NCIA Request for Information (RFI)

INTEGRATED EVENT OPERATIONS (IEO) PLATFORM
RFI-07127-IEO

NCIA/ACQ/2026/07127
Friday, 15 May 2026

NCIA Request for Information (RFI)

To: Industry Partners

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 an Integrated Event Operations (IEO) Platform. To that end, we are issuing the attached Request for Information (RFI) **RFI-07127-IEO** 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 Sven Schumacher, Senior Contracting Officer at RFI-07127-IEO@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.

8. In accordance with the NATO Management of Non-Classified NATO Information policy (*internal NATO reference: C-M(2002)60*), this RFI shall not be published on the internet.

For the Chief of Acquisition:

Sven Schumacher

Digitally signed by Sven Schumacher
Date: 2026.05.18 10:58:02 +01'00'

Sven Schumacher
Senior Contracting Officer

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 an **Integrated Event Operations (IEO) Platform** to support the end-to-end event lifecycle for NATO Education, Training, Exercises and Evaluation (ETEE) activities (e.g., create, plan, coordinate, approve, publish, execute and close events), and to provide for data exchange with other relevant services and applications. 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 (IFB).

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.
2. NCI Agency is primarily interested in solutions that support two core capability areas:
   a) event registration / participant management workflows;
   b) event-related resource management (e.g., rooms/venues, IT resources, catering, accommodation, transportation), including request/approval/allocation tracking and change handling.
3. In addition, NCIA seeks industry input on:
   a) realistic integration/toolset approaches where a single COTS product does not cover all capability areas;
   b) on-premises and multi-network deployment constraints;
   c) cybersecurity maturity/security-by-design evidence;
   d) support models, service delivery maturity, and user experience/usability;
   e) the supplier's ability to operate under an underpinning support contract where NCIA remains accountable for service delivery to the user community (i.e., supplier maturity, support governance, and responsiveness);
   f) Rough Order of Magnitude (ROM) costs (licensing, implementation, integration, O&M).

C. Background

1. The IEO Platform is expected to support use by multiple entities/communities, and be adaptable/configurable to different processes across those entities.
2. The IEO Platform shall support the end-to-end event lifecycle for NATO ETEE activities (create, plan, coordinate, approve, publish, execute and close events).
3. In addition to registration/participant management and resource management, the solution shall support event-adjacent processes such as Real-Life Support (RLS) planning/coordination and IT provisioning, either natively or via integration.
4. The solution must be deployable and operable on-premises within NATO secured networks (Software-as-a-Service (SaaS)-only solutions are not acceptable), and it must support controlled data exchange with other applications (e.g., IT Service Management (ITSM) systems) using standard integration mechanisms (e.g., APIs).

5. Detailed capability and evidence requests are provided in Annex A (structured tables) and Annex B (draft requirements).

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 **29 May 2026**.

   b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
      i. Responses to Annex A and comments on Annex B

      excluding:
      i. Cover page
      ii. Company brochures or product literature (if included)
      iii. Attachments such as past performance references

   c. Use the following subject line for submission
      i. "Response to RFI-07127-IEO – [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 Requirements.

E. Industry Engagement

1. Technical discussions and/or demonstrations may take place following the submission of responses, with the purpose of clarifying or further augmenting those responses where required. Respondents are requested to await further instructions after their submissions and are requested not to contact any NCI Agency staff directly other than the POC identified at paragraph H.

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. Mr. Sven Schumacher, Senior Contracting Officer

2. E-mail: RFI-07127-IEO@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:

2. **General Questions**:

   1. Do you have an industry solution that currently meets the requirements as detailed in ANNEX B?
      ☐ Yes ☐ No

   2. Which solution approach best describes your proposal (select one):
      ☐ A. Single product covering the required capability areas
      ☐ B. Primary product + integrations to cover remaining required capability area(s)
      ☐ C. Toolset (two or more products) integrated to cover the required capability areas

   3. Can your solution be implemented and operated fully on-premises within NATO secured networks (SaaS-only solutions are not acceptable)?
      ☐ Yes ☐ No
      If "No", identify which components require external services and whether on-premises alternatives exist.

