NCIA/ACQ/2025/06531
14 February 2025

REQUEST FOR INFORMATION
Stage 1

PROJECT "IPTV Overhaul"

NCI Agency Reference: RFI-06531 Stage 1

NCI The Agency is requesting information from Nations and their qualified vendors regarding potential solutions to replace the outdated IPTV system with a modern, state-of-the-art alternative and digital signage capacities designed to operate on SHAPE NATO RESTRICTED local area network.

NCI Agency Point of Contact

Senior Contracting Assistant:

Esteban Diaz E-mail:

Esteban.Diaz@ncia.nato.int

To : Distribution List (Annex A)

Subject : **NCI Agency Request for Information SHAPE Radio Overhaul**

1. NCI Agency requests the assistance of the Nations and their Industry to identify a commercially available solution that can meet or exceed NATO requirements for ensuring enhanced IPTV and digital signage capabilities on SHAPE NATO RESTRICTED local area network.
2. A summary of the requirements is set forth in the Annex B attached hereto. Respondents are requested to reply to the required information at Annex C. Other supporting information and documentation (technical data sheets, descriptions of existing installations, etc.) are also desired.
3. The NCI Agency reference for this Request for Information is **RFI-06531 Stage 1** and all correspondence and submissions concerning this matter should reference this number.
4. Respondents are requested to sign a NDU (Attachment D) to be considered eligible for RFI Stage 2. RFI Stage 2 will include the full technical details for this RFI to the eligible respondents.
5. Respondents are invited to carefully review the requirements in Annex B.

6. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a NATO UNCLASSIFIED description of the capability available and its functionalities. This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by NCI Agency.

7. Non-binding pricing information is also requested as called out in Annex C. A response to the pricing information questions (Annex C, point 4: Cost and pricing information; Q4.1 to Q4.3) is not expected for RFI Stage 1. This information is expected for RFI Stage 2.

8. Responses for RFI Stage 1, including the signed NDU, are due back to NCI Agency no later than **12:00 Brussels time on 14 March 2025**.

9. Clarification requests for RFI Stage 1 can be submitted no later than 15 calendar days prior the Request for Information closing date.

10. Please send all responses via email to the following NCI Agency Point of Contact:

    For the attention of: Mr Esteban Diaz at Esteban.Diaz@ncia.nato.int

11. Expected release date for RFI Stage 2 is **21 March 2025**. Response time for RFI Stage 2 will be approximately 30 calendar days.

12. NCI Agency reserves the right to request for a service demonstration to selected suppliers. However, the NCI Agency may seek additional clarification from respondents.

13. Respondents are requested to await further instructions after their submissions and are requested **not to contact directly any NCI Agency staff other than the POC identified above in Paragraph 8**.

14. Any response to this request shall be provided on a voluntary basis. Not responding will not prejudice or cause the exclusion of companies from any future procurement that may arise from this Request for Information.

15. Responses to this Request for Information, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as information only and will not be construed as binding on NATO for any future acquisition.

16. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this Request for Information and this shall not be regarded as a commitment of any kind concerning future procurement of the items described.

17. Your assistance in this Request for Information is greatly appreciated.

FOR THE CHIEF OF ACQUISITION

Esteban Diaz
Senior Contracting Assistant

Esteban Diaz
Digitally signed by Esteban Diaz
Date: 2025.02.13 15:53:16 +01'00'

Enclosures:

Annex A (Distribution List)
Annex B (Request for Information – Scope and Requirements)
Annex C (Request for Information – Information requested)
Non-Disclosure Undertaking

ANNEX A

Distribution List for Request for Information
RFI-06531 Stage 1

All NATO Delegations (Attn: Investment Adviser)

NATO Members Embassies in Brussels (Attn: Commercial

Attaché) NCI Agency – All NATEXs

NCI Agency – (reserved)

ANNEX B

Scope and Requirements

1 Information:

1.1 Purpose of the RFI: this RFI aims to gather insights from qualified vendors about solutions to replace SHAPE outdated IPTV system with a modern, state-of-the-art alternative. The proposed solution should include digital signage capabilities and be designed to operate on SHAPE NATO RESTRICTED local area network.

1.2 Scope of the RFI: Vendors are invited to share insights on technical feasibility, especially on cyber security compliance of the new system with installation on a NATO RESTRICTED Local Area Network (LAN).

2 Project :

2.1 The scope of the "IPTV Overhaul" Project is to support the award of a ten-years contract consisting of ten one-year tranches.

2.2 The first tranche is allocated to the project phase, which involves replacing the existing obsolete IPTV solution on the SHAPE campus with a state-of-the-art solution and digital signage capacities all to be accredited in keeping with NATO security directives. This phase also includes all maintenance activities until the end of the year, comprising the hand-over to the contractor of the associated satellite dishes.

2.3 The subsequent tranches are dedicated to maintaining the new IPTV solution and its digital signage capabilities.

3 Procurement Approach:

3.1 NCIA evaluates two possible approaches for the implementation and operation of the new IPTV/digital signage service/capability:

1. NATO Owned – Contractor Operated (NOCO):

   Under this approach, NCIA will own the equipment while the supplier provides operational and maintenance services.

