on this solicitation to confirm receipt of video file. Please allow up to 24 hours to respond.
Interview Questions:

a. NATO has 32 member nations. As the Protocol Officer, how could you organize the order of precedence between the Nations? What about Partner nations?

b. During a Flag Raising Ceremony a national flag accidentally goes up up-side down. As the Protocol Officer responsible for the ceremony, what action do you take?

c. A Minister of Foreign Affairs from a Partner nation is visiting ACT. As the Protocol Officer in charge of the visit, which elements of support will you arrange regarding the welcome, logistical support and the agenda, taking into consideration the following details:

1. Arrival on previous day and departing at 13:00;
2. The ACT representation includes Flag and General Officers from France, Germany, United States of America, United Kingdom, Portugal, Norway, Italy.

Annex B

Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the compa ny and individuals proposed to perform the work. Individuals' résumés will be measured against
each of the criteria specified below in order to ascertain whether the individuals have adequ ate qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates).

Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for LABOR CATEGORY 48: PROTOCOL SPECIALIST

Item	**Compliant**	**Non-Compliant**
Minimum of one past performance citations within the la st seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STAN AG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of **70 Points** in the Subject Matter Expert Crite ria		
Key personnel citizen of NATO member nation (Nati onality must be indicated to include other citizenships)		

Item	**Range** **Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification.**	**Page, Paragraph and Line Number referencing where candidates meet the criteria and how.**	**Score (100 Pts possible)**
1. Experience working in an international military or governmental agency protocol environment.	• No Exp: 0 points • <3 years: 2 points • 3-5 years: 3 points • 6-10 years: 4 points • 11+ years: **5 points**		
2. Experience on major joint or international military staff that includes planning of high-level events such as: Conferences, Exercises, Seminars, Ceremonies and High-Level Visits. (Preferably NATO).	• No Exp: 0 points • <3 years: 2 points • 3-5 years: 3 points • 6-10 years: 4 points • 11+ years: **5 points**		
3. Familiarity with NATO Protocol standards.	• No familiarity – 0 points • Familiarity – **1-5 points**		
4. Excellent professionalism, organization, and communication skills.	• Not Demonstrated – 0 points • Demonstrated – **1-5 points**		
5. Experience in managing complex schedules.	• No Exp: 0 points • <3 years:2 points • 3-5 years: 3 points • 6-10 years: 4-9 points • 11+ years: **10 points**		
6. Experience in Management of electronic registration using CVent or another equivalent Protocol main tool.	• No Exp: 0 points • <3 years: 2 points • 3-5 years: 3-4 points • 6-7 years: 5-9 points • 8+ years: **10 points**		

7. Experience in management of Protocol seating/check-in software i.e. Social Tables, on Arrival.	• No Exp: 0 points • <3 years: 2 points • 3-5 years: 3 points • 6-7 years: 4 points • 8+ years: **5 points**		
8. Experience in Management of electronic drawing tools i.e. Autocad.	• No Exp: 0 points • <3 years: 2 points • 3-5 years: 3 points • 6-7 years: 4 points • 8+ years: **5 points**		
9. Experience on Database managing tools (Microsoft Access).	• No Exp: 0 points • <3 years: 2 points • 3-5 years: 3 points • 6-7 years: 4 points • 8+ years: **5 points**		
10. University degree or 5 years of equivalent military professional experience in a protocol or similar environment.	• Not Demonstrated: 0 points • Demonstrated: 1-**5 points**		
11. External NATO Protocol Course Certificate.	• Not Provided – 0 points • Provided – 1- **5 points**		
12. Ability to work independently, proactively, and resourcefully on several tasks at one time with minimum supervision.	• Not Demonstrated: 0 points • Demonstrated: 1-**5 points**		
13. Present a mature, professional appearance; interact well with others in international environment. (Based on submitted video from provided ceremony script example (English))	• Not Demonstrated: 0 points • Demonstrated: 1-**5 points**		
14. Project management	• Not Demonstrated: 0 points • Demonstrated: 1-**5 points**		
15. Previous experience working with Flag/General Officers or equivalent	• Not Demonstrated: 0 points • Demonstrated: 1-**10 points**		

16. Foreign Language proficiency (French preferred)	• Not Demonstrated: 0 points • Demonstrated: 1-**5 points**		
17. Ability to work outside of normal working hours to include weekends and evenings, often on short notice.	• Not Able: 0 points • Acknowledged and able: **5 points**		

LABOR CATEGORY 49: ISC DATA ANALYSTS

Location: Norfolk, VA, USA, (On-site)

Number of Candidates: One (1) Candidate

Period of Performance: Base Period: Award – 31 December 2026, Option Period One: 1 January 2027 – 31 December 2027, Option Period Two: 1 January 2028 – 31 December 2028.