   4. Can your solution be deployed in multiple security domains/networks, (i.e., separate instances per domain), including in environments with no direct Internet access (effectively air-gapped)?
      ☐ Yes ☐ No
      If "Yes", can it support controlled replication/synchronisation of selected data between the two instances via approved NATO cross-domain mechanisms (not provided by the supplier), including one-way transfer mechanisms (e.g., data diodes), where permitted by security policy?
      ☐ Yes ☐ No ☐ Depends (please state assumptions)?

   5. Provide details of where it is used and deployed and the number of users/events supported (include scale comparable to ~15,000 users if applicable).

   6. Provide a brief summary of your company's experience delivering and supporting on-prem enterprise services under contract for defence/government customers.

3. Detailed Questions

1. Capability coverage (mandatory)

Table 1 - Capability coverage

Capability area	Native	Via integration	Not available	Notes
End-to-end event lifecycle (create/plan/approve/publish/execute/close)	☐	☐	☐	
Registration workflows	☐	☐	☐	
Participant management	☐	☐	☐	
Resource management - rooms/venues	☐	☐	☐	
Resource management – room layout / space allocation plan	☐	☐	☐	
Resource management - catering	☐	☐	☐	
Resource management - accommodations	☐	☐	☐	
Resource management - transportation	☐	☐	☐	
Resource management - communications	☐	☐	☐	
Resource management - IT resources	☐	☐	☐	
RLS planning/coordination	☐	☐	☐	
IT provisioning workflows	☐	☐	☐	
Provide event/event-related information to other applications (e.g., IT Service management (ITSM)	☐	☐	☐	
Multi-entity support (different communities/processes)	☐	☐	☐	
Integration/data exchange mechanisms (APIs and/or standard methods)	☐	☐	☐	
Receive event/event-related information from other applications	☐	☐	☐	
Role-based access control and audit logging	☐	☐	☐	
Scale to large communities (up to ~15,000 users)	☐	☐	☐	

2. Integration effort (mandatory)

a. Does your proposed solution require integration with other tool(s)/system(s) to meet all mandatory requirements in ANNEX B?
☐ Yes ☐ No

b. If "Yes":
   i. Estimated number of integrations required (best estimate): ____
   ii. Who would deliver the integrations (select one):
   ☐ Supplier ☐ Supplier/Partner ☐ NCIA ☐ Combination
   iii. Are integration costs included in your ROM pricing (Section 5.1)?
   ☐ Yes ☐ No

3. External/cloud dependency disclosure (mandatory)

a. Does the solution require external/cloud connectivity for any of the following? (Y/N)
   i. Licence activation/validation ☐ Yes ☐ No
   ii. Telemetry/usage reporting ☐ Yes ☐ No
   iii. Patch/update repositories ☐ Yes ☐ No
   iv. Support portal access ☐ Yes ☐ No
   v. Map/geocoding services ☐ Yes ☐ No
   vi. Email/SMS gateways ☐ Yes ☐ No

vii. Other (specify): ☐ Yes ☐ No

b. If "Yes" to any item above, state whether it can be disabled or replaced with an on-premises alternative and whether the solution can be fully operated without Internet access (air-gapped operation): _____

4. Cybersecurity evidence (mandatory)

Table 2 - Cybersecurity evidences

Evidence item	Available now (enclose/reference)	Available on request	Not available	Reference
Secure Development Lifecycle (SDLC) description	☐	☐	☐	
Vulnerability disclosure policy / intake process	☐	☐	☐	
Vulnerability remediation policy (target timelines by severity)	☐	☐	☐	
Independent penetration test evidence (within last 24 months)	☐	☐	☐	
Internal penetration testing practice (frequency): ☐ Annual ☐ Per major release ☐ Ad hoc ☐ None	☐	☐	☐	
Use of automated security testing	☐	☐	☐	
Software Bill of Materials (SBOM) available	☐	☐	☐	
Dependency vulnerability monitoring / CVE tracking	☐	☐	☐	
Secure configuration / hardening guide for on-prem deployment	☐	☐	☐	
Commitment to remediate Critical/High findings from NCIA security testing as part of acceptance and O&M	☐	☐	☐	

a. For "Independent penetration test evidence (within last 24 months)", respondents shall state one of the following (mandatory):