   The supplier must provide a cost estimate Rough Order of Magnitude (ROM) for:

   - Initial investment: including the supply of the new IPTV solution and its associated digital capabilities, and initial training for users and operators
   - The accreditation/certification of the new IPTV solution and its associated digital capabilities to run on SHAPE NATO RESTRICTED LAN

- Operation & Maintenance (O&M): covering services on-site support with required response times (restore target: 2 working days – P3), routine maintenance, updates, and periodic security testing.

2. Contractor Owned – Contractor Operated (COCO):

   Under this approach, the supplier retains ownership of all equipment and provides the required services under a comprehensive yearly fee. The supplier must provide a ROM for the yearly fee.

   The yearly fee must include:

   - The installation of the new IPTV solution and the associated digital signage capabilities
   - The accreditation/certification of the service to run on SHAPE NATO RESTRICTED LAN
   - The supply and maintenance of provisions for the service.
   - The hand-over to the contractor of the associated satellite dishes.
   - Comprehensive O&M services as detailed above, including technical support and training.

3.2 Both approaches will be evaluated based on their overall cost-effectiveness, scalability, and alignment with the project's operational and strategic objectives. Vendors are encouraged to outline the benefits and risks associated with each approach and to provide detailed cost breakdowns for comparison.

4 Existing IPTV system overview

INFORMATION TO BE RELEASED TO ELIGIBLE RESPONDENTS AT STAGE 2, AFTER SIGNATURE OF THE NON-DISCLOSURE UNDERTAKING (NDU)

5 Technical Requirements:

5.1 IPTV focus:

The objective is to acquire and deploy a market-ready IPTV solution that integrates seamlessly with satellite dishes and the SHAPE NATO RESTRICTED LAN. The solution shall support high-quality IPTV services, scalable to at least 500 users, and provide additional digital signage capabilities with controlled content management.

The new system, initially planned for installation

INFORMATION TO BE RELEASED TO ELIGIBLE RESPONDENTS AT STAGE 2, AFTER SIGNATURE OF THE NON-DISCLOSURE UNDERTAKING (NDU)

on the SHAPE campus, will need to be relocated to another building later to accommodate real-estate transformations on the campus.

5.1.1 System requirements:

5.1.1.1 Integration with Satellite Dishes:

- Support for receiving and decoding signals from satellite dishes.
- Compatibility with standard satellite receivers and LNBs (Low-Noise Block downconverters).
- Integration of required equipment such as multi switches or amplifiers to support simultaneous channel processing.

5.1.1.2 IPTV Content Delivery:

- Encoding and streaming of satellite TV channels into an IPTV-ready format.
- Support for multicast and unicast streaming protocols.
- Adaptive bitrate streaming for consistent quality across devices and varying network conditions.

5.1.1.3 Middleware Platform:

- A centralized IPTV management system (middleware) to manage channel line-ups, user access, and service configuration.
- Integration with Electronic Program Guide (EPG) data for easy user navigation.
- Tools to manage user authentication and access rights.

5.1.1.4 End-User Devices and Accessibility:

- IPTV solution shall support access for:
- A minimum of 500 users on workstations, laptops, or tablets via web or app interfaces.
- 70 standalone televisions with compatible set-top boxes or embedded IPTV functionality.
- Applications and interfaces for mobile devices, smart TVs, and desktops.

5.1.1.5 Digital Signage Capabilities:

- The solution shall include digital signage functionalities, allowing content creation and broadcasting.
- Controlled delegation of access rights for digital content management to at least ten (10) different content managers in a secure and managed way.

5.1.2 Infrastructure and Environment Requirements:

5.1.2.1 Customer-Provided Resources:

- The IPTV solution shall be connected to SHAPE local private network via 1 Gbit/s optical network access, provided by the customer.
- One electrical plug shall be provided by the customer (characteristics and power to be defined during implementation).
- The system shall be installed in an office-type environment with controlled temperature.

5.1.2.2 Contractor Responsibilities:

- The contractor shall provide a technical cabinet to host all IPTV solution components.
- Provision and Installation of UPS systems capable of automatically shutting down servers safely in the event of a power outage lasting more than five minutes.
- Ensure that the IPTV solution is housed in the technical cabinet, with adequate provisions for cooling and cable management.

5.1.3 Scalability and Network Integration:

- The system shall scale to accommodate additional users, televisions, or channels as needed.
- Integration with the customer's existing LAN infrastructure, supporting VLANs and QoS for optimized IPTV traffic.

5.1.4 Monitoring, Analytics, and Security:

- Real-time monitoring of IPTV streams, with alerts for performance issues or disruptions.
- Basic analytics to track content usage, system health, and user engagement.
- Compliance with copyright and licensing regulations for distributed content.