1. Introduction

a. Allied Command Transformation (ACT) is NATO's leading agent for change: driving, facilitating, and advocating the continuous improvement of Alliance capabilities to maintain and enhance the military relevance and effectiveness of the Alliance. The main objectives of ACT are: providing appropriate support to NATO missions and operations; leading NATO military transformation; improving relationships, interaction and practical cooperation with partners, nations and international organisations. ACT therefore leads Alliance concept development, capability development, training and lessons learned initiatives and provides unfettered military support to policy development within NATO.

b. The Strategic Plans and Policy (SPP) Directorate and the Defence Planning Integration Branch is currently focused on the implementation of the NATO Warfighting Capstone Concept (NWCC) and particularly the Rapid Adaptation of New Force Design Options.

2. Background

a. The NWCC is a 20-year vision for the development of NATO's Military Instrument of Power (MIoP). The NWCC, together with the Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA), implement NATO's Military Strategy. NATO Heads of State and Government committed to the full implementation of both concepts at their summit meeting in 2021. They comprise the military adaptation component of the broader NATO Agenda 2030. ACT is implementing appropriate elements of the NWCC through the Warfare Defence Agenda (WDA).

b. The Rapid Adaptation of Force Design Options seeks to accelerate the adoption of transformational force improvements, seizing every opportunity for efficient investment in new capabilities to augment the force with emerging and disruptive technologies particularly in the rapidly advancing areas of AI, robotics, and autonomy.

c. The ISC (Innovation Solutions Catalogue) will be the tool to track the solutions to new Force Design Options. Driven by the Rapid Adoption Action Plan (RAAP) and the strategic need for continuous transformation, the notion of an Innovation Solutions Catalogue (ISC) was tabled. The RAAP and the Step 3 Capability Summary Report tasked IS-DPP and IS-D2IA with ACT in support. SACT agrees the idea to create an ISC and to develop and maintain the ISC for Allied input and use.

3. Scope

a. The scope of this statement of work (SoW) is to define the requirements for contracting an analyst in support of SPP DPI work to the deliver the ISC.

b. Within this framework, the contractor will work within SPP DPI under the directives of the Branch Head (BH). A Contracting Officer Technical Representative (COTR) will be assigned. The contractors will be working in close coordination with the other staff officers, the other branches of SPP and HQ ACT on topics listed above. The contractor's main effort in 2026 will be the development and management of the pilot and production ISC. The contractors will also help in daily work coordination and collaboration efforts, by provision of the DPI input to associated SPP and ACT outputs.

4. Taskings

a. The contractors will be under the responsibility of the SPP DPI BH and be involved in all aspects of SPP DPI ISC work, to include developing the pilot Catalogue, populating the Catalogue with inputs provided by Allies, acting as a technical support desk , designing, implementing, and populating the production Catalogue, including its connectivity and data sharing with other relevant tools, as agreed in consultations with ISC stakeholders; collecting and assessing lessons identified from the pilot phase as well as their application to the production catalogue; participation in working groups, liaising with other ISC stakeholders including within the NATO International Staff, and development of numerous products relating to the ISC.

b. The contractors will be assigned to SPP DPI Branch to support the development and implementation of ISC but also support the ACT activity/work, where ISC input is required.

c. The Contractor will be required to:

(1) Based upon the unclassified information collected from Allies through an existing online form[1] and other evidence, lead the development work to implement a pilot of the ISC to be completed in accordance with the IS/ACT defined timeline.

(2) Additionally, in coordination with each Allied Single Point of Contact, populate the pilot ISC with information received from FLE, FLEX, and other additional sources, as necessary, to inform and facilitate decisions by NATO and Allied stakeholders on their inclusion in the ISC.

