NCIA/ACQ/2025/07448
Monday, 10 November 2025

NCIA Request for Information (RFI)

To: **Industry Partners**

Subject: **COMMERCIAL LOCAL CIS SUPPORT**
RFI 07448

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming acquisition for provision of local on-site support for CIS services up to Level 2 support activities across various sites. To that end, we are issuing the attached Request for Information (RFI) 07448 to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning purposes only and is not a request for bids. It is part of NCIA's effort to ensure it has a clear understanding of the marketplace, available capabilities, and potential acquisition strategies.

3. We value your insight and invite you to:
   a. Share relevant corporate capabilities and experience;
   b. Review and comment on our draft requirements (Annexes A and B) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.

4. Submission instructions and additional details can be found in the enclosure to this RFI.

5. Only companies from a NATO member country can participate in or respond to this RFI (https://www.nato.int/cps/en/natohq/nato_countries.htm).

6. Should you have any questions or need clarification, please contact Esteban Diaz at Esteban.diaz@ncia.nato.int.

7. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

Esteban Diaz
Digitally signed by Esteban Diaz
Date: 2025.11.10 12:30:50 +01'00'

Esteban Diaz
Senior Contracting Assistant

Enclosure:

- Request for Information with Annexes A and B
- Distribution List

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

1. Albania	**12.** Greece	**23.** Poland
2. Belgium	**13.** Hungary	**24.** Portugal
3. Bulgaria	**14.** Iceland	**25.** Romania
4. Canada	**15.** Italy	**26.** Slovakia
5. Croatia	**16.** Latvia	**27.** Slovenia
6. Czechia	**17.** Lithuania	**28.** Spain
7. Denmark	**18.** Luxembourg	**29.** Sweden
8. Estonia	**19.** Montenegro	**30.** Türkiye
9. Finland	**20.** Netherlands	**31.** United Kingdom
10. France	**21.** North Macedonia	**32.** United States
11. Germany	**22.** Norway	

2. All NATEXs

Table of Contents

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support the provision of local on-site support for CIS services up to Level 2 support activities across various sites. This Request for Information (RFI) is issued solely for informational purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

B. Purpose

1. The purpose of this RFI is to obtain input from industry to help inform the NCIA's acquisition planning. Responses to this RFI will assist in refining requirements, identifying capabilities, and shaping the strategy for any future solicitation.

C. Background

1. The NCI Agency as the main CIS provider to NATO Force Structure. It supports the NATO Communications & Information systems Group (NCISG), which mission is to provide in Theatre CIS Services in support of Alliance Operations, Missions and Exercises. NCISG maintains, in particular, operational readiness of Deployable CIS Modules (DCM), on 15 different locations across Europe.
2. In order to deliver on their mission, NCISG is dependent on Static CIS services, all delivered under the responsibility of the NCI Agency. The aim of the current statement of work, is to get a scalable support capability from a third party to support mainly all localized Static CIS services delivered to NCISG, strengthening existing NCI Agency on-site CIS support units (CSUs) capacities, providing "as-a-service" the full support capacities to mainly DCMs where there is no co-located NCI Agency CSU and to become for each of the supported elements, a Commercial CIS Support Unit Element (C-CSE).
3. Therefore, this Statement of Work (SOW) outlines the requirements and expectations for the provision of local on-site support for CIS services up to Level 2 support activities across various sites.
4. The contractor is expected to carry out these activities in alignment with ITIL best practices, delivering up to 24/7 support as required by the scope of work to ensure continuous service availability.

D. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:

   a. Submit responses via the email address in section H no later than **12:00 hours Central European Time (CET)** on **13 February 2026**.

b. Responses should be submitted in PDF or Word format, including:
   - **i.** Responses to Annex A and comments on Annex B
   - **ii.** Cover page
   - **iii.** Company brochures or product literature (if included)
   - **iv.** Attachments such as past performance references

c. Use the following subject line for submission
   - **i.** "Response to RFI [RFI Number] – [Company Name]"

d. All responses should address the items listed in Annex A – Requested Information.

e. Respondents are also encouraged to review and comment on the draft requirements in Annex B – Draft Statement of Work (SOW)/Performance Work Statement (PWS).

E. Industry Engagement (Optional)

1. N/A

F. Disclaimer

1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. The NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. The NCIA will consider and analyse all information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.

2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

G. Use of Information Provided through Responses

1. Confidentiality of Responses

The NCIA may incorporate industry comments and responses, in part or in whole, into a future release of a solicitation. Should respondents include proprietary data in their responses that they do not wish to be disclosed to the public for any purpose, or used by NCIA (except for internal evaluation purposes), they must:

a. Mark the title page with the following legend:

This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than for NCIA internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit the NCIA's right to use information contained in this data without restriction if it is obtained from another source. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]

b. Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

H. RFI Point of Contact

1. Esteban Diaz

2. Esteban.diaz@ncia.nato.int

Annex A – Requested Information

1. Respondents are encouraged to provide the following information in their response:

   a. **Company Information**
      i. Legal Business Name
      ii. Address
      iii. Website
      iv. Primary Point of Contact
      v. Email address

   b. **Technical Capability**
      i. Summary of relevant capabilities and past performance

   c. **Feedback and Recommendations**
      i. Comments on the draft Statement of Work (SOW)/ Performance Work Statement (PWS)
      ii. Responses to the following RFI Questions
         1. How clear is the overall description of the required service?

            → [ ] Very clear [ ] Mostly clear [ ] Somewhat unclear [ ] Unclear

         2. Which parts of the SoW would benefit from additional detail or clarification?

         3. Are the defined deliverables and acceptance criteria achievable as written?

         4. Are the described roles/responsibilities between the purchaser and the contractor sufficiently defined?

         5. Do you foresee any major operational challenges delivering the service as described at each site?

         6. Are there site-specific constraints that might affect delivery?

         7. Based on your understanding, what type and size of team would be required per location?

         8. What do you see as the main cost drivers for this service (e.g., accommodation, local labor rates, equipment transport, etc.)?

         9. Are there specific requirements in the SoW that, if adjusted, could reduce costs without lowering quality?

         10. Are there assumptions or exclusions that should be made explicit to avoid cost ambiguity later?

11. What are the key risks or uncertainties from your perspective?

12. Do you have suggestions to improve clarity, fairness, or enforceability of the SoW?

13. Are there any best practices or industry standards you recommend referencing?

14. Please provide non-binding indicative comments on lead times?

15. Based on your current understanding of the draft SoW, could you please provide a non-binding indicative total cost estimate (or cost range) for delivering the described service across all locations? **Please consider this as a "must answer".**

16. If useful, you may also provide a separate estimate per site or indicate cost differences by location.

17. Do you have feedback on the format, level of detail, or structure of the SoW itself?

18. Any other comments or recommendations?

iii. Innovations or alternatives
iv. Rough Order Magnitude (ROM), including any assumptions upon which they are based

d. Questions or Concerns

i. Risks, concerns, or barriers
ii. Suggestions for risk mitigation or enhancing competition

Annex B – Draft Requirements / Statement of Work (SOW/PWS)

Note: This is a DRAFT and subject to change. The NCIA is seeking industry feedback.

Statement of Work (SOW)

For

Commercial Local CIS Support

Contents

1 Background information

The NCI Agency as the main CIS provider to NATO Force Structure. It supports the NATO Communications & Information systems Group (NCISG), which mission is to provide in Theatre CIS Services in support of Alliance Operations, Missions and Exercises. NCISG maintains, in particular, operational readiness of Deployable CIS Modules (DCM), on 15 different locations across Europe.

In order to deliver on their mission, NCISG is dependent on Static CIS[1] services, all delivered under the responsibility of the NCI Agency. The aim of the current statement of work, is to get a scalable support capability from a third party to support mainly all localized Static CIS services delivered to NCISG,

- strengthening existing NCI Agency on-site CIS support units (CSUs) capacities,
- providing "as-a-service" the full support capacities to mainly DCMs where there is no co-located NCI Agency CSU and to become for each of the supported elements, a Commercial CIS Support Unit Element (C-CSE).