5.1.5 Implementation and Training:

- The contractor shall handle the setup, configuration, and testing of the entire IPTV solution including network integration and satellite dish alignment.
- Training and documentation shall be provided to system administrators and content managers.
- The contractor shall ensure that the system is operational and meets all requirements before handover.

5.1.6 Deliverables:

- Fully functional IPTV system connected to existing satellite dishes and the customer's private network.
- Middleware platform for channel and content management.
- Digital signage capabilities with multi-user access rights.
- UPS systems for safe power management.
- Technical cabinet for hosting IPTV and Digital signage components.

- User manuals, network diagrams, and training materials for IPTV system and associated Digital signage system.
- Technical support and maintenance plan for IPTV and Digital signage systems.

5.1.7 Miscellaneous:

The current IPTV solution is permanently connected to three satellites that will be hand-over to the contractor for maintenance as part of the contract:

INFORMATION TO BE RELEASED AT STAGE 2, AFTER SIGNATURE OF THE NON-DISCLOSURE UNDERTAKING (NDU)

The new IPTV solution shall offer a minimum capacity of 20 channels.

The following 10 channels shall have to be available:

INFORMATION TO BE RELEASED AT STAGE 2, AFTER SIGNATURE OF THE NON-DISCLOSURE UNDERTAKING (NDU)

The Subscription fees for television channels are to be included in the contract. The addition or the removal of a channel will be managed through a customer's change request.

5.2 Digital Signage focus:

The aim is to procure and implement a readily available, market-proven digital signage system that meets the SHAPE's essential communication needs without requiring extensive customization. The selected solution shall demonstrate reliability, ease of use, and alignment with modern standards for digital signage technology.

5.2.1 System Requirements:

The digital signage solution shall meet the following baseline capabilities:

5.2.1.1 Content Management and Delivery:

- A centralized Content Management System (CMS) to create, upload, schedule, and manage multimedia content.
- Support for multiple file types, including images, videos, text, and live web feeds.

5.2.1.2 Display and Hardware Support:

- Compatibility with standard commercial-grade digital screens (e.g., LCD/LED) of various sizes.
- Integration with off-the-shelf media players or systems embedded in display hardware.

5.2.1.3 Remote Management:

- Tools to remotely monitor, manage, and update screens across multiple locations.
- on-premises to suit operational needs.

5.2.1.4 Content Scheduling:

- Ability to schedule content for specific times, dates, and locations.

- Support for playlist creation and automated rotation of multiple content items.

5.2.1.5 Multi-Zone Capabilities:

- Enable screens to display multiple types of content simultaneously (e.g., videos, text tickers, clock).

5.2.1.6 Real-Time Updates:

- Support for live updates to content in response to events or changing circumstances (e.g., alerts or news feeds).

5.2.1.7 User-Friendly Interface:

- Intuitive administrative dashboard accessible via web browser.
- Role-based access to allow secure content management by authorized personnel only.

5.2.1.8 Integration and Scalability:

- Compatibility with third-party tools and APIs for future integration.
- Easily scalable to manage additional screens and locations as needed.

5.2.1.9 Basic Analytics and Reporting:

- Logging capabilities to track content usage and screen uptime.
- Reports on system performance and engagement metrics.

5.2.2 Implementation and Adoption Approach:

Adoption Strategy: Preference shall be given to established, market-ready solutions requiring minimal customization and offering flexibility for implementation within the SHAPE's existing infrastructure.

5.3 Security requirements / Accreditation:

5.3.1 Information Classification:

The IPTV solution shall host various levels of sensitive information that need to be viewed and processed by the Contractor.

- The maximum classification and ownership level of the information that can be processed by the Solution is NATO RESTRICTED.
- It is of utmost importance that the integrity and availability of the information is ensured at all times.
- While integrating with the Purchaser's CIS or CIS provided by 3rd party contractors, the Contractor might have to process NATO SECRET information.

5.3.1.1 (SHALL) The data in the future IPTV Solution shall be protected up to NATO RESTRICTED.

5.3.1.2 (SHALL) The Contractor shall be aware of sensitivity and ownership of the data being processed and shall adhere to the applicable Security Requirements of the data according to the policies (ref. Table 1)

INFORMATION TO BE RELEASED AT STAGE 2, AFTER SIGNATURE OF THE NON-DISCLOSURE UNDERTAKING (NDU)

5.3.2 Security Accreditation Requirements:

The SAA for the Solution is the SHAPE J2.6. Coordination with the SAA will be conducted by the customer.

5.3.2.1 (SHALL) The Solution shall achieve Security Accreditation (SA), in order to demonstrate compliance with the NATO relevant Security Policy, supporting directives and system-specific documentation (e.g., System Security Requirement Statements (SSRS) and to be granted authority to go live.

5.3.2.2 (SHALL) To receive a SA statement from the SAA, the Contractor shall develop an ADS (ref. § 3) and obtain SAA approval for the individual documents. The Contractor should expect a number of review rounds per document before it will be approved by the SAA.