☐ Redacted report ☐ Executive summary/attestation ☐ Not available.

b. Penetration test remediation commitment (mandatory):
Can you commit to remediation of Critical/High findings identified during NCIA security testing within agreed timeframes?
☐ Yes ☐ No
If "Yes", propose targets (e.g., Critical __ days; High __ days):
_____

5. Support model (mandatory)

Table 3 - Support model (fill all rows)

Support element	Supplier response)
Support coverage (select)	☐ 8x5 ☐ 12x5 ☐ 24x7 ☐ Other: ____
Incident intake channels (select):	☐ Portal ☐ Email ☐ Phone ☐ Other: ____
Severity levels used (e.g., Sev1–Sev4)	
Target response times by	

severity (e.g., Sev1 __h; Sev2 __h; Sev3 __h; Sev4 __h)	
Target workaround/resolution times by severity (if applicable)	
Escalation model (L1/L2/L3; supplier vs partner)	
Patch/hotfix process (how security fixes are delivered for on-prem)	
Typical release cadence (e.g., monthly/quarterly)	
Support language(s) provided (e.g., English)	

6. User interface / usability (mandatory – structured)

Table 4 – User interface / usability (fill all rows)

UI element	**Supplier response)**
Primary UI type (select):	☐ Web UI ☐ Desktop ☐ Mobile app ☐ Hybrid
Role-based UI support (select):	☐ Event planners ☐ Support staff ☐ Participants
Accessibility statement available (e.g., WCAG alignment):	☐ Yes ☐ No
Localisation/language support (list):	
Evidence provided (select):	☐ Screenshots ☐ User guide excerpt ☐ Short demo video link Reference: ____

7. Assumptions (mandatory)

List key assumptions used in your response (e.g., users, entities, environments, integrations):

_____

8. Commercial Aspects

a. Are there any restrictions on the use and deployment of the proposed solution within: NATO; NATO nations; or NATO deployed operations?
☐ Yes ☐ No
If "Yes", please describe

b. Can you or a third party provide additional life cycle support services for on-premises deployments (e.g., implementation, integration, testing, and O&M support)?
☐ Yes ☐ No
If "Yes", please describe at high level

9. Rough Order of Magnitude (ROM) price data

ROM costs (EUR) - provide 5-year estimate and assumptions:
Please provide ROM pricing data for the solution, including initial costs for licenses / subscriptions (if applicable), implementation/configuration, integration (if applicable), and O&M costs for the next 5 years (state all assumptions and pricing drivers, e.g., users/modules/environments).

Table 5 - ROM costs

Cost element	**Year 0 (one-time)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Assumptions / pricing basis** (e.g., users, entities,

							environments, integrations)
Licenses / subscription							
Implementation/configuration							
Integration (if required)							
O&M / support							
Training (optional)							
TOTAL							

10. Previous NATO or Equivalent National Defence Experience

a. Does your company have experience in achieving Security Certification and Accreditation through the NATO or equivalent national defence process?
☐ Yes ☐ No
If "Yes", please list applicable past projects and any existing product certifications your solution may already hold

b. Does your company have experience in achieving approval through the NATO Request for Change (RFC) or an equivalent national defence process?
☐ Yes ☐ No
If "Yes", please list applicable past projects

d. Questions or Concerns

i. Risks, concerns, or barriers

ii. Suggestions for risk mitigation or enhancing competition

Annex B – Draft Requirements

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

1. Background

The NATO Communications and Information Agency (NCIA) requires an Integrated Event Operations (IEO) Platform in support of the Education, Training, Exercises and Evaluations (ETEE) Functional Services (FS) capability. The IEO Platform is intended to support NATO entities in the end-to-end event lifecycle for ETEE-related activities (e.g., create, plan, coordinate, approve, publish, execute and close events), and to enable controlled data exchange with other relevant services and applications. The capability is expected to be deployable and operable within NATO secured networks and supported as an NCIA-managed service.