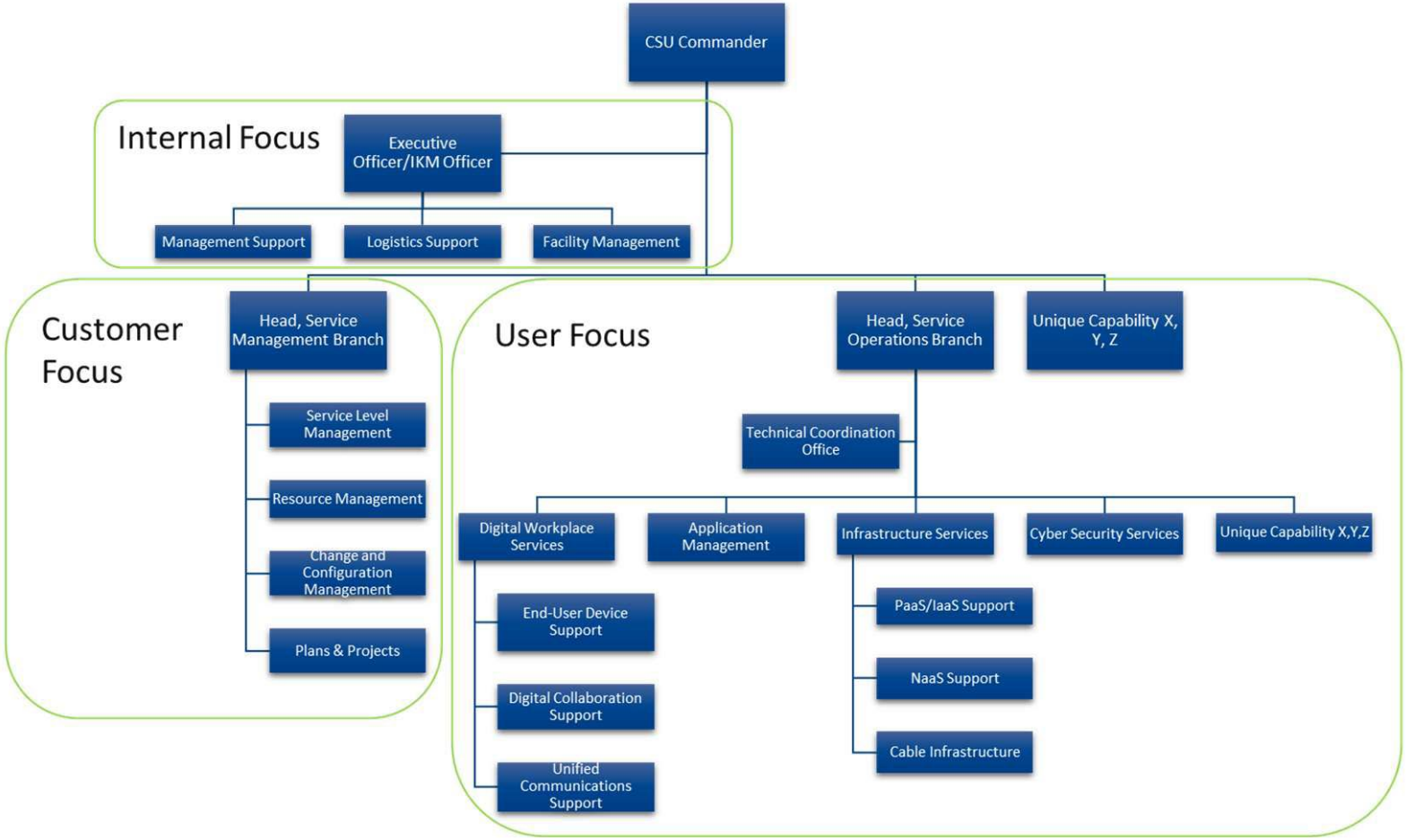
Therefore, this Statement of Work (SOW) outlines the requirements and expectations for the provision of local on-site support for CIS services up to Level 2 support activities across various sites.

The contractor is expected to carry out these activities in alignment with ITIL best practices, delivering up to 24/7 support as required by the scope of work to ensure continuous service availability.

From thereon, the NCI Agency is called the "Purchaser", and the customer being an organisational or a user supported by the NCI Agency.

[1] The supporting systems are stationary or location-bound. They may include standard office setups, workstations, or even phones (by opposition to Deployable CIS which involves self-contained, lightweight setups with satellite connectivity to maintain communication in remote or temporary locations, such as field operations, disaster recovery sites).

1.1 Overview of a CSU structure



In keeping with the above structure, a CSU has support capacities mainly in the six following technical areas:

- Technical Coordination
  - Incident coordination
  - Request fulfilment (coordination across all Service Operations sections)
  - Release and Deployment coordination
  - Overall patch management (coordination, tracking, reporting)
- Digital workplace services:
  - Installation and maintenance of end-user devices (in response to incidents or service requests)
  - System administration for localized core services (end-point security, local collaboration tools)
  - Ongoing maintenance of end-user devices (patch deployment, preventive maintenance, etc.)
  - User support/guidance
  - Voice, VTC and AV support
- Application Management
  - Local application-level support to FAS
  - Software installation, configuration, maintenance and update for bespoke NATO application baseline
  - Local database management and system administration of locally hosted back-end FAS server infrastructure.
- Infrastructures services
  - System administration (incidents, maintenance and request fulfilment) for PaaS
  - Platform and infrastructure layer support to all local and centralized and local services
  - Server OS/Middleware/Platform patch deployment
  - System administration and physical infrastructure support (incidents, maintenance and request fulfilment) for IaaS
  - Management of datacentre real estate (rack space, power, cooling, etc.)
  - LAN/WAN management
  - Cable plant (inside/outside) management
- Cyber security services
  - COMSEC accounting
  - Security Awareness and Compliance (customer-facing)
  - Accreditation support (if funded)
  - Security Incident Response
- Logistical services
  - Asset Management
  - Shipping and Receiving
  - Delivery and receipting of property
  - Collection and disposal

1.2 Agency support model

The NCI Agency support structure is organized in three levels:

- Level 1 support: mainly provided remotely by virtual Centralized Service Desk, and on-site by CSUs
- Level 2 support: provided remotely by Enterprise Support Team of engineers and on-site by CSUs
- Level 3 support: provided remotely by Enterprise Support Team of engineers, with the support of on-site CSU's support level 2 capacities when such a capacity exists.

Further details as to Incident Management are available in:

Agency Standard Operating Procedure (SOP) 06.04.01	Incident Management SOP 0(
Process definition & execution document (PDEP) 06.04.01	Incident Management PDED

2 Scope of Work

The contractor will provide on-site technical support and maintenance for CIS services, at designated locations, strengthening either a CSU's capacities or being a substitute for a CSU.

This can include 24/7 support for physical interventions, implementing standard changes, and supporting project-related activities.

2.1 Site Locations in scope

- Current Sites: a list of sites in scope of this SoW and their locations is provided in Annex C. These are identified as the "initial sites" covered under this contract.

- New Sites: In the event that new sites are added to the scope of support after the contract award, there will be a negotiation process to determine the appropriate service/support structure and costs. The purchaser will consider additional costs proposed by the contractor for these new locations.

2.2 Security and Access Requirements

- Security Clearance: All contractor personnel assigned to this contract must undergo and pass the necessary security clearance process for each site and be able to maintain their clearance while working under the terms of the contract.

- Prohibited Items: Personal IT devices are not permitted on supported sites under local security policies. Only NATO-issued assets (e.g., workstations, laptops, smartphones) may be used. Exceptions require prior written approval from the local security authority.

2.3 Strengthening existing CSUs' capacities

2.3.1 Request for support

With a four months' notice, the contractor can be asked to support in any of the above technical areas (ref. § 1.1). For each technical area where a CSU (ref. CSUs in Annex C) needs support, the request will detail the following point:

- The location;
- The technical area(s) which capacity is to be strengthened;
- The level of security clearance required (up to NATO COSMIC TOP SECRET);
- A summary of the scope of the requirement;
- The requirement, in the form of a project, focusing on scope (expected deliverables), time (start date, expected delivery date) and quality;
- Project acceptance criteria[2].
- Local NATO authority in charge of receipting the support once provided.

Upon reception of the request, the contractor has 15 working days to agree to support, and five additional days to provide the related quotation to the purchaser, with a reference number.

Upon reception of the quotation, the purchaser has fifteen working days to respond. If the purchaser approves within this period (i.e. a purchase order is issued), the contractor becomes liable to the Purchase. After this deadline, the contractor is no longer obligated to proceed.

2.3.2 Performance Monitoring

Once the contractor considers/assesses the support as provided, it is the contractor's responsibility to issue a receipt including as a minimum the following pieces of information:

- The reference number of the quotation and the purchaser PO number;
- The technical area in scope;
- The summery of the related request for support;
- The acceptance criteria completed;
- The approval signature of the designated authority (ref. § 2.3.1).

2.4 Commercial-CSE (C-CSE)- A substitute for a CSU

2.4.1 Background information

A DCM is composed of about 60 users. A DCM is considered as being a geographically isolated unit (GIU), when it is not supported by a local CSU.

In such a case, the contractor is to mitigate this situation, and be a substitute for a CSU, by becoming a C-CSE (outsourced service) and able to perform all support activities (ref. § 1.2) related to the six technical areas listed in paragraph 1.1.