(3) Act as Support Desk for any technical related question about the ISC.

(4) Following conclusion of the pilot, support the development, implementation, and population of a production version of the ISC. This should include the consultation with ISC stakeholders, including IS-DPP, IS-CDT, and

[1] https://www.act.nato.int/about/isc-survey/

IS-D2IA, to collect requirements for the production ISC covering the design, functionalities, content, data exchange and integration with relevant tools, such as NATO Industry Front Door, NATO Innovation Range network tool, DIANA OS, CRIT, etc.

(5) Improve integration of the ISC work into existing ACT and Alliance activity through stakeholder engagement and, in particular the linkage to other Innovation work strands and tools.

(6) Attend weekly SPP DPI meetings, both scheduled and unscheduled, at the direction of the BH. Currently there is one scheduled SPP DPI and one FLEX meeting per week, with impromptu meetings called when required.

(7) Additionally:

(a) Provide feedback about their work clearly and concisely.

(b) Provide input on ISC and offer ideas and related analysis.

(c) Understand the NATO's/ACT's strategy and mission.

(d) Share ideas with multiple stakeholders and gain alignment from them.

(e) Collaborate as required with HQ SACT cross-functional teams to provide improving thoughts and inputs.

(f) Fulfil other specific DPI related tasks directed by SPP DPI BH.

(g) Look beyond 2027 to develop further plans to progress FLEX and ISC thinking and understanding across the ACT and the Alliance.

(h) Conduct research to identify threats and opportunities.

(i) Construct forecasts and analytical models.

5. **Level of Effort.**

a. One person's year per annum with 1800 hours of service. Person hours are further defined in para. 1(a) of Special Terms and Conditions.

6. **Surge Capability**

a. A surge capability requirement is included to have a contract vehicle in place should emerging circumstances require a quick and temporary increase in contractor support (LOE or Deliverable) to meet new requirements within the scope of the existing Statement of Work. The Supplier shall be prepared to provide support services per labor category described above. The contractor shall be prepared to evaluate requirements and submit a price proposal for any new in scope

requirement for consideration by HQ SACT. Surge proposals will be evaluated by the Contracting Officer for fair and reasonable pricing and should be developed based upon the same pricing structure as the original contract proposal. The rate for surge effort shall not exceed the base/option year rate. Surge requirements will be incorporated by formal contract modification. Requests for pricing are made on a non-committal basis and do not constitute a formal commitment by HQ SACT to contract for additional work; supplier will not be reimbursed costs for preparing price proposals or other related expenses in response to a surge request.

b. HQ SACT surge efforts will not exceed 80% of the annual contract value or 80% of the cumulative contract value. Requests to surge from other organisations outside of HQ SACT are not counted against the HQ SACT when calculating the surge tolerances.

7. **Place of performance**

a. SPP DPI Branch requires full time, on-site support. Nevertheless, by exception (e.g. Covid-19 mitigation measures in place), work may be performed remotely from contractor's facility, except for the work on NATO SECRET network.

b. The decision of working remotely or in HQ will depend on COS, SPP DPI BH discretion.

c. Overseas travel, normally within the Euro Atlantic AOR can be expected.

8. **Professional qualifications and personal attributes**

This is a LoE contract with a maximum limit or fraction thereof as set forth in the SoW.

a. Professional qualifications. The contractor shall have:

1. Demonstrable experience (3 years or more) in Enterprise Architecture, Systems Architecture, Programme Management, IT systems requirements or equivalent.

2. University degree level education (bachelor and/or master) in a relevant field (Computer Science and Electrical Engineering, Information Sciences and Technology, Mathematics, Business Administration, etc.).

3. Ability to participate effectively in high-level discussions, workshops, panels, etc. and prepare professional, high-quality documents for review.

4. Experience working in defence environments or previous military experience.

b. Personal attributes. The contractor shall have:

(1) NATO SECRET security clearance.

(2) Capacity to work under general direction within a clear framework of accountability with substantial personal responsibility.

(3) Ability to effectively multi-task and prioritize in a fast-paced environment.

(4) Capacity to work effectively as the member of a multinational and multi-disciplinary team.