5.3.2.3 (SHALL) The Contractor shall produce a Security Test and Verification Plan (STVP), execute security testing witnessed by the Purchaser and formally documented in a Security Test and Verification Report (STVR) as part of the ADS.

5.3.2.4 (SHALL) The Contractor shall support security audits executed by the Customer, including but not limited to:

- Security Testing and Verification
- Type 3 Security Audits (i.e. validation tests)
- Type 4 Security Audits (i.e. pen-testing)

5.3.2.5 (SHALL) Type 3 and Type 4 Security Audits are conducted by the NATO Cyber Security Center (NCSC) …

INFORMATION TO BE RELEASED TO ELIGIBLE RESPONDENTS AT STAGE 2, AFTER SIGNATURE OF NON-DISCLOSURE UNDERTAKING (NDU)

5.3.2.1 (SHALL) Where the remediation of audit findings results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components, the Contractor shall consider these changes to be within the technical and financial scope of this Contract, and at no additional cost for the customer. Where the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, a request for change shall be raised by the Contractor for the Customer's

decision.

5.3.2.2 (SHALL) The Contractor shall take action to follow, carry out the necessary work, and to implement the advice, instructions and changes required to remediate findings resulting from security testing and security audit(s).

5.3.2.3 (SHALL) The Contractor shall take action to follow, carry out the necessary work, and to implement the advice, instructions and changes required by the SAA.

5.3.2.4 (SHALL) The Contractor shall designate Security Subject Matter Experts (SME) as points of contact for SA and security-related issues.

5.3.2.5 The Contractor may need to request Approval for Pilot (AfP) before the interim Security Accreditation (iSA) can be requested to the SAA. The AfP will have to be agreed by the Customer with the SAA, in order to define to what extent the Solution may be operated during a period of time ad until iSA is requested and granted.

5.3.3 Security Accreditation Documentation Set (ADS):

The achievement of the IPTV Solution SA will require a prescribed set of security documentation to be produced based on SA documentation templates. The templates will be made available to the Contractor after Contract Award.

5.3.3.1 (SHALL) The Contractor shall produce SA documentation and provide inputs to documents in support of the Solution SA.

5.3.3.2 (SHALL) The Contractor shall identify and document any Commercial of the Shelf (COTS) products included in the system in the security documentation.

5.3.3.3 The documentation to be developed to support the Solution SA process is listed in the table; which also summarizes responsibilities related to the development of each document Column “Baseline/Guidance” lists available templates, relevant NATO Security Directives and Guidance, and similar documentation existing NATO CIS which can be used as an example or initial input. All Security Accreditation documents will be subject to Customer and SAA approval.

INFORMATION TO BE RELEASED TO ELIGIBLE RESPONDENTS AT STAGE 2, AFTER SIGNATURE OF NON-DISCLOSURE UNDERTAKING (NDU)

5.3.4 Security Accreditation Plan (SAP):

5.3.4.1 (SHALL) A Security Accreditation Plan for the Solution shall be developed by the Purchaser.

5.3.4.2 (SHALL) The SAP shall describe the steps to be taken to achieve SA of the Solution.

5.3.4.3 (SHALL) The Contractor shall strictly adhere to the SA activities described in the SAP as approved by the SAA. All activities related with the SA process shall be identified in the project management plan maintained by the contractor and correlated with the overall system design and implementation.

5.3.5 CIS Description (CISD):

5.3.5.1 (SHALL) A CISD for the Solution shall be developed by the Contractor. A template will be provided by the Customer.

5.3.5.2 (SHALL) The CISD shall be formulated by the Contractor at the earliest stage of the project. The Contractor shall maintain the CISD during the project, including all relevant information taken from the SDS as required to understand the content of the CISD document. CISD shall be standalone document and shall not refer to any document from SDS.

5.3.5.3 (SHALL) The Contractor shall take into account any comments from the Customer and SAA and shall update the CISD document as many times as necessary in order to obtain SAA approval.

5.3.6 Security Risk Assessments (SRA):

5.3.6.1 (SHALL) The Contractor shall support the development of the SRA, including risks related to modern CIS technologies and the Solution specific risks. The SRA shall be conducted in accordance with AC/35-D/1017.

5.3.6.2 (SHALL) The Contractor shall consider any change to be within the technical and financial scope of this Contract whenever the implementation of security measures results in the modification of the design, other documentation requirements, and changes to the Solution; no changes to the Contract shall be generated.

5.3.6.3 (SHALL) The Contractor shall take into account any comments from the Customer and SAA and shall update the SRA as many times as necessary in order to obtain SAA approval.

5.3.7 System-specific Security Requirements Statement (SSRS):

A SSRS will be developed, as directed by the SAA, defining the security requirements for the Solution.

5.3.7.1 (SHALL) The Contractor shall support the development of the SSRS to include the minimum levels of security deemed necessary.

5.3.7.2 (SHALL) The SSRS shall be formulated at the earliest stage of the project and shall be further developed and enhanced and updated as the project develops.