A high-level vision of what is expected is presented in Annex D.

[2] Each project acceptance criteria should be clear, measurable, aligned with project manager expectations, and address functional, quality, and compliance aspects, ensuring realistic and achievable outcomes within project constraints.

2.4.2 C-CSE / Service description

The main deliverable of this SoW is the provision and delivery of a C-CSE service on nine different locations (ref. Annex C).

The C-CSE service comprises the following up to level 2 support activities: collect/configure/connect and move CIS hardware for repairs, changes, or disposals.

All the required admin privileges will be granted as necessary by the purchased, as well as the necessary spare parts to support the services locally consumed.

The contractor's personnel forming a C-CSE will all have at minimum a NATO SECRET SECURITY clearance.

Being a substitute for a CSU, a C-CSE is expected to perform at each location at least the following tasks:

- **Installation:**
  - Execute the onsite installation and configuration of CIS equipment, software, and systems as requested by the CSU.
  - Ensure that installations are completed efficiently and in accordance with organizational standards.
- **Move Management:**
  - Facilitate the physical relocation of CIS equipment and systems due to office moves or departmental reorganizations.
  - Support coordination between the relevant parties to ensure smooth transitions between locations.
- **Addition of Resources:**
  - Assist with the onsite addition of new CIS resources, such as user accounts, devices, or possibly software licenses, as needed.
  - Ensure that additions are properly documented and configured onsite to fulfil CSU's business and guidance.
- **Change Implementation:**
  - Execute onsite changes to existing CIS configurations, settings, in response to organizational needs and requests.
  - Implement changes effectively onsite.
- **Documentation and Reporting:**
  - Maintain accurate onsite records of all C-CSE activities, including documentation of changes made and any associated configurations.
  - Generate onsite reports on P-IMAC activities, including metrics related to turnaround time and customer satisfaction.
- **User Support and Training:**
  - Provide onsite and on the spot support and guidance to end-users regarding P-IMAC related processes and procedures.
- **Feedback and Improvement**
  - Update configuration management database.
  - Analysing the feedback to identify areas for improvement.
  - Implementing changes to enhance the user experience.

2.5 Contractor Responsibilities

2.5.1 General requirements

- **Personnel Management & Expertise**
  - The Contractor shall manage and be responsible for all personnel, whether assigned to strengthen a CSU or support a C-CSE service.
  - Contractor personnel shall be knowledgeable, experienced, and fully competent in performing the tasks and activities outlined in the Service.
  - All on-site contractor personnel shall hold the required Security Clearances for the entire duration of the contract.
  - Personnel shall maintain professionalism and courtesy when interacting with NATO and Purchaser's staff.
  - Contractor personnel must possess sufficient English language proficiency to ensure seamless verbal and written communication.
  - The Contractor shall strive to minimize staff rotation and maintain continuity of personnel assigned under this Statement of Work (SoW).
  - In order to manage personnel turnover effectively, the Contractor shall obtain the Purchaser's endorsement before appointing new personnel under this SoW.
- **Personnel Replacement & Transition**
  - The Contractor shall submit Requests for Change (RFC) regarding personnel replacements at least 20 working days in advance to facilitate access to required locations.
- **Equipment Handling & Compliance**
  - The Contractor shall handle Purchaser-Furnished Equipment (PFE) with due care to prevent damage or operational issues.
  - The Contractor shall install and operate all equipment in compliance with manufacturer specifications and NCI Agency guidelines.
  - During service execution, the Contractor shall minimize disruptions and impact on end users.
  - Any issues preventing service execution shall be promptly reported to the Purchaser's Point of Contact.
- **Access & Collaboration**
  - Contractor personnel shall comply with local procedures to obtain escorted/unescorted access to office spaces and locations.
  - The Contractor shall collaborate with other Purchaser support teams as necessary to ensure seamless service delivery.
  - Contractor personnel assigned to C-CSE shall use the Purchaser's IT Service Management (ITSM) ticketing system(s) in accordance with Purchaser's procedures.
- **Asset Management & Accountability**
  - The Contractor shall act as the Account Holder, taking responsibility for assigned Configuration Items and adhering to Purchaser procedures for Asset Management and NCI Agency Asset Accounting.
  - The Contractor shall conduct an annual physical inventory of assigned assets in compliance with purchaser policies.

  Further details as to Asset Management & Accounting are available in:

Agency Directive(AD) 06.00.15	Accounting for Assets AD 06-15.pdf
Agency Directive(AD) 06.00.12	Asset Management AD 06-0012.pdf

- **ITIL Alignment**
  - All contractor activities shall align with ITIL best practices and adhere to the Purchaser's specific process implementations.
  - In case of any discrepancies between ITIL guidelines and Purchaser-defined processes, the latter shall take precedence.
- **Security & Compliance**
  - Contractor personnel must strictly comply with NATO security policies and procedures, including but not limited to:
    - Confidentiality agreements
    - Access controls
    - Additional security requirements specified by the Purchaser
- **Training & Certification**
  - All contractor personnel must hold the necessary training, certifications, and qualifications relevant to their assigned tasks.
  - The Contractor shall ensure that personnel remain competent and up to date with industry standards and regulatory requirements.

2.5.2 ITIL focus for C-CSE service

- **On-site Service Operation**: Provide local support for incident resolution, request fulfilment, and other service operation activities as per ITIL guidelines.

  Further details as to Request Fulfilment are available hereafter:

Agency Standard Operating Procedure (SOP) 06.04.02	Request Fulfilment SOP 06-04-02.pdf

- **24/7**: Ensure availability of personnel for response to urgent incidents including outside standard working hours (ref. § 2.5.3).
- **Incident Management**: Respond according to the urgency and nature of the issue, as assessed in the Agency IT service Management (ITSM) tool by the Agency Centralised Service Desk (CSD).
- **Service Transition Support**: Support the implementation of changes and project activities, ensuring compliance with ITIL processes and client policies.
- **Configuration management**: Upon the effective establishment of a C-CSE service on a location, the contractor has four months to create a local CMDB focusing on the following assets categories:

- Workstations: Including age, type/brand, TEMPEST compliance, security level, and location.
- Laptops: Including age, type/brand, TEMPEST compliance, and security level.
- Mobile Phones: Documenting age and type/brand.
- Fixed Phones: Differentiating between legacy and VoIP systems, with details on security level and location.
- Crypto Assets: Specifying type/brand and location.
- Active Network Drops: Organized by building, security level, and office.

The CMDB must remain adaptable to accommodate changes in assets or organizational needs. It should be updated regularly to ensure accuracy, with random samples subject to verification by the purchaser.

- **ITSM Integration**: Utilize the ITSM tool(s) for logging, tracking, and managing all activities, ensuring detailed and accurate records.

2.5.3 Incident Priorities for C-CSE

C-CSE's Response/Restore target times have to be smaller than the one of the NCI Agency as CIS provider.

Response Target Time - durations from incident opening to assigned					
NCI Agency	P0 = 30mins wall clock	P1 = 1h wall clock	P2 (+ & -) = 1h during business hours P2 (+ & -) = 2h outside business	P3 = 9h business hours or 1 working day	P4 = 18 business hours or 2 working days
C-CSE	P0 = 15 min wall clock	P1 = 15 min wall clock	P2 (+ & -) = 30 min during business hours P2 (+ & -) = 30 min outside business hours	P3 = 8 h business hours	P4 = 16 business hours

Restore Target Time - durations from incident opening to service restored (irrespective of fault resolution)					
Agency	P0 = 1h wall Clock	P1 = 4h wall clock	P2+ = 8h wall Clock P2- = 8h business hours	P3 = 18 business hours or 2 working days	P4 = 27 business hours or 3 working Days

C-CSE	P0 = 45 min wall Clock	P1 = 3 h wall clock	P2+ = 6 h wall Clock P2- = 6 h business hours	16 business hours	24 business hours

2.5.4 NCI Agency services in scope for C-CSE service

The initial list of CIS services and their corresponding service restoration times (yearly updated in NCISG static ESLA) is available in Annex A.

2.5.5 Reporting for C-CSE service

Each C-CSE Service assigned to a location shall be **monitored and reported** as follows:

2.5.5.1 Reporting Schedule & Distribution

Report Type	Frequency & Deadline	Copies	Medium/Format	Recipients
Monthly Performance Report	By the **5th of the following month**	1 copy	Electronic / Email	Purchaser will communicate the list of recipients.
Quarterly Service Performance Report	By the **15th of the following month** after each quarter	1 copy	Electronic / Email	Purchaser will communicate the list of recipients.
List of Personnel	**Initial List**: Within **30 days** after contract award.	1 copy	Electronic / Email	Purchaser will communicate the list of recipients.
	Updates: Immediately upon any changes.			