2. Scope

The Contractor shall provide an Integrated Event Operations (IEO) solution including (but not limited to), the following high-level scope elements:

a. **End-to-end event lifecycle**. Support the end-to-end event lifecycle for NATO ETEE activities (e.g., create, plan, coordinate, approve, publish, execute and close events)

b. **Core capability areas.** Provide capabilities covering
   - Event registration / participant management workflows;
   - Event-related resource management (e.g., rooms/venues, IT resources, catering, accommodation, transportation), including request/approval/allocation tracking and change handling.

c. **Multi-entity use.** Support use by multiple entities/communities, with adaptability/configuration to different processes (e.g., workflows, roles, forms/fields) and appropriate segregation options.

d. **Integration and data exchange**. Be able to receive information from other applications (e.g., lists of events or event-related data) and provide information to other applications (e.g., IT Service Management (ITSM) systems) in a transparent, controlled, and documented manner, using standard integration and data exchange mechanisms (e.g., APIs and/or other standard methods).

e. **Deployment constraints.** Be deployable and operable **on-premises** within NATO secured networks. SaaS-only solutions are not acceptable. The Contractor shall identify any external/cloud dependencies (e.g., licence validation, telemetry, support portals, update repositories, map services, email/SMS services) and whether these can be disabled or replaced with on-premises components

f. **Multi-network deployment (high level).** The solution may be deployed in more than one NATO network/security domain. The Contractor shall describe any constraints and the options available for controlled and policy-compliant data transfer/replication between domains (e.g., via approved cross-domain mechanisms), subject to NATO security policy.

g. **Scale.** Support large-scale events (up to approximately **15,000 users**) as well as small events with only a few participants.

h. **Adjacent processes (as applicable).** Where required, indicate whether the solution can support event-adjacent processes such as **Real Life Support (RLS) planning/coordination** and **IT provisioning** natively and/or via integration with external systems.

3. Objectives

The objectives of the IEO Platform are to:

a. Provide a coherent and scalable capability to support event operations for NATO ETEE activities;
b. Reduce fragmentation across multiple tools used today by different communities;
c. Enable controlled data exchange and integration to reduce manual work and duplication;
d. Meet NATO constraints for secure on-premises deployment and support accreditation/security assurance activities; and
e. Enable practical operations and maintenance as an NCIA-managed service.

4. Performance Requirements

The Contractor shall meet the following high-level performance requirements (*to be refined in later stages*):

a. **Availability and scalability.** The solution shall support the anticipated user scale and event workload. *[Respondents shall indicate typical sizing drivers and any known limits (e.g., concurrent users, number of events, environments)]*;
b. **Cybersecurity / security-by-design and assurance support**. The solution shall be engineered and maintained following security-by-design practices. The Contractor shall:
   - Provide NATO UNCLASSIFIED evidence of secure development lifecycle and vulnerability management practices;
   - Support NCIA security assurance activities, including cooperation during NCIA security testing (including penetration testing);
   - Commit to remediation of Critical/High findings within agreed timeframes as part of acceptance and throughout operations.
c. **Auditability.** The solution shall support role-based access control and audit logging suitable for enterprise use.
d. **Integration robustness.** Integration mechanisms (e.g., APIs) shall be documented and support reliable exchange of agreed data objects. *[Respondents shall describe API documentation and versioning approaches].*
e. **Support model (O&M).** The Contractor shall provide support for on-premises deployments, including:
   - Support coverage hours (e.g., 8x5 and/or 24x7 options);
   - Response targets and escalation processes by severity;
   - Security patch/hotfix process and typical release cadence;
   - Clear roles/responsibilities (L1/L2/L3; supplier/partner) aligned with NCIA service delivery governance.
f. **User interface / usability.** The solution shall provide a usable interface for key roles (event planner/coordinator, participant, support staff). *[Respondents shall provide evidence/examples (e.g., screenshots or UI guide excerpts) and indicate accessibility and localisation support where applicable]*

Table 6 - High-level requirements checklist

Requirements ID	Description	MoSCoW Priority
IEO_REQ_01	Deployable and operable fully on-premises within NATO secured networks (no SaaS-only dependency)	Must
IEO_REQ_02	Supports end-to-end event lifecycle management (create, plan, coordinate, approve, publish, execute, close)	Must