5.3.7.3 (SHALL) The Contractor shall take into account any comments from the Customer and SAA and SHALL update the SSRS as many times as necessary in order to obtain SAA approval.

5.3.8 Security Test and Verification Plan (STVP):

The STVP provides a plan of all security tests. The STVP shall be generated by the Customer with support provided by Contractor.

5.3.8.1 (SHALL) The Contractor shall support the development of STVP, using the STVP template provided by the Purchaser.

5.3.8.2 (SHALL) The Contractor shall ensure all security mechanisms are planned for testing.

5.3.8.3 (SHALL) The Contractor shall take into account any comments from the Purchaser and SAA and shall update the STVP as many times as necessary in order to obtain SAA approval.

5.3.8.4 The Security Test and Verification Report (STVR) provides results of all security tests specified in the STVP.

5.3.8.5 (SHALL) The Contractor shall execute the SAA approved STVP under the supervision of the Customer.

5.3.8.6 (SHALL) The Contractor shall produce and deliver a STVR, containing results of all security tests specified in the STVP, using the template provided by the Purchaser.

5.3.8.7 (SHALL) The Contractor shall ensure security test identifiers are preserved in the Report as defined in the STVP.

5.3.9 Security Operating Procedures (SecOPs):

SecOPs will be developed for the Solution. The SecOPs are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel.

5.3.9.1 (SHALL) The Contractor shall deliver the Solution SecOPs using the template provided by the Purchaser.

5.3.9.2 (SHALL) SecOPs shall also cover all security requirements identified in the SRA and SSRS which are not fully fulfilled by technical countermeasures. For example, following security procedures should be addressed (not exhaustive list):

- System configuration and maintenance;
- System backup;

- System recovery, etc.

5.3.9.3 (SHALL) The Contractor shall take into account any comments from the Customer and SAA and shall update the SecOPs as many times as necessary in order to obtain SAA approval.

5.3.10 Security Documentation Review:

5.3.10.1 All documents for SA shall be subject to Customer and SAA review and approval. The Contractor should expect a number of review rounds per document before it will be approved by the SAA.

5.3.10.2 (SHALL) The Contractor shall produce Security Documentation under the close supervision and guidance of Customer's specialists.

5.3.10.3 (SHALL) The Contractor shall submit Security Documentation to the Customer for review before submission to SAA for approval.

5.3.10.4 (SHALL) The Contractor shall take into account any comments from the Customer and SAA and shall update the ADS as many times as necessary in order to obtain SAA approval.

5.3.10.5 The Security Mechanisms to be implemented by the Solution will be based on:

INFORMATION TO BE RELEASED TO ELIGIBLE RESPONDENTS AT STAGE 2, AFTER SIGNATURE OF NON-DISCLOSURE UNDERTAKING (NDU)

5.3.10.6 (SHALL) The Contractor shall address SRA-recommended changes in security mechanisms in the design.

5.3.10.7 (SHALL) The Contractor, in the Solution design, shall include implementation of the Security Mechanisms and provide full traceability of high level security measures requirements down to the implementation level.

5.3.10.8 (SHALL) The Contractor shall maintain an end-to-end traceability of the required security measures throughout the project.

5.3.10.9 (SHALL) The Contractor shall include any additional security measures resulting from the follow-on risk assessments as part of the end-to-end traceability.

5.3.10.10 (SHALL) The Contractor shall design the security mechanisms for the Solution to be complementary to not overlap with the NATO wide IA Services capability already provided by other NATO systems.

5.3.10.11 (SHALL) The Contractor shall design the Solution security mechanisms to integrate with the existing NATO wide IA Services capability.

5.3.10.12 (SHALL) The Contractor shall implement the security mechanisms, approved by the Customer after coordination with the SAA, as a part of the Solution design and SA work and shall produce the associated documentation.

ANNEX C

Information requested

Company name:

Contact name & details (phone number and email address):

Please **DO NOT** enter any company marketing or sales material as part of your answers within this Request for Information. But please submit such material as enclosures with the appropriate references within your replies.

Please **DO** try and answer the relevant information requested as comprehensively as possible.
All points within this document should be answered in conjunction with the summary of requirements in Annex B.

Cost details required in the questions refer to Rough Order of Magnitude (ROM) Procurement & Life Cycle cost, including all assumptions the estimate is based.

1. **Technical and Implementation Details:**

   Q 1.1 What is your proposal for an IPTV and digital state of the art solution?

   Q 1.2 Which are your Security accreditation strategies for the solution to be authorised to run on SHAPE NATO RESTRICTED Local Area Network?

   Q 1.3 What is your Transition plan from the old to the new service?

2. **Operations and Maintenance:**

   Q 2.1 What are your Service level agreements (SLAs) for maintenance and incident resolution?

   Q 2.2 What are your Routine testing, updates, and reporting protocols?

3. **Risks and Mitigations:**

   Q 3.1 What are the potential anticipated risks (e.g., technical, or security accreditation) and your proposed mitigation strategies?