2.5.5.2 Monthly Performance Report

The **Monthly Performance Report** shall provide an **operational overview** and key performance metrics. It must include the following elements:

1. **Activity Summary**
   - Detailed breakdown of activities performed during the reporting period, categorized by technical area.
   - Notable achievements and challenges encountered.
2. **ITSM Task Metrics**
   - Total number of assigned tasks during the reporting period.
   - Number of successfully closed tasks.
3. **ITSM Ticket Statistics**
   - Total number of **new ITSM tickets** created.
   - Total number of **resolved ITSM tickets** during the period.
   - Breakdown of tickets by request type (e.g., incidents, service requests, change requests).
4. **Breach Analysis**

- Summary of ITSM tickets **breached against SLA** during the period.
- **Root cause analysis** and justifications for each breach.
- Corrective actions or mitigation measures applied.

5. **Local CMDB Updates**
   - Documentation of **any changes to the local CMDB**, as specified in § 2.5.
   - Compliance with asset management procedures.
6. **Asset Inventory Accuracy**
   - Report on **asset inventory accuracy**, including discrepancies found.
   - This shall be provided **annually** unless otherwise specified by the Purchaser.
7. **Approved Contractor's Assets**
   - A list of all **approved contractor commercial tools and assets** currently in use.
   - Confirmation of compliance with the approved IT asset list.
8. **Trend Analysis**
   - **Comparative analysis** of task volumes, ticket resolution trends, and CMDB updates over previous reporting periods.
   - Identification of **recurring issues** or emerging service patterns.
9. **Recommendations & Lessons Learned**
   - Suggestions for **service efficiency improvements**.
   - Observations related to recurring operational challenges and potential solutions.

2.5.5.3 Quarterly Service Performance Report

The **Quarterly Service Performance Report** shall provide a **higher-level assessment** of overall service quality and compliance. It must include the following elements:

1. **Issue Highlights & Remediation Actions**
   - Summary of **significant issues encountered** during the quarter.
   - Description of **corrective actions taken** and their effectiveness.
2. **Performance Compliance**
   - Evaluation of **compliance with service-level performance metrics** defined in this SoW.
   - Assessment of SLA adherence for ITSM tickets, asset management, and personnel performance.
3. **Continual Service Improvement (CSI)**
   - Report on **improvements implemented** during the reporting period.
   - Summary of **planned service enhancements** for the next quarter.
4. **Assessed Penalties & Justifications**
   - Documentation of **any penalties assessed** during the reporting period.
   - Justifications or root cause explanations for **penalty triggers**.
   - Contractor's response and **corrective action plans**.
5. **Trend Analysis**
   - Overview of **recurring issues or improvements** over previous quarters.
   - Data-driven insights into **service trends**.
6. **Risk & Opportunity Assessment**
   - Summary of potential risks that may **impact future service delivery**.
   - Identification of **opportunities for service enhancement**.

2.5.5.4 Additional Reporting Requirements & Compliance

- **Timeliness**: All reports must be submitted **within the defined deadlines**. Delayed reports may be subject to contractual penalties.
- **Accuracy & Completeness**: Reports must be **comprehensive, accurate, and free of inconsistencies**.
- **Format & Templates**: The Purchaser may provide **standard templates** for reporting. The Contractor must **adhere to these formats** unless otherwise authorized.

2.6 Provision of Office Space and Equipment for C-CSE service

To support the establishment of the C-CSE, the Purchaser will provide office space suitable for up to four staff members, accommodating a maximum of four workstations. Each workstation will be equipped with a fixed telephone, a NATO SECRET workstation with access to the Agency's ITSM system, and a NATO RESTRICTED laptop with controlled Internet access. The office will also include desks and chairs, appropriate lighting, reliable power supply, and climate control.

The contractor is responsible for ensuring that their personnel have all necessary tools, consumables, and resources required to perform their tasks efficiently and in compliance with service requirements. Consumables include, but are not limited to, stationery, printer supplies, and maintenance materials for IT equipment. Additionally, the contractor is responsible for the repair and maintenance of their tools.

To meet security and operational standards, the contractor must submit a detailed inventory of commercial tools and assets as part of the bidding process. This inventory is subject to approval by the purchaser and must be reviewed and updated as necessary (ref. 2.5.5). Updates shall be included in the monthly performance reports.

3 Purchaser Responsibilities

- **Centralized Help Desk (Levels 1 to 2) and Level 3 Support:**
  Operate a Centralized Service Desk available 24/7 to log incidents, provide initial support, and escalate urgent or complex issues to higher-level support (level 3 and above) as needed.
- **ITIL Process Framework:**
  Provide the contractor with relevant documentation, guidelines, and training resources on the purchaser's ITIL-based processes to ensure alignment with established workflows and standards.
- **Project Definition and Approval:**
  Define and approve the scope, objectives, and timelines for all project-related activities. Review, evaluate, and formally approve the contractor's proposed solutions, ensuring they align with project goals and compliance requirements.
- **Office Space and Equipment Provision:**
  Provide office space and equipment as specified in §2.6, ensuring a secure, functional, and compliant working environment for contractor personnel.
- **Access Management and Security Compliance:**
  Issue necessary credentials, permissions, and access to physical and digital systems while ensuring adherence to security and compliance protocols.

- **On boarding and Orientation:**
  Facilitate orientation sessions for contractor personnel to familiarize them with internal tools, workflows, and security practices.
- **Operational Performance Reviews:**
  Schedule and conduct regular review meetings to evaluate the contractor's performance, address challenges, and provide constructive feedback.
- **Data and Information Sharing:**
  Ensure timely provision of relevant data, templates, and resources required for contractor operations and reporting.
- **Change Management Oversight:**
  Review and approve proposed changes to workflows, processes, or systems, ensuring seamless integration with existing operations and alignment with organizational goals.
- **Disaster Recovery and Business Continuity Support:**
  Share disaster recovery plans, protocols, and resources to ensure seamless collaboration during service interruptions or emergencies.
- **Tool and Resource Validation:**
  Validate and approve tools, software, or other assets proposed by the contractor before deployment to ensure compatibility and compliance with organizational standards.
- **Stakeholder Communication Support:**
  Facilitate effective communication between the contractor, internal stakeholders, and external vendors as necessary to ensure smooth operations.
- **Knowledge Management Support:**
  Provide access to historical records, incident reports, and documentation to support informed decision-making and operational continuity.

4 Transition and Knowledge Transfer

4.1 Handover Requirements

The incumbent contractor (the existing contractor) must fully cooperate in transitioning services to the new service contractor at the end of the contract period or upon contract termination. All processed information artefacts remain the property of NATO.

A detailed handover plan must be created by the incumbent contractor in coordination with the Purchaser and the new contractor. This plan should cover:

- Transfer of service knowledge, including incident histories, unresolved tickets, common issues, and specific user needs.
- Documentation of all technical configurations, infrastructure, and systems supported by the on-site C-CSE team.
- Transfer of any access rights, credentials, or security tokens necessary to maintain continuity of service.

4.2 Knowledge Transfer Process

The incumbent contractor must facilitate knowledge transfer to the new contractor within a transition period of 90 days.

During this period, the incumbent contractor must:

- Provide all relevant documentation (procedures, system configurations, network diagrams, etc.).

- Participate in joint training sessions or shadowing between the old and new teams to ensure that technical know-how is not lost.
- Transfer all open incidents or service requests to the new contractor, ensuring clear communication on each ticket's status.

The new contractor must confirm the receipt and understanding of all documentation and knowledge transferred.

4.3 Asset Transfer

If any physical or software assets (e.g., laptops, servers, licenses) are owned by the incumbent contractor and required to maintain services, there must be a clear plan for the return, replacement, or reassignment of these assets during the transition.

Inventory lists of all such assets should be created and verified by both the incumbent and new contractors.

4.4 Key Performance Indicators (KPIs) During Transition

During the transition, both the incumbent and the new contractors must maintain adherence to agreed service-level agreements. The incumbent must continue providing full service support until the handover is completed.

Performance monitoring must continue during the transition phase, and any service disruptions or lapses caused by the transition must be documented and reported immediately.

The new contractor should establish a transition plan that ensures a smooth ramp-up of their team, minimizing downtime and maintaining operational standards.

4.5 Collaboration and Cooperation

Both the incumbent and new contractors are expected to demonstrate cooperation and transparency during the handover process.

If the incumbent contractor fails to provide the required support during the handover period, penalties may be imposed as stipulated in the contract.

4.6 Final Acceptance of Transition

The Purchase will perform a final audit or assessment of the handover process before formally accepting the new provider.

This acceptance will be based on:

- A review of all documentation and knowledge transfer materials.
- A joint review meeting with the incumbent and new contractor to confirm that the handover is complete.
- Confirmation that the new contractor is fully operational and meeting service level agreements.