(5) Execute a broad range of complex professional or technical work activities in a variety of contexts.

(6) Ability of disciplined and systematic approach to problem solving.

(7) Excellent ability of using contemporary office tools, including MS office and communications systems.

(8) Excellent written and oral skills.

(9) Creative and innovative thinking.

Annex B
Requirements Matrix

Contractor's technical proposals will be assessed on the qualifications of the both the company and individuals proposed to perform the work. Individuals' résumés will be measured against each of the criteria specified below in order to ascertain whether the individuals have adequately qualifications to be considered compliant. (HQ SACT reserves the right to conduct technical discussions of nominated candidates). Examples of how detailed knowledge levels were attained are expected. Ultimately Contractor companies shall clearly demonstrate by providing unequivocal reference to where company/key personnel meet the criteria set forth in this solicitation (please include page number, reference to CV or links as applicable).

Company Name:

Proposed Candidate Name:

Proposed Candidate's Nationality (identify if multiple citizenship & nation):

Best Value Criteria for **LABOR CATEGORY 49: ISC DATA ANALYSTS**

Item	Compliant	Non-Compliant
Minimum of one past performance citations within the last seven years to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW		
Demonstrated proficiency in English as defined in STANAG 6001 (Standardized Linguistic Profile (SLP) 3333 - Listening, Speaking, Reading and Writing) or equivalent.		
Active NATO or National SECRET (or higher) security clearance		
Valid NATO Nation passport with no travel restrictions to NATO nations		
Proficiency in the use of the Microsoft Office Tool suite and collaborative software		
Minimum of **70 Points** in the Subject Matter Expert Criteria		
Key personnel citizen of NATO member nation (Nationality must be indicated to include other citizenships)		

Item	Range Point values assigned based on level of knowledge/experience in relation to the tasks contained in the SOW – not solely on the number of years' experience. Failure to provide exact reference (page, paragraph, line #, ref to CV) to where experience can be validated will result is disqualification. ANY SCORE OF ZERO IS NONCOMPLIANT UNLESS OTHERWISE STATED	Page, Paragraph and Line Number referencing where candidates meet the criteria and how.	Score (100 pts possible)
1)1. Demonstrable experience (3 years or more) in Enterprise Architecture, Digital Transformation activities (Change Management), Capability Architecture, Systems Architecture, Programme Management, IT systems requirements or equivalent.	• No Knowledge or less than 3 years: 1-5 Points • 3-10 years: 6-11 Points • More than 10 years: 12-16 Points Points shall be assigned based on duration, level and relevance of experience.		
2) University degree level education (bachelor and/or master) in a relevant field (Computer Science and Electrical Engineering, Information Sciences and Technology, Mathematics, Business Administration, etc.).	• Degree – 1-10 Points • No Degree – 0 Points Points shall be assigned based on level and relevance of degree(s).		
3) Ability to participate effectively in high-level discussions, workshops, panels, etc. and prepare professional, high quality documents for review.	• No: 1 Point • Yes: 2-12 Points		
4) Demonstrable experience (3 years or more) in Software Development, to include XML language and web-based frameworks.	• Less than 3 years: 0 Points • 3-5 years: 1-5 Points • 5-10 years: 6-11 Points • More than 10 years: 12-16 Points		

5) Demonstrable experience (3 years or more) in Business Intelligence and Reporting techniques.	• Less than 3 years: 0 Points • 3-5 years: 1-5 Points • 5-10 years: 6-11 Points • More than 10 years: 12-16 Points		
6) Knowledge of NATO, its organisational structure and previous experience working in an international organisation.	• No Knowledge or less than 3 years: 1-3 Points • 3-10 years: 4-7 Points • More than 10 years: 8-10 Points		
7) Experience working in defence environments or previous military experience.	• No Knowledge or less than 3 years: 1-3 Points • 3-10 years: 4-7 Points • More than 10 years: 8-10 Points		
8) Familiarity and knowledge of the specific area of military capability requested (e.g. CIS, Cyber, MDO, AI)	• No Knowledge: 1-2 Points • Only Knowledge: 3 Points • Knowledge & 1-3 years' Experience: 4-7 Points • More than 3 years experiences: 8-10 Points		