4. **Cost and Pricing Information:**

   Vendors are required to provide a ROM (including a ROM breakdown) based on the two procurement approaches outlined in Section 4:

   Q 4.1 For the NOCO Model:

   Q 4.1.1 ROM for the initial investment, covering:

   - Provision of the new IPTV and digital signage capabilities
   - Security accreditation of new IPTV and digital signage capabilities

- Connection of new IPTV and digital signage capabilities to SHAPE NATO RESTRICTED LAN.
- Hand-over to the contractor of existing satellite dishes for maintenance.
- Initial training for users and operators.

Q 4.1.2 Annual ROM for Operation & Maintenance (O&M), including:

- Channels subscription fees.
- 24/7 service desk for incident and change management.
- On-site technical support with specified response times (2 working days).
- Routine maintenance, updates, and periodic security update/testing.

Q 4.2 For the COCO model:

Q 4.2.1 What is the minimum contract duration that will make the COCO approach a suitable approach for your company?

Q 4.2.2 Comprehensive ROM for the yearly fee that encompasses:

- Ownership, supply, and maintenance of the IPTV system and the digital signage capabilities.
- Security accreditation of new IPTV and digital signage capabilities
- Connection of new IPTV and digital signage capabilities to SHAPE NATO RESTRICTED LAN.
- Hand-over to the contractor of existing satellite dishes for maintenance.
- All O&M services detailed in the NOCO approach.

Q 4.3 For both models, the vendor must include:

- A comparison of the projected costs over the system's lifecycle (10 years).
- Clear identification of any optional costs, such as additional IPTV Set-Top Boxes.
- Recommendations for optimizing cost efficiency while maintaining service quality and compliance with the stated requirements.

NATO Communications and Information Agency

Acquisition Office

Boulevard Léopold III
B-1110 Brussels, Belgium

NON-DISCLOSURE UNDERTAKING

NATO Communications and Information Agency, a subsidiary body of the North Atlantic Treaty Organisation (NATO) established pursuant to Article 9 of the North Atlantic Treaty and subject to the 1951 Ottawa Agreement (hereinafter referred to as the "NCI Agency")	[CLICK HERE TO INSERT COMPANY DETAILS, a company incorporated in [NATION], and having its registered office at [ADDRESS] (hereinafter referred to as the "Supplier")
Each a "Party" and together the "Parties".	

In pursuit of the SHAPE IPTV Overhaul Project (hereinafter referred to as the "Purpose"), the NCI Agency wishes to share certain Confidential Information, as defined in Article 1 hereunder, to the Supplier.

The disclosure of any Confidential Information belonging to the NCI Agency, either preceding, during, or in the aftermath of the Purpose, shall be governed by the conditions of confidentiality set out in this Undertaking.

Article 1. Confidential Information

1.1 For the purposes of this Undertaking, "Confidential Information" shall mean any information shared by the NCI Agency, or any information that is not generally available to the public and that is treated as confidential by the NCI Agency, or which the Supplier otherwise obtains as knowledge or as a result of its relationship with, access to premises of, or communication with the NCI Agency's employees or independent contractors, whether in written, oral, graphic, electromagnetic, digital, or any other tangible or intangible form, including information without limitation relating to NCI Agency's organization, business, projects, technology, products, services, marketing, research, activities and/or the existence of the Purpose itself.

1.2 Without being limited thereto, Confidential Information shall include the following tangible and intangible forms of information: concepts, agendas, designs, drawings, presentation slides, ideas, minutes, e-mails, inventions, specifications, techniques, discoveries, models, data, database structures, database schema, metadata, source code, object code, documentation, diagrams, flow charts, videos (including GIFs and other formats), research, development, processes, procedures, know-how, new product or new technology information, training materials, marketing techniques and materials, marketing plans, letters, online messages, verbal conversations, timetables, strategies and development plans (including prospective trade names or trademarks), intellectual property, customer names and any other information related to customers, pricing and pricing policies, and financial information.

1.3 The NCI Agency shall only disclose Confidential Information to the Supplier as necessary for the Purpose.

Article 2. Confidentiality Obligation

2.1 Scope and identification of the Parties:

(a) The NCI Agency shall include divisions, organizations, agencies, and other bodies of the NATO Organization, including NATO HQ, agencies, and military commands in accordance with the NATO's policy framework relating to the need-to-know principle.

(b) The Supplier shall limit the internal dissemination of Confidential Information to the most restricted number of individuals required for the satisfactory execution of the Purpose (need-to-know). Only the following exhaustive list of members of the Supplier shall have access to Confidential Information under the present Undertaking:

#	Name	Title
1		
2		
3		

(c) Every addition to the list at Article 2.1(b) above shall occur on an exceptional basis only, following the prior written approval of an authorized representative of the NCI Agency, in accordance with Article 2.2(a) below.