4.7 Post-Transition Support (Incumbent)

The incumbent contractor may be required to offer post-transition support for 30 days after the new provider takes over. This support should be limited to answering questions or clarifying issues related to the handover.

Any lingering issues or disputes regarding the handover should be resolved during this period.

5 Key performance indicators

All following indicators apply to each C-CSE.

#	Indicator focus	Threshold	Measurement	Report
1	Incidents	95% and above of the incidents received within each calendar month are responded, updated, resolved or escalated within targets (ref. 2.5.3)	ITSM tool	Monthly
2	Service Requests	95% and above of the service requests received within each calendar month are resolved within 1 working days when “simple” and 3 working days when “normal”.	ITSM tool	Monthly
3	Change Request	85% and above of the change requests are resolved within 10 working days when “CAT 1” and 60 working days when “CAT 2”.	ITSM tool	Monthly
4	ITSM Ticket volume	The number of the resolved Incidents, Service Requests and Change Requests within each calendar month.	ITSM tool	Monthly
5	First Contact Resolution (FCR)	The number and the rate of the incidents resolved on the first contact.		Monthly
6	Ticket Escalation Rate	The number of tickets issues that are escalated to higher levels of support.		Monthly
7	SLA Breaches	P0 and P1 Post-Breached Incident Analysis Report		AD HOC
8	Configuration management	Completeness and accuracy of the local CMDB	Site Survey versus contractor’s report	Monthly
9	User satisfaction	No more than one user complaint by month.	User written complaint received by purchaser.	Monthly
10	Annual Inventory	No discrepancies between account holder balance list and the purchaser’s one.	EBA (Enterprise Business Application)	Yearly
11	Monthly performance report	“standalone” quality - Self-contained: it includes everything needed for understanding. - Comprehensive report: it’s complete and covers all aspects of the subject. - Autonomous report: it functions independently.	Purchaser appraisal	Monthly

12	Quarterly service performance report	"standalone" quality - Self-contained: it includes everything needed for understanding. - Comprehensive report: it's complete and covers all aspects of the subject. Autonomous report: it functions independently.	Purchaser appraisal	Quarterly

6 Penalties

6.1 General Provisions

The Contractor shall comply with all obligations set forth in this Statement of Work (SoW). Failure to meet these obligations may result in penalties, deductions, or contract termination as outlined in this clause.

6.2 Types of Non-Compliance & Associated Penalties

Non-Compliance Category	Description	Penalty & Consequence
Failure to Provide Personnel	Unavailability of required personnel, excessive turnover, or failure to meet security clearance requirements.	**5% deduction per occurrence from the monthly invoice** per unfilled position exceeding 10 working days. Persistent issues may lead to **contract review/termination**.
Late Personnel Replacement	Failure to submit Requests for Change (RFC) **at least 30 days in advance**.	**2% deduction per instance from the monthly invoice** if the delay impacts service continuity.
Non-Compliance with Security Policies	Breach of NATO security policies, including unauthorized access, confidentiality breaches, or failure to follow access control procedures.	**Immediate corrective action required**. Failure to comply within 5 working days results in **10% deduction from the monthly invoice** per infraction. Severe violations may trigger **contract termination**.
Service Disruption Due to Contractor's Actions	Any failure causing disruption to end users due to negligence, improper equipment handling, or non-adherence to ITIL best practices.	**5% deduction from the monthly invoice** per major disruption. Repeated failures (>3 in a quarter) may result in **contract re-evaluation**.

Failure to Adhere to ITIL Processes & Asset Management	Non-compliance with asset accountability, failure to conduct annual inventory, or deviation from ITIL best practices.	**2% deduction per non-compliance event**, increasing to **5% for repeated infractions**.
Failure to Use Approved IT Tools & Devices	Use of unauthorized IT equipment, software, or failure to follow the IT asset approval process.	**Immediate removal of unauthorized tools**. Failure to comply results in a **5% deduction per month until rectified**.
Breach of Training & Certification Requirements	Any personnel performing tasks without the required certifications or training.	**3% deduction per non-compliant staff member per month** until rectified.
Failure to Report Issues Promptly	Any failure to inform the Purchaser's Point of Contact about service execution issues in a timely manner (in monthly report at latest).	**2% deduction from the monthly invoice** per occurrence.

6.3 Escalation & Corrective Actions

- **First Occurrence**: Written warning with a request for corrective action within **5 working days**.
- **Second Occurrence**: Financial penalties as outlined above.
- **Repeated Non-Compliance (≥3 occurrences per quarter)**: Contract performance review, with possible **increase in penalties or contract termination**.

6.4 Force Majeure Exception

Penalties shall not apply if the Contractor's failure to perform is due to **force majeure events** (natural disasters, war, government-imposed restrictions, etc.), provided that:

- The Contractor **notifies** the Purchaser within **5 working days** of the event.
- Reasonable efforts are made to **mitigate** the impact on service continuity.

7 Invoicing

As part of the contract, the Purchaser will support only following types of expenditures:

1. Annual fee for management of the contract:
    a. meetings,
    b. reports.
2. Annual fee for the provisioning of the C-CSE services (ref. § 2.4).

3. Cost for "Transition and Knowledge Transfer" (ref. § 4)
4. Variable cost that is only to occur after the Purchaser's receipting of a request for strengthening the capacities of a CSU (ref. § 2.3), or the set-up of an additional C-CSE service in a new location. The invoicing for this type of cost will be done upon the contractor's request on successful completion of the contractual obligations, or half at the start of the support, and the other half at the end of the current year at latest (assuming successful completion of the contractual obligations).

From one year to the next, all types of cost will be updated to take into account the market conditions prevailing on the 1st of December of year N, for year N+1.

8 Timelines

Contract Duration: the current contract is a ten years contract.

Service Start Date: as of the first of January 202x.

9 Bid evaluation

The Contractor bid for this SoW will be assessed using a best value approach.

- ITIL Certification and Experience in Service Delivery: the contractor is to elaborate on this topic in less than 200 words.

#	Focus point	Max Weight	Level of confidence
/	ITIL Certification and Experience in Service Delivery	10	High/Low

- C-CSE service: the contractor is to explain in a memo how they plan to deliver the C-CSE service (further details as to the memo are available in Annex E).

#	Focus point	Max Weight	Level of confidence
A	Service Integration & Workflow	20	High/Medium/Low 20/10/0
B	Response & Resolution Times	30	High/Medium/Low 30/15/0
C	Technical Expertise & Resources	20	High/Medium/Low 20/10/0
D	Proactive vs. Reactive Support	10	High/Medium/Low 10/5/0
E	Reporting, Metrics, & Service Improvement	5	High/-/Low 5/-/0
F	User Experience & Satisfaction	20	High/Medium/Low 20/10/0
G	Flexibility & Customization	5	High/Medium/Low 5/-/0
H	Risk Management & Business Continuity	30	High/Medium/Low 30/15/0
	Max score on C-CSE memo	**140**	**/**

- Each quotation of a Purchaser's request for strengthening a CSU capacity is to be broken-down against the three following unitised costs:

#	Type of cost – CSU XYZ	Hourly cost
1	Administrative and management matters	
2	Technical support	
3	Engineer support	

One table is to be created by CSU listed in Annex C.

No additional cost will be supported by the Purchase related to a request once the contractor acceptance of the request has happened.

The contractor's best value is to be assessed using the fictitious requests available in Annex F.

- Cost of the C-CSE service: the cost is all-inclusive, and is to be broken-down by location (ref. Annex C).