IEO_REQ_03	Supports configurable event registration / participant management workflows	Must
IEO_REQ_04	Supports multi-entity/communities usage with configurable workflows/forms/fields/roles per entity	Must
IEO_REQ_05	Supports event-related resource management (e.g., rooms/venues, IT, catering, accommodation, transportation)	Must
IEO_REQ_06	Supports request/approval/allocation tracking and change handling for event resources	Must
IEO_REQ_07	Provides integration and data exchange mechanisms (e.g., APIs and/or other standard methods	Must
IEO_REQ_08	Supports role-based access control and audit logging suitable for enterprise use.	Must
IEO_REQ_09	Scales to support large communities/events (up to ~15,000 users) and also small events	Must
IEO_REQ_10	Indicate support for multi-network deployment (separate instances), including operation in an effectively air-gapped network, and controlled, policy-compliant data transfer/replication between domains (where permitted), including support for one-way transfer mechanisms (e.g., data diodes)	Must
IEO_REQ_11	Indicate support for adjacent processes (e.g., RLS planning/coordination, IT provisioning) natively and/or via integration	Must
IEO_REQ_12	Cybersecurity / security-by-design: supplier provides NATO UNCLASSIFIED evidence of existing security assurance practices (including penetration testing evidence/attestation), vulnerability management and disclosure processes, and commits to remediation of findings from NCIA security testing (including penetration testing)	Must
IEO_REQ_13	Can receive information from other applications and provide information to other applications (e.g., ITSM) in a controlled and documented manner	Must
IEO_REQ_14	Minimises life cycle costs and supports practical O&M (support model, patching/upgrades for on-prem.)	Should

5. Deliverables

[Respondents are invited to comment on the indicative deliverables below and propose additions/removals that better reflect typical delivery and sustainment of an on-prem enterprise application/service in a secured environment].

Deliverable	Description	Frequency	Format
D1: Solution design overview	High-level solution architecture and deployment view (components, environments, dependencies, sizing drivers).	Once	Document (PDF/Word)
D2: On-prem deployment package	Installation/deployment instructions, prerequisites, configuration, and upgrade procedure (incl. air-gapped considerations where applicable)	Once + updates	Document
D3: Security package	Secure configuration/hardening guide, security operational guidance, and the security evidence set requested in Annex A.	Once + updates	Document set / references
D4: Integration & API package	API/interface documentation, supported integration methods, versioning approach, and data exchange patterns supported.	Once + updates	Document / API spec
D5: Service operations & support package	Runbooks/admin guide, monitoring/logging approach, backup/restore, and support model (SLAs/response targets, escalation, patch/hotfix process, release cadence).	Once + updates	Document set
D6: Acceptance & transition support	Support to testing, troubleshooting and remediation during acceptance and during NCIA security testing (incl. penetration testing).	As required	Services
D7: Training	Training materials (admin/user	Once +	Slides /

materials *(optional)*	quick guides) and knowledge transfer sessions.	updates	guides

6. Purchaser Furnished Equipment (PFE) / Information (PFI)

NCIA expects to provide, as applicable:

- **a.** Target on-prem hosting environment within NATO secured networks (infrastructure/platform services as available).
- **b.** Network connectivity and access to relevant security domains, where permitted.
- **c.** Identity/IAM integration endpoints and guidance (as applicable).
- **d.** ITSM integration endpoints/guidance (as applicable).
- **e.** Representative user roles, test accounts, and test scenarios.
- **f.** Applicable NATO/NCIA policies and standards relevant to security/compliance.
- ***g.*** *[Respondents shall list any additional PFE/PFI assumptions required for their solution].*

7. Period of Performance

- **a.** The system design shall minimise total system life cycle costs, including its future Operations and Maintenance (O&M).
- ***b.*** *[Respondents shall describe typical implementation timelines for an initial on-prem deployment and initial operational readiness (ROM), including key prerequisites and assumptions].*
- **c.** *[Respondents shall describe the proposed on-prem support duration options (e.g., 1-year base + option years) and typical patch/upgrade cadence].*

8. Place of Performance

- **a.** Place of performance is expected to include NCIA/NATO sites for on-prem deployment and operation within NATO secured networks.
- **b.** Supplier off-site/remote support may be permitted if compliant with NATO security policies and specific contract terms.