NATO Communications and Information Agency

Acquisition Office

Boulevard Léopold III
B-1110 Brussels, Belgium

2.2 The Supplier undertakes with respect to all Confidential Information:

(a) to maintain strict confidentiality and to not disclose or reveal to any third party (not mentioned in the list under Article 2.1(b) above), including professional consultants or affiliates of the Supplier, any Confidential Information received hereunder from the NCI Agency without the clear and express prior written consent of a duly authorized representative of the NCI Agency.
For the avoidance of doubt, the Supplier shall only communicate about Confidential Information with the following individuals acting as duly authorized representatives of the NCI Agency for this Undertaking, unless explicitly instructed otherwise in writing by the following individuals:

Esteban Diaz, NCI Agency Senior Contracting Assistant

(b) to solely use the Confidential Information for the Purpose, and not to make any use, directly or indirectly, by act or by omission, of the Confidential Information in a manner inconsistent with the Purpose;

(c) to inform the NCI Agency of the location of any physical representations of Confidential Information in the possession of the Supplier, and to inform the NCI Agency should the location of this Confidential Information change following physical handling;

(d) to not produce tangible or intangible copies or reproductions of any part of the Confidential Information without the prior express written consent of an NCI Agency's representative;

(e) to use the same degree of care and means that it utilizes to protect its own information of a similar nature, but in any event not less than reasonable care and means, technical or other, to ensure the confidentiality of such Confidential Information and avoid a third party to have access to the Confidential Information;

(f) not to alter, modify, disassemble, reverse engineer or decompile any Confidential Information without the clear and express prior written consent of a duly authorized representative of the NCI Agency;

(g) to immediately, upon instructions from the NCI Agency, return or destroy any Confidential Information in tangible or intangible form, together with any copies that may have been made, in accordance with Article 2.2(d):
i) upon completion or abandonment of the Purpose or the activities to which they relate; or
ii) upon termination of the Undertaking or any business or other relationship between the Parties; or
iii) in any event, upon written request of the NCI Agency:

(h) in the event of an actual or suspected breach of confidentiality, not limited to but including any misappropriation or unauthorized disclosure of Confidential Information, to inform the NCI Agency immediately in writing of such breach and of the actions the Supplier has undertaken to remediate the actual or suspected breach;

(i) to remain exclusively responsible for any of its staff, agents or similar personnel's compliance with the terms of this Undertaking.

Article 3. Exceptions to the obligation of confidentiality

3.1 The restrictions on the use or disclosure of Confidential Information set out in Article 2 hereinabove shall not apply to any Confidential Information which:

(a) is or falls within the public domain through no act or omission of the Supplier and as such loses its confidential character; or

(b) is disclosed to the Supplier by a third party who is not in breach of any obligation of confidentiality; or

(c) was known to the Supplier before such Confidential Information was imparted by the NCI Agency as can be evidenced by its records; or

(d) is independently developed by the Supplier without any reference to any Confidential Information.

3.2 In the event the Supplier is required to disclose any Confidential Information relating to the Purpose of this Undertaking, due to any statute, law, rule or regulation of any governmental authority or pursuant to any order of any court of competent jurisdiction, the Supplier shall advise the NCI Agency of the request for disclosure within 14 calendar days to apply for such legal protection as may be available with respect to the confidentiality of the Confidential Information. The Supplier shall not disclose any Confidential Information until a non-appealable decision is granted. The Supplier shall let the NCI Agency interact with any authority, instance, or legally competent requestor.

Article 4. Indemnity and Enforcement

4.1 The Supplier acknowledges that the Confidential Information has been developed or obtained by the investment of significant time, effort and expense, and that this Confidential Information, as well as its confidential nature, is key for the continued well-functioning and critical security of the NCI Agency. The Supplier understands that the NCI Agency will thus suffer substantial and irreparable harm in the event that the Supplier fails to comply with any of its obligations set forth in this Undertaking.

4.2 The Supplier acknowledges that the NCI Agency reserves the right to record instances of any actual breaches of confidentiality by the Supplier, as defined within the terms of this Undertaking, for the purposes of minimising risk and safeguarding Confidential Information. In the extreme circumstance the Supplier is found to have caused repeated or grave breaches of confidentiality, the NCI Agency reserves the right of imposing monetary relief in the form of compensation, for the actual or potential harm caused by the actual breach(es) of confidentiality.

Article 5. Scope of the Undertaking

5.1 This Undertaking shall not be assignable by the Supplier and the NCI Agency may not delegate its duties hereunder, without the clear and express prior written consent of a duly authorized representative of the NCI Agency, which consent may be granted or denied in the sole discretion of the NCI Agency. All of the terms and provisions contained herein shall be binding upon the Supplier and their respective heirs, successors and permitted assigns.

5.2 Nothing in this Undertaking shall be construed as creating any obligation on the part of the NCI Agency to disclose any Confidential Information whatsoever.

5.3 All Confidential Information is, and shall remain, the sole property of the NCI Agency. Nothing in this Undertaking shall be construed as granting the Supplier any license or any other rights with respect to the NCI Agency's Confidential Information or proprietary rights.