#	Unit	Supporting Unit	Cost
1	NCISG 1NSB DCM D Blandford/Dorset (GBR)	C-CSE (United Kingdom)	
2	NCISG 1NSB DCM E Haderslev (DNK)	C-CSE (Denmark)	
3	NCISG 1NSB DCM F Pleso (HRV)	C-CSE (Croatia)	
4	NCISG 2NSB DCM E Bucharest (ROU)	C-CSE (Romania)	
5	NCISG 2NSB DCM F Gorna Malina (BGR)	C-CSE (Bulgaria)	
6	NCISG 3NSB DCM B Lipnik nad Becvou (CZE)	C-CSE (Czechia)	
7	NCISG 3NSB DCM C Ruzomberok (SVK)	C-CSE (Slovakia)	
8	NCISG 3NSB DCM D Vilnius (LTU)	C-CSE (Lithuania)	
9	NCISG 3NSB DCM E Szekesfehervar (HUN)	C-CSE (Hungary)	

- Cost of Transition and Knowledge Transfer (ref. § 4):

#	Supporting Service	Cost
1	C-CSE (United Kingdom)	
2	C-CSE (Denmark)	
3	C-CSE (Croatia)	
4	C-CSE (Romania)	
5	C-CSE (Bulgaria)	
6	C-CSE (Czechia)	
7	C-CSE (Slovakia)	
8	C-CSE (Lithuania)	
9	C-CSE (Hungary)	

Annex A Indicative list of consumed services

Hereafter the list of CIS services and their corresponding restoration times (yearly updated in NCISG ESLA)

NCI Agency Service Code	NCI Agency Static CIS Services in scope	Priority
INF001	LAN Service	P1 (4WC)
WPS001	Managed Device Service	P1 (4WC)
WPS002-1	Enterprise Identity Access Management Service (Former User Access Service)	P1 (4WC)
WPS009-1	Unclassified Voice Collaboration Service	P1 (4WC)
WPS010-1	Soft Client	P1 (4WC)
WPS010-10	Immersive Telepresence Meeting (ITP) Room	P1 (4WC)
WPS012	Workstream Collaboration Service	P1 (4WC)
WPS014-1	Secure Voice Static	P1 (4WC)
WPS014-2	Secure Voice Mobile	P1 (4WC)
APP001	Approved COTS Products Procurement Service (APP001)	P2 (8 hrs)
PLT001-7	Information Sharing and Collaboration Platform Services, flavour Advanced Portal	P2 (8 hrs)
WPS006	REACH Mobile Workplace Service	P2 (8 hrs)
WPS007-1-A	Print/Scan/Copy Service - COCO-A3 Large Print Volume MFD	P2 (8 hrs)

NCI Agency Service Code	NCI Agency Static CIS Services in scope	Priority
WPS007-1-B	Print/Scan/Copy Service - COCO-A3 MFD	P2 (8 hrs)
WPS007-1-C	Print/Scan/Copy Service - COCO-A4 MFD	P2 (8 hrs)
WPS007-1-D	Print/Scan/Copy Service - COCO-A4 Desktop-sized MFD	P2 (8 hrs)
WPS007-2	Print/Scan/Copy Service - NONO	P2 (8 hrs)
WPS008	Enterprise Services Operations Centre (ESOC) Service	P2 (8 hrs)
WPS010-11	B2B Connection	P2 (8 hrs)
WPS010-2	VTC System Only	P2 (8 hrs)
WPS010-3	Desktop VTC Terminal	P2 (8 hrs)
WPS010-5	VTC Room - Roll About DDS	P2 (8 hrs)
WPS010-6	VTC Room - 15 person	P2 (8 hrs)
WPS010-7	VTC Room - 25 person	P2 (8 hrs)
WPS010-8	VTC Room - 50 person	P2 (8 hrs)
WPS010-9	VTC Room - 175 person	P2 (8 hrs)
WPS016-5	Enterprise Managed Mobility Service - Multi-Factor Authentication token for non- managed devices	P2 (8 hrs)
WPS016-6	Enterprise Managed Mobility Service - Option: Mobile Secure Communication on Smartphones	P2 (8 hrs)

NCI Agency Service Code	NCI Agency Static CIS Services in scope	Priority
WPS016-A	Enterprise Managed Mobility Service - Smartphone/Tablet (iOS Only)	P2 (8 hrs)
WPS016-B-1	Enterprise Managed Mobility Service - Cellular Subscription (Profile Plan 1 – Basic)	P2 (8 hrs)
WPS016-B-2	Enterprise Managed Mobility Service - Cellular Subscription (Profile Plan 2 – Standard)	P2 (8 hrs)
WPS016-B-3	Enterprise Managed Mobility Service - Cellular Subscription (Profile Plan 3 – Traveller)	P2 (8 hrs)
WPS016-B-4	Enterprise Managed Mobility Service - Cellular Subscription (Profile Plan 4 – Traveller Unlimited)	P2 (8 hrs)
WPS016-B-5	Enterprise Managed Mobility Service - Cellular Subscription (Profile Plan 5 - Data Plan Hotspot)	P2 (8 hrs)
WPS016-C	Enterprise Managed Mobility Service - Remote Access for NU WPS001 Laptops	P2 (8 hrs)

Annex B Tool and Resource Validation

This annex defines the approval process for IT assets, tools, and software proposed by the Contractor to ensure compliance with local security policies, compatibility with the work environment, and adherence to organizational standards.

SCOPE

This process applies to:

- All owned Contractor's IT devices, tools, and software proposed for use by the Contractor.
- Any Contractor's owned devices intended for integration into the supported environment.

GENERAL PRINCIPLES

- Only NATO-provided assets and Purchase-approved devices may be used within the work environment.
- All tools, software, and IT assets proposed by the Contractor **must undergo validation and approval** by the purchaser, before deployment.
- Unauthorized devices are strictly prohibited on supported sites.
- The Purchaser retains the right to reject any proposed tool or asset if deemed non-compliant with security policies.

APPROVAL PROCESS WORKFLOW

Step 1: Submission of Approval Request

- The Contractor shall submit a formal request to the Purchaser, including:
  - **Asset Type:** Hardware, software, or tool.
  - **Purpose & Justification:** Explanation of the need for the asset.
  - **Technical Specifications:** Manufacturer details, model, version, and system requirements.
  - **Security & Compliance Assessment:** Any known security risks and mitigation measures.
  - **Compatibility Assessment:** Expected interactions with existing systems.

Step 2: Initial Review & Validation

- The Purchaser's designated team will perform an initial review to:
  - Assess security and compliance requirements.
  - Validate technical feasibility and compatibility.
  - Request additional documentation if necessary.

Step 3: Security & Compliance Approval

- If applicable, the asset will be assessed by the **relevant NATO Team** to:
  - Verify adherence to local security policies.

- Identify any risks associated with its deployment.
- Approve or recommend modifications for compliance.

Step 4: Final Decision & Approval

- The Purchaser will:
  - Approve or reject the request.
  - Provide feedback or conditions for approval.
  - Issue formal authorization for deployment (if approved).

Step 5: Deployment & Monitoring

- Upon approval, the Contractor may deploy the asset following the approved implementation plan.
- The Purchaser reserves the right to **audit and revoke approval** if compliance issues arise.

TIMELINES

Stage	Responsible Party	Estimated Timeline
Submission of Request	Contractor	As needed
Initial Review	Purchaser Team	5-10 working days
Security & Compliance Check	Security Team	10-15 working days
Final Decision & Approval	Purchaser	5 working days
Deployment & Monitoring	Contractor	Ongoing

Note: Timelines may vary based on the complexity of the request and additional security reviews.

RESPONSIBILITIES

- **Contractor:**
  - Submits complete and accurate approval requests.
  - Ensures that only approved assets are used.
  - Implements security measures for all approved assets.
- **Purchaser:**
  - Reviews and validates all requests.
  - Ensures compliance with security policies.
  - Provides timely approval or feedback.
- **NATO "Security & Compliance" relevant Team:**
  - Conducts security assessments and risk evaluations.
  - Check compliance with NATO policies and procedures.

NON-COMPLIANCE & CONSEQUENCES

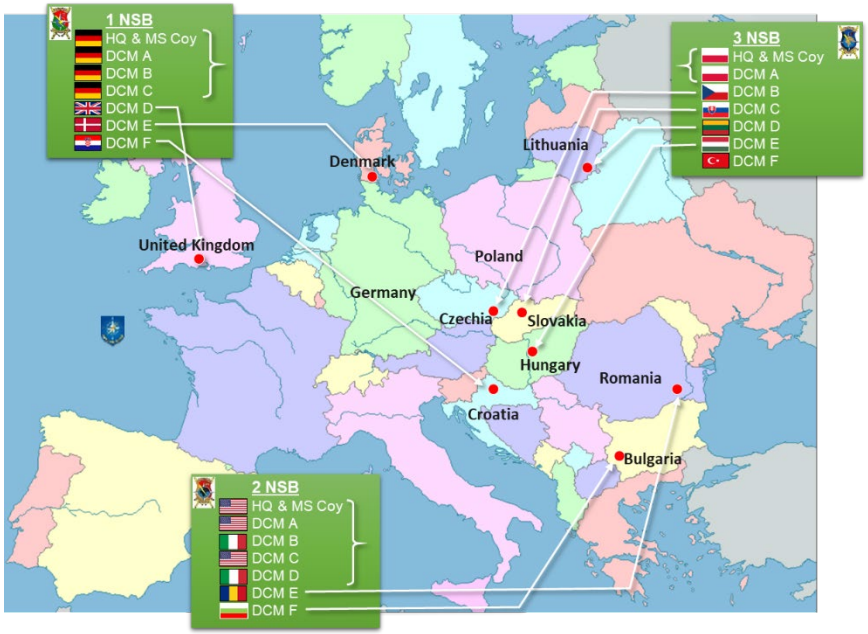
- Unauthorized IT assets may be subject to **immediate removal** from the work environment.
- Security violations resulting from unauthorized assets may lead to penalties or contract review.

- The Purchaser reserves the right to **audit the Contractor's compliance** at any time.

Annex C Locations in scope

List of current NCISG units, with their supporting unit. Nine C-CSE services are required.

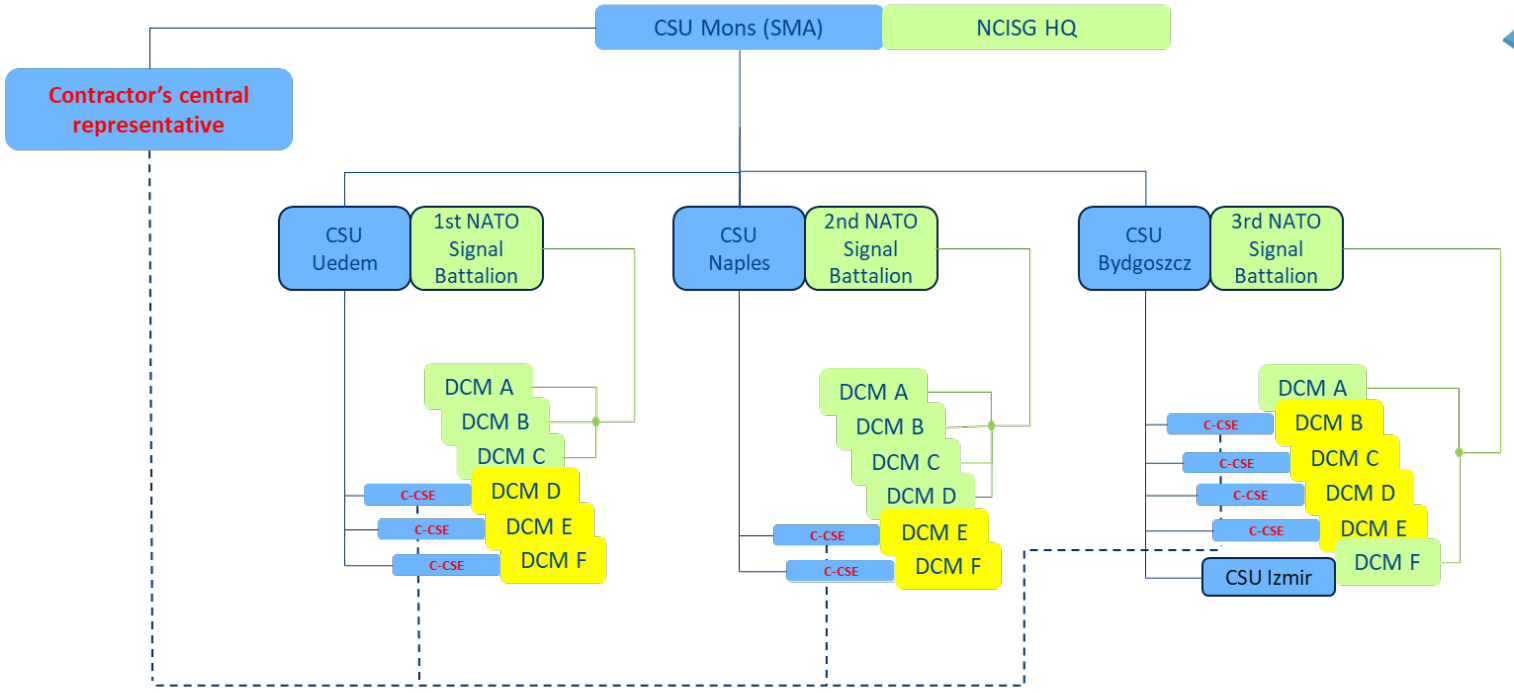
Unit	Supporting Unit
NCISG HQ Mons (BEL)	CSU Mons
NCISG 1NSB HQ Wesel (DEU)	CSU Uedem
NCISG 1NSB M&S COY Wesel (DEU)	CSU Uedem
NCISG 1NSB DCM A Wesel (DEU)	CSU Uedem
NCISG 1NSB DCM B Wesel (DEU)	CSU Uedem
NCISG 1NSB DCM C Wesel (DEU)	CSU Uedem
NCISG 1NSB DCM D Blandford/Dorset (GBR)	**C-CSE (United Kingdom)**
NCISG 1NSB DCM E Haderslev (DNK)	**C-CSE (Denmark)**
NCISG 1NSB DCM F Pleso (HRV)	**C-CSE (Croatia)**
NCISG 2NSB HQ Grazzanise (ITA)	CSU Naples
NCISG 2NSB M&S COY Grazzanise (ITA)	CSU Naples
NCISG 2NSB DCM A Grazzanise (ITA)	CSU Naples
NCISG 2NSB DCM B Grazzanise (ITA)	CSU Naples
NCISG 2NSB DCM C Grazzanise (ITA)	CSU Naples
NCISG 2NSB DCM D Grazzanise (ITA)	CSU Naples
NCISG 2NSB DCM E Bucharest (ROU)	**C-CSE (Romania)**
NCISG 2NSB DCM F Gorna Malina (BGR)	**C-CSE (Bulgaria)**
NCISG 3NSB HQ Bydgoszcz (POL)	CSU Bydgoszcz
NCISG 3NSB M&S COY Bydgoszcz (POL)	CSU Bydgoszcz
NCISG 3NSB DCM A Bydgoszcz (POL)	CSU Bydgoszcz
NCISG 3NSB DCM B Lipnik nad Becvou (CZE)	**C-CSE (Czechia)**
NCISG 3NSB DCM C Ruzomberok (SVK)	**C-CSE (Slovakia)**
NCISG 3NSB DCM D Vilnius (LTU)	**C-CSE (Lithuania)**
NCISG 3NSB DCM E Szekesfehervar (HUN)	**C-CSE (Hungary)**
NCISG 3NSB DCM F Izmir (TUR)	CSU Izmir



List of the CSUs in direct support of NCISG: CSU Mons, CSU Uedem, CSU Naples, CSU Bydgoszcz, CSU Izmir

Annex D Vision – On-site support reporting lines

On-site support reporting lines



SMA: ESLA Service Management Authority
SPOC: ESLA Single Point of Contact for NCISG HQ

Internal contractor's reporting line
On-site support focused reporting line
Co-located

On-site Support: Agency in-house capacity
On-site Support: Agency outsourced capacity

Annex E Evaluation criterions of C-CSE memo

The memo outlining the Contractor's plans to deliver the C-CSE service shall not exceed 5,000 words (approximately 10–15 double-spaced pages) and shall, at a minimum, address the following areas:

A. Service Integration & Workflow

Key Points:

- **Coordination with CSD**: How seamlessly does the C-CSE integrate with the CSD? The memo is to describe a clear handover process when a ticket escalates from remote to on-site?
- **Communication Channels**: Are the communication methods between the CSD and C-CSE clearly defined? The contractor is to provide detailed explanations of collaboration tools and escalation pathways.
- **Ticket Management**: How is ticket tracking, progress updates, and closure handled? The contractor is to explain how they plan to use the Agency ITSM platform to keep both the CSD and C-CSE synchronized.

Evaluation Focus: Efficient, well-defined integration workflows between CSD and CSE, minimizing any downtime or confusion during escalations.

B. Response & Resolution Times

Key Points:

- **Response Time Commitment**: Does the C-CSE guarantee a timely response to requests when dispatched from the CSD?
- **Restoration Time Targets**: What restoration or resolution time commitments are made, and how do they align with § 2.5.3?
- **Availability & Coverage**: Is there 24/7 coverage? What happens during weekends, holidays, or off-hours?

Evaluation Focus: The proposal should demonstrate an ability to meet or exceed agreed response and restoration targets.

C. Technical Expertise & Resources

Key Points:

- **Skill Set of On-Site Team**: What qualifications and certifications are required for the C-CSE team? The contractor's staff have the necessary expertise for the specific environment (e.g., hardware, network, and software support).
- **Specialized Support**: Are there specialists available if required (network engineers, security experts)? How does the contractor plan to escalate complex issues?
- **Resource Scalability**: Can the C-CSE team scale up (either in size or skills) if needed, for special projects or peak times?

Evaluation Focus: Ensure that the C-CSE team has the right technical skills and can adapt to Purchase's needs, with scalability options in place.

D. Proactive vs. Reactive Support

Key Points:

- **Proactive Monitoring**: Does the C-CSE service include proactive monitoring or preventive maintenance to reduce the number of escalations to the CSD? How does the C-CSE detect and prevent issues before they impact users?
- **Preventive Actions**: Are any preventative measures or audits part of the service offering to avoid recurrent issues?

Evaluation Focus: Services that offer more than reactive support, emphasizing preventive maintenance and reducing overall ticket volume.

E. Reporting, Metrics, & Service Improvement

Key Points:

- **Performance Metrics**: Does the service offer detailed reporting on key performance indicators (KPIs) such as ticket resolution time, user satisfaction, or incident recurrence?
- **Continuous Improvement**: Does the contractor outline a continuous improvement process? Look for feedback loops, regular review meetings, and actionable insights for better service delivery.
- **Transparency & Accountability**: How are issues tracked by the C-CSE, and how transparent is the C-CSE in reporting ongoing problems?

Evaluation Focus: Strong, regular reporting mechanisms and a commitment to continuous service improvement.

F. User Experience & Satisfaction

Key Points:

- **User Feedback Mechanisms**: How does the contractor ensure that the on-site service meets user satisfaction? Are there user surveys, feedback loops, or satisfaction metrics included in the proposal?
- **Communication with Users**: How well does the proposal describe the C-CSE's ability to communicate with users, providing clear updates on ticket status, delays, and expected resolution times?

Evaluation Focus: Contractors that prioritize user experience, communication, and satisfaction. This will likely result in more effective on-site support.

G. Flexibility & Customization

Key Points:

- **Customization of Service**: Does the proposal allow for customization of the service to meet Purchase's specific requirements? Can the contractor adapt the C-CSE offering to different locations, user groups, or special conditions?
- **Flexibility in SLAs**: Can the contractor adjust service-level agreements based on varying needs in different areas (e.g., alert status of supported DCM)?

Evaluation Focus: How flexible is the contractor in tailoring the service to Purchase's specific needs and circumstances?

H. Risk Management & Business Continuity

Key Points:

- **Risk Mitigation**: What plans are in place to mitigate risks such as high staff turnover, supply chain delays, or failure of IT infrastructure on the C-CSE side?
- **Continuity of Service**: How does the proposal ensure that on-site support continues during emergencies or unexpected events (e.g., pandemics, natural disasters)?

Evaluation Focus: Proposals should have solid risk management and business continuity strategies in place.

Annex F User cases

User Case 1: CSU Mons issued the following request:

- **Date of the Request**: 01/02/2026
- **Technical Area(s) to be Strengthened**: Infrastructure services
- **Required Security Clearance**: NATO SECRET
- **Summary of the Requirement**:
  During excavation work for a new construction project, the underground cable pathway between Building 101 and Building 306 was severed. Both fibre and copper cabling were impacted and require full repair, replacement, and certification testing.
- **Detailed Requirements:**
  - **Fibre Cabling**:
    - Repair or replace all affected fibre cables using **OM3 outdoor-rated cable** suitable for inter-building runs.
    - Confirm whether single-mode fibre strands are present and require repair.
    - Provide fusion splicing as required, with proper protection in enclosures.
  - **Copper Cabling**:
    - Repair or replace all affected copper cables with Cat6 (minimum) outdoor-rated cabling.
    - Terminate in existing or new patch panels where applicable.
  - **Cable Pathway**:
    - Repair or replace the damaged pathway between Buildings 101 and 306.
    - Specify whether this involves new ducting, manholes, or conduit repairs, and provide material specifications.
    - Ensure pathway is compliant with fire, safety, and building regulations.
  - **Testing & Documentation**:
    - OTDR test results for each repaired/replaced fibre strand.
    - TDR test results for each repaired/replaced copper line.
    - Provide labelled, updated as-built drawings (digital and hard copy) showing origin and termination points for each connection.
  - **Timeline**:
    - Work to commence at the earliest possible date.
    - Completion, including testing and reporting, required within **60 calendar days**.
  - **Constraints**:
    - Work permitted only during normal working hours due to ongoing construction.
    - Contractor must coordinate daily with local construction teams to avoid conflicts.
    - Site access and security requirements will be managed in cooperation with the Purchase.
- **Project Acceptance Criteria:**
  - OTDR test results confirm all fibre strands are operational.
  - TDR test results confirm all copper lines are operational.
  - Updated as-built files delivered, accurate, and approved.
  - Final acceptance by CSU MONS Technical Coordinator.
- **Additional Information for Quotation:**
  - Approximate distance of the pathway between Buildings 101 and 306: **150 meters**.

- Number of impacted fibre strands: **24-core cable, of which 12 are damaged**.
- Number of impacted copper cables: **48 pairs**.
- Existing infrastructure: ducts, manholes, or conduits are present but damaged; bidders to propose repair or replacement approach.
- Contractor to provide warranty terms for all materials and workmanship.
- All work to comply with **Agency cabling standards** and relevant **ISO/IEC 11801** and **TIA/EIA** standards.

- **Local Authority Responsible for Receipting:**
  - CSU MONS Technical Coordinator

User Case 2: CSU Uedem issued the following request:

- **Date of the Request**: 01/02/2026
- **Technical Area(s) to be Strengthened:** Application services
- **Required Security Clearance:** NATO SECRET
- **Summary of the Requirement:**
  A new software package is to be deployed for 20 users on the NATO SECRET Network. Each user's workstation requires specific configuration changes, and Group Policy updates must be applied accordingly. The software must be fully integrated into the Agency's Software Center for controlled deployment.
- **Detailed Requirements:**
  - **Pre-Deployment**:
    - Support compatibility testing of the software on the NATO SECRET Network and confirm compliance with Agency security and configuration standards.
    - Identify and document any prerequisites (e.g., OS version, patch levels, required frameworks).
  - **Software Upload & Deployment**:
    - Upload the approved software package to the NATO SECRET Network.
    - Configure deployment parameters for each of the 20 workstations (user-specific settings, registry changes, local config).
    - Update Group Policy Objects (GPOs) to apply consistent settings for all impacted users/workstations.
    - Package the software for deployment via Software Center (SCCM), ensuring silent install/uninstall functionality and rollback capability.
  - **Coordination**:
    - Liaise with 20 identified users to schedule installation windows.
    - Provide basic user instructions or FAQs if required.
  - **Testing & Reporting**:
    - Validate successful installation on pilot workstations before mass deployment.
    - Confirm correct application of Group Policies.
    - Deliver final report including deployment steps, GPO changes, pilot results, and list of affected users.
  - **Timeline**:
    - Deployment to start at the earliest possible date.
    - Full completion, including testing and reporting, within **30 calendar days**.
- **Project Acceptance Criteria:**

- Software successfully deployed and accessible through Software Center by authorized users only.
- All installations meet the functional requirements of the requestor.
- GPO updates applied consistently across all affected users.
- Final report accepted by CSU MONS Technical Coordinator.

- **Additional Information for Quotation:**
  - Software details: name, version, vendor, and licensing model (per-user, per-device, concurrent).
  - Licensing: confirm whether licenses are provided by the Purchase or to be supplied by the Contractor.
  - Workstation environment: OS version, hardware specs, and current domain/AD configuration.
  - Existing SCCM/Software Center environment: confirm available packaging standards and deployment model.
  - Whether user training or handover documentation is required.
  - Warranty/support requirements for the deployed software.
- **Local Authority for Receipting:**
  CSU Uedem Technical Coordinator

User Case 2: CSU Naples issued the following request:

- To Be Completed -

User Case 2: CSU Bydgoszcz issued the following request:

- To Be Completed -

User Case 2: CSU Izmir issued the following request:

- To Be Completed -

The cost related to of each of the user case above is to be broken down as follows:

User case	Type of cost	Proposal	Total
1 – CSU Mons	Admin and Management		
	Technical support		
	Engineer support		
2 – CSU Uedem	Admin and Management		
	Technical support		
	Engineer support		
3 – CSU Naples	Admin and Management		
	Technical support		
	Engineer support		
4 – CSU Bydgoszcz	Admin and Management		
	Technical support		
	Engineer support		
5 – CSU Izmir	Admin and Management		

	Technical support		
	Engineer support		
Grand-total			

Annex G Acronyms

AD	Agency Directive
AV	Audio Video
C-CSE	Commercial CIS Support Element
CIS	Communication and Information System
CMDB	Configuration Management Database
COMSEC	Communications security
CSU	CIS Support Unit
DCM	Deployable CIS Modules
FAS	Functional Area Systems
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
LAN	Local Area Network
NATO	North Atlantic Treaty Organisation
NCI Agency	NATO Communications & Information Agency
NCISG	NATO Communications & Information systems Group
OS	Operating System
PaaS	Platform as a Service
PDED	Process definition & execution document
PFE	Purchaser's furnished equipment
P-IMAC	Provisioning, Install, Move, Add, Change
PO	Purchase Order
SMA	Service Management Authority
SOP	Agency Standard Operating Procedure
SoW	Statement of Work
VTC	Video Teleconferencing
WAN	Wide Area Network