5.4 Nothing contained in this Undertaking shall be construed as creating any obligation or an exception on the part of the NCI Agency to enter into a business relationship with the Supplier, or an obligation to refrain from entering into a business relationship with any third party. Nothing contained in the Undertaking shall be construed as creating a joint venture, partnership or employment relationship between the Parties, it being understood that the Parties are independent contractors vis-à-vis one another. Except as specified herein, neither Party shall have any right, power or implied authority to create any obligation or duty express or implied, on behalf of the other Party.

Article 6. General

6.1 This Undertaking shall take effect on its signature date or the first exchange of Confidential Information by the NCI Agency to the Supplier, whichever occurs first, and shall only cease in effect upon the express written consent of an authorized representative of the NCI Agency (regardless of the status of the Purpose). The Supplier agrees that any undertaking given in relation to the Confidential Information shall remain valid after termination of the discussion process relating to the Purpose between Parties.

6.2 This Undertaking sets forth the entire agreement between the Parties with respect to the subject matter hereof and supersedes all other oral or written representations and understandings.

6.3 No provision of this Undertaking shall be amended, modified or waived without the clear and express prior written consent of a duly authorized representative of the NCI Agency.

6.4 If any provision of this Undertaking is held invalid or unenforceable for any reason, this Undertaking shall remain otherwise in full force apart from such provision which shall be deemed deleted, or be amended.

6.5 The fact that the NCI Agency does not demand the strict execution by the Supplier of any provision or condition of the present Undertaking at any time will not be considered as a final waiver of the exercise of this right.

6.6 The Supplier agrees that, without the prior written consent of the NCI Agency, the Supplier will refrain from attributing any Confidential Information to the NCI Agency in any external or internal communication for any purpose, including but not limited to press releases or otherwise to the media, web sites, offering memoranda, and conversations with third parties including professional consultants and affiliates of the Supplier.

NATO Communications and Information Agency NCI AGENCY

Acquisition Office

Boulevard Léopold III
B-1110 Brussels, Belgium

Article 7. Disputes and arbitration

7.1 The Supplier acknowledges that the NCI Agency, as a subsidiary body of the NATO and subject to the 1951 Ottawa Agreement enjoys full immunity from every form of legal process, unless expressly waived by the NATO Secretary General. Similarly, the NCI Agency staff is immune from legal process with respect to words spoken or written, and of acts conducted within their official capacity and limits of their authority.

7.2 All disputes arising under, or which are related to this Undertaking or with respect to its effectiveness, shall be resolved by consultation between the Parties. If no agreement can be found, either Party may open arbitration proceedings in accordance with the following arbitration provisions.

7.3 The Party instituting the arbitration proceedings shall advise the other party by registered letter, with official notice of delivery, of their desire to have recourse to arbitration. Within a period of thirty (30) days from the date of receipt of this letter, the Parties shall jointly appoint an arbitrator. In the event of failing to appoint an arbitrator, the dispute or disputes shall be submitted to an Arbitration Tribunal consisting of three arbitrators, one being appointed by the NCI Agency, another by the Supplier and the third, who shall act as President of the Tribunal, by these two arbitrators. Should one of the Parties fail to appoint an arbitrator during the fifteen (15) days following the expiration of the said first period, the appointment shall be made, within twenty-one (21) days, at the request of the party instituting the proceedings, by the Secretary General of the Permanent Court of Arbitration at The Hague.

7.4 Regardless of the procedure concerning the appointment of this Arbitration Tribunal, the third arbitrator will have to be of a nationality different from the nationality of the other two members of the Tribunal. Any arbitrator must be of the nationality of any one of the member states of the NATO and shall be bound by the rules of security in force within NATO.

7.5 Any individual appearing before the Arbitration Tribunal in the capacity of an expert witness shall, if they are of the nationality of one of the member states of the NATO, be bound by the rules of security in force within NATO; if they are of another nationality, no NATO classified documents or information shall be communicated to them.

7.6 An arbitrator, who, for any reason whatsoever, ceases to act as an arbitrator, shall be replaced under the procedure laid down in Article 7.3 above.

7.7 The Arbitration Tribunal will take its decisions by a majority vote. It shall decide where it will meet and, unless it decides otherwise, shall follow the arbitration procedures of the International Chamber of Commerce in force at the date of signature of the present Undertaking. The awards of the arbitrator or of the Arbitration Tribunal shall be final and there shall be no right of appeal or recourse of any kind. These awards shall determine the appointment of the arbitration expenses

7.8 Pending final decision of a dispute, the Supplier shall proceed diligently with the performance of the Purpose, unless otherwise instructed by the NCI Agency.

Article 8. Representation

8.1 The Supplier warrants and represents that it has carefully read and understood this Undertaking, and acknowledges receipt of a copy thereof. The individual executing this Undertaking warrants and represents that they have the authority to enter into this Undertaking on behalf of the individual, firm or corporation, of any, listed below their name.

IN WITNESS WHEREOF, the duly authorized representative of the Supplier has executed this Undertaking electronically, each Party retaining a copy of the signed document.

For the Supplier

Name:

Title:

Date:

Signature: