# Headquarters Supreme Allied Commander Transformation Norfolk Virginia

# RFI-ACT-SACT-24-44

## NATO INFORMATION TECHNOLOGY MODERNISATION INCREMENT 3 OPERATIONAL NETWORK EXTENSION (NATO ITM INC 3 ON-X)

This document contains a Request for Information (RFI) Call for Nations and Industry input to NATO's Information Technology Modernization (ITM) Capability.

Suppliers wishing to respond to this RFI should read this document carefully and follow the guidance for responding.

This RFI is open to Nations, and Industry located in NATO Nations.

| **HQ Supreme Allied Commander Transformation RFI 24-44**<br>**General Information** | |
|---|---|
| Request For Information No. | RFI-ACT-SACT-24-44 |
| Project Title | Request for Nations and industry input to NATO's Information Technology Modernization (ITM) Capability. |
| Due date for submission of requested information | 14 June 2024 at 0900 EDT |
| Due date for questions | No later than 0900 on 24 May 2024 |
| Contracting Office Address | NATO, HQ Supreme Allied Commander Transformation (SACT)<br>Purchasing & Contracting Suite 100<br>7857 Blandy Rd, Norfolk, VA, 23511-2490 |
| Contracting Points of Contact | 1. Ms Tonya Bonilla<br>e-mail: tonya.bonilla@act.nato.int<br>Tel: +1 757 747 3575<br>2. Ms Catherine Giglio<br>e-mail: catherine.giglio@act.nato.int<br>Tel:+1 757 747 3856<br>3. Mr. Robert McMaster<br>e-mail: robert.mcmaster@act.nato.int<br>Tel:+1 757 747 3869 |
| Technical Points of Contact | 1. Dr Arnau Pons<br>e-mail: arnau.pons@act.nato.int<br>Tel: +1 757 747 3876<br>2. LTC Pedro Sanabria<br>e-mail: pedro.sanabria@act.nato.int<br>Tel: +1 757 747 3543<br>3. Ernest Bartley<br>email: ernest.bartley@act.nato.int<br>Tel: +1 757 747 3367<br>4. Dr. Renee Baggott<br>email: renee.baggott@act.nato.int<br>Tel: +1 757 747 3257 |
| **All request for clarifications, questions and responses to this RFI must be sent via email to all Points of Contact reported above. Individually addressed emails will not be accepted and should not be sent. Contracting and Technical POCs must be included in all correspondence. Check the RFI website often for updates and information https://www.act.nato.int/opportunities/contracting/rfi-act-sact-24-44/** | |

## 1. INTRODUCTION

1.1 Summary. Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with Nations, and industry. The intention is to establish the art-of-the-possible and state-of-the-art with respect to technologies and products in the area of networks and data management in order to support NATO Governance decision-making on a Common-Funded Capability Development for the future - the NATO Information Technology Modernization (ITM).

1.2 This request for information does not constitute a commitment to issue a future request for proposal (RFP). The purpose of this request is to involve Nations, and industry through collaboration, in an examination of future capabilities related to ITM with a focus on IT technologies and commercial products. HQ SACT has not made a commitment to procure any of the items described herein, and release of this RFI shall not be construed as such a commitment, nor as authorisation to incur cost for which reimbursement will be required or sought. Furthermore, respondents are advised that HQ SACT will not pay for any information or administrative costs incurred in responding to this RFI. The costs for responding to this RFI shall be borne solely by the responding party. Not responding to this RFI does not preclude participation in any subsequent RFP if issued in the future.

1.3 **This in an RFI ONLY. This RFI DOES NOT constitute a current Request for Proposal (RFP) nor a commitment to issue a future RFP.** HQ SACT is not seeking proposals at this time; therefore, HQ SACT will not accept unsolicited proposals in respect to this RFI.

## 2. GENERAL BACKGROUND: ACT FRAMEWORK FOR COLLABORATIVE INTERACTION (FFCI)

2.1 HQ SACT has implemented a Framework for Collaborative Interaction (FFCI) to increase opportunities for industry to contribute to HQ SACT's capability development efforts through collaborative work. Such collaboration enables HQ SACT, and NATO as a whole, to benefit from industry models, advice, capabilities and experience in the course of this work. In addition to the benefits, HQ SACT gains from such projects, this collaborative effort will provide Nations and Industry with an improved understanding of NATO's capability requirements and the associated issues and development challenges to be addressed by HQ SACT.

2.2 Potential collaborative projects are on specific topics that are of mutual interest to both parties but shall be restricted to collaborations in non-procurement areas. Several mechanisms have been already developed to support the initiation of collaborative projects between industry and ACT ranging from informal information exchanges, workshops, studies or more extensive collaboration on research and experimentation.

2.3 Depending on the level and type of interaction needed for a collaborative project, a specific agreement may be needed between parties. The FFCI agreement for any specific project, if required by either party for the project to proceed, will range from “Non-disclosure Agreements” (NDAs) for projects involving exchange of specific information to more extensive “Declaration of Mutual Collaboration” (DOMC) to address intellectual property and other issues.

2.4 More extensive information on the ACT FFCI initiative can be found on the ACT web site being developed to support FFCI projects at http://www.act.nato.int/ffci.

2.5 No FFCI agreement is required to respond to this RFI. However, the principles underlying the FFCI initiative apply to this RFI.

## 3. DESCRIPTION OF THE PROGRAMME

3.1 **Programme Vision**. The NATO IT Modernization vision involves shifting from a decentralized system, where individual locations manage their own equipment and capabilities, to a centrally managed IT infrastructure. This centralized setup, known as NATO Information Technology Modernisation Increment 1 Operational Network (NATO ITM INC 1 ON), will serve Enhanced, Standard, and Remote Nodes or consumer sites within a single domain. NATO ITM INC 1 ON is designed to transform the secret network and its services to a cloud ready maturity level. Additionally, NATO Information Technology Modernisation Increment 3 Operational Network Extension (NATO ITM INC 3 ON-X) aims to transition the cloud ready secret network and its services to the cloud, enhancing collaboration across NATO by offering a federation of services within the NATO Enterprise as outlined below.

3.2 **NATO ITM INC 3 ON-X.** NATO ITM INC 3 ON-X is poised to enhance mobility at NATO Secret (NS) level in support of operational processes. It will contribute to the foundation for NATO digital transformation by include support for a data centric approach, cloud computing, federation and NDW (NATO Digital Workspace), service based approach and enhanced Cyber Security. By 2027, it aims to foster improved collaboration across NS by delivering a federation of services within the NATO Enterprise. NATO ITM INC 3 ON-X's data processing and storage capabilities are crucial to meet the anticipated surge in demand for compute, storage, backup, recovery, and archive. This surge is expected due to a substantial increase in users, data sets, and application capacity requirements. The expansion also necessitates the incorporation of new sites, a heightened emphasis on resilience, and fully synchronous data replication. NATO ITM INC 3 ON-X is tasked with providing services across the entire NATO enterprise, which comprises approximately 29,000 users across 100+ sites spanning 32 countries.

3.3 **Scope**. The scope of this RFI is to encourage collaboration between Nations and industry in exploring future capabilities in Information Technology Modernization (ITM), particularly focusing on information technologies and commercial products.

NATO is actively seeking an up to Secret level cloud solution that provides essential data processing and storage capabilities to meet the anticipated rise in demand for compute power, storage capacity, backup, recovery, and archive services. As NATO expands its membership of nations, it strives to anticipate and meet the growing demand from increased users, data volumes, and application capacity needs. Additionally, as operations expand, there is a requirement to incorporate new sites, prioritizing resilience and fully synchronous data replication. This includes execution of identified business continuity plans to maintain business as usual with minimum disruption by providing necessary redundancy and backup/recovery capabilities. In addition, NATO ITM INC 3 ON-X will provide always-on critical services in a disconnected mode, achieving offline synchronization capabilities.

3.3.1. The vision under the scope of this RFI is that core services will provide Enterprise-wide collaboration at NATO SECRET (NS) within the various Communities of Interest (COI), across all commands and elements of the NATO Enterprise and, where appropriate, to Nations.

3.3.2. The NATO ITM INC 3 ON-X capability is currently in the development phase of the capability programme plan. This plan aims to deliver the required capability described within the capability programme plan by directing the necessary actions across the NATO recognised lines of development including: doctrine, organisation, training, materiel (including software), leadership, personnel, facilities and interoperability.

3.4 Amongst other aims, the Capability Programme Plan intends to analyse alternative options to deliver this capability. This is achieved by:

3.4.1. The identification of different available alternatives to satisfy the defined requirements.

3.4.2. Careful analysis to compare the operational effectiveness, risk and life cycle costs of each alternative.

3.5 The analysis process is designed to assist decision makers in selecting solutions that offer the Alliance value for money. Outline programme options available include consideration of “Adopt”-ing a solution (from Nations), “Buy”-ing (acquiring a solution from Industry), or “Create”-ing (developing a solution bespoke to NATO).

## 4. INTENT/OBJECTIVES

4.1 To support the transformational change of how NATO ITM will provide future operational support, a robust Analysis of Alternatives is needed across the Adopt, Buy, and Create space to identify and determine relevant technologies and products existing within the commercial market.

4.2 This request for information is intended to provide Nations and industry an opportunity to provide information that would allow NATO to identify prospective

products, systems or sub-systems and their potential benefits to the delivery of the NATO ITM INC 3 ON-X. This is not a formal request for submissions as part of a procurement; it is intended to provide support to subsequent and additional in-depth survey to determine possible systems or products, which should be identified in the development of the Capability Programme Plan.

## 5. EXPECTED BENEFITS TO RESPONDENTS

5.1 Nations and industry participants will have the opportunity to present state-of-the-art technologies and products to NATO ITM operators and subject matter experts, such as cloud-based service offerings for NATO private cloud solutions.

5.2 Nations and industry are expected to provide their insights on relevant current and future technologies and products in response to this RFI.

## 6. REQUESTED INFORMATION

6.1 The requested information is embedded in the attached word document.

6.2 **Answers to the RFI**. The answers to this RFI may be submitted by e-mail to the Points of Contact listed above on page 2 of this document.

6.3 **Follow-on**. The data collected in response to this RFI will be used to develop a report to inform the NATO ITM programme. The data collected will be used to provide an assessment to support a decision as to whether NATO should pursue an Adopt, Buy, or Create approach to future ITM products and services.

6.4 **Non-disclosure.** Non-disclosure principles and/or nondisclosure agreement (NDA) with third parties.

6.4.1. HQ SACT will follow non-disclosure principles and possibly conclude an NDA with any companies to protect submitted information from further disclosure. As the third party beneficiary of this nondisclosure, this RFI serves to inform you of how HQ SACT plans to proceed and of HQ SACT's intent to protect information from unauthorized disclosure, requiring the third party company to protect the disclosed information using the highest degree of care that the company utilizes to protect its own Proprietary Information of a similar nature, and no less than reasonable care. The third party company receiving the information shall not, without explicit, written consent of HQ SACT. This includes the following responsibilities and obligations:

6.4.1.1 Discuss, disclose, publish or disseminate any Proprietary Information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is concluded;

6.4.1.2 Use disclosed Proprietary Information in any way except for the purpose for which it was disclosed in furtherance of the goals of the instant project, collaboration, activity or contract; or

6.4.1.3 Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interviews.

6.4.2. Exceptions to Obligations. The third party company receiving the information may disclose, publish, disseminate, and use Proprietary Information:

6.4.2.1 To its employees, officers, directors, contractors, and affiliates of the recipient who have a need to know and who have an organizational code of conduct or written agreement with the recipient requiring them to treat the disclosed Proprietary Information in accordance with nondisclosure principles and the NDA (if executed);

6.4.2.2 To the extent required by law; however, the company receiving the information will give HQ SACT prompt notice to allow HQ SACT a reasonable opportunity to obtain a protective order or otherwise protect the disclosed information through legal process; or

6.4.2.3 That is demonstrated in written record to have been developed independently or already in the possession of the company receiving the information without obligation of confidentiality prior to the date of receipt from HQ SACT; that is disclosed or used with prior written approval from HQ SACT; obtained from a source other than HQ SACT without obligation of confidentiality; or publicly available when received.

6.4.2.4 Any response to this RFI is considered to establish consent to this process. A copy of the NDA, if or when concluded, can be provided on request.

6.5 **Organizational Conflicts of Interest.** Companies responding to this RFI are hereby placed on notice responding to this RFI could conceivably create an organizational conflict of interest (OCI) on a future procurement, if a future procurement were to occur within the capability development process. Companies are cautioned to consider OCI when responding to this RFI, and to consider internal mitigation measures that would prevent OCI's from adversely affecting a company's future procurement prospects. OCI's can often be mitigated or prevented with simple, early acquisition analysis and planning and the use of barriers, teaming arrangements, internal corporate nondisclosure policies and firewalls, and similar prophylactic measures. HQ SACT is not in a position to advise responding companies on the

existence of OCI or remedial measures, and encourages responding companies to consult internal or external procurement and legal consultants and in-house counsel.

6.6 **Handling of Proprietary information.** Proprietary information, if any, should be minimised and clearly marked as such. HQ SACT will treat proprietary information with the same due care as the command treats its own proprietary information, and will exercise due caution to prevent its unauthorised disclosure. Please be advised that all submissions become HQ SACT property and will not be returned**.**

6.7 Provision of data, or lack of, will not prejudice any respondent in the event that there is a competitive bidding process later as part of NATO Common-Funded Capability Development.

## 7. QUESTIONS

7.1 Questions of a technical nature about this RFI announcement shall be submitted by e-mail solely to the above-mentioned POCs. Accordingly, questions in an e-mail shall not contain proprietary and/or classified information. Answers will be posted on the HQ SACT P&C website at: https://www.act.nato.int/opportunities/contracting/rfi-act-sact-24-44/

## 8. SUMMARY

8.1 **This is a RFI only.** The purpose of this RFI is to involve Nations/industry/academia, through collaboration, in an examination of future capabilities related to NATO's ITM with a focus on the IT technologies and commercial products**.** HQ SACT has not made a commitment to procure any of the items described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought. It is emphasised that this is a RFI, and not a RFP of any kind.

# ANNEX A: NATO's ITM Survey to the Nations and Industry

## 1. PURPOSE

1.1 This survey provides an opportunity for nations and industry stakeholders to propose potential solutions for consideration to fulfill the operational needs of NATO's future IT services, known as the Information Technology Modernisation (ITM). The data gathered from this survey will support the Analysis of Alternatives (AoA) for ITM, conducted by the Analysis of Alternatives Branch of HQ Supreme Allied Commander Transformation (HQ SACT).

1.2 ACT is in search of innovative solutions that align with the needs and vision outlined in the background section below. If your proposed solution does not fully meet all the requirements, ACT is open to considering alternative solutions that still address the objectives and vision of the ITM project."

## 2. BACKGROUND

2.1 "NATO's IT Modernization (ITM) initiative is focused on developing a cloud-based IT system that is flexible, interoperable, and scalable, suitable for the NATO SECRET (NS) security classification level. This system aims to enhance collaboration across all NATO commands, various Communities of Interest (COI), and, where necessary, member nations. The ITM project will deliver a network that is reliable, scalable, secure, mobile, resilient, and contemporary, facilitating efficient and secure collaboration among NATO staff and network users. Additionally, to accommodate a significant anticipated increase in the number of users, data sets, and applications, the project requires a scalable solution that offers adequate data storage and processing capabilities to support data synchronization throughout the NATO enterprise.

2.2 ITM will achieve:

- Core services will facilitate collaboration across the entire NATO SECRET (NS) framework, spanning diverse Communities of Interest (COI). This collaboration extends to all commands and components of the NATO Enterprise and, when suitable, to individual Nations;
- Data storage and synchronization across NATO and establishing interconnectivity within NATO networks to maximize the effectiveness of the organization's assets;
- Modern data processing and storage capacity, through the chosen solution, to maintain NATO's progress in becoming a data centric organisation;
- Compatibility with NATO’s Federated Mission Networking concept (FMN);
- Initial steps of NATO’s 2030 Vision to align alliance with modern world technologies.

## To Nations and Industry:

*Organization Name:*

*Organization Address:*

TO ASSIST WITH FOLLOW-ON QUESTIONS, ALL COMMUNICATION DETAILS OF YOUR MAIN POINT OF CONTACT (POC) IS REQUIRED.

*POC Name and Title:*

*POC Email:*

*POC Phone Number:*

FOR ALL QUESTIONS WITHIN THIS RFI, *ACRONYMS ARE TO BE EXPANDED AND* IF ANSWERS/SOLUTIONS PROVIDED ARE CURRENTLY IN USE BY A NATION, YOUR RESPONSES SHOULD INCLUDE:

a. Is the nation ready to provide that capability for NATO Enterprise as a service?

b. Is the nation ready to provide that capability for NATO Enterprise as a “buy” solution?

c. Is the nation able to act as a host nation or as a provider under NCIA as the host-nation?

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

1. What is the name along with detailed information of your solution for servicing the requirements of the ITM capability? Details should include any thresholds and limits of these services, such as the number of users, data storage, capacity or other metrics.
2. A brief overview of your system's architecture, including any commercial software that is leveraged and any additional documentation expanding the details, such as dependencies on other products, etc.
3. Is your proposed system/technology currently in active service as a COTS solution or is it still in development? If it is in service, where is it used and what types of support does your organisation currently provide for such a capability?
4. Are there any legal, geo-political constraints and commercial considerations (e.g. Intellectual Property Rights (IPR) availability, export controls, facilities or National regulations) preventing its use by NATO, NATO nations, or its use on NATO Deployed operations?
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

PROVIDE THE FOLLOWING COST INFORMATION ACCORDINGLY FOR EACH OF THE QUESTIONS:

1. How do you cost the provision of your solution? Do you have cloud service catalogues that contain service decomposition, cost submissions and flexible pricing based on quality of service parameters?
2. Can you provide Rough Order of Magnitude (ROM) Cost estimate for the installation and maintenance of the system for the following structure:
    - 29 000 normal users per year
    - 100+ Main locations in 32 countries
    - Extra locations for exercises and operational bases

**COST-BENEFIT ANALYSIS:**

1. Have you conducted a cost-benefit analysis that explores private cloud implementation alternatives? If yes, elaborate on your analysis, evaluation criteria, and assessment reports to include:
    a. Resiliency: Examining availability, RPO (Recovery Point Objective), and RTO (Recovery Time Objective) values.
    b. Edge computing and business continuity: Assessing backbone determination for always-on critical services, offline synchronization capabilities.
    c. Desktop virtualization: Analysing potential capacity usage, end-user scenarios, centralization of back-end services, and considering the use of VDI (Virtual Desktop Infrastructure) for processing power and storage as opposed to distributed solutions.

**APPLICATION/SERVICE MIGRATION:**

1. Have you evaluated and formulated specific migration choices for transferring services or applications to a private cloud setting? If yes, provide the reports detailing your assessment of migration options.
2. What unique requirements do individual applications or services have to fully utilize and optimize cloud functionalities?
3. What are the outlined plans for configuring and customizing COTS applications and services that are scheduled to be hosted on your cloud environment in the future?
4. Can you provide instances where you have restructured your current non-commercial off-the-shelf (non-COTS) products to fully utilize cloud features and adopt cloud-native solutions?
5. Provide examples of transitioning Infrastructure as a Service (IaaS) backend services, like Database Servers, to Platform as a Service (PaaS) or Software as a Service (SaaS)? If applicable, elaborate on how these changes have enhanced your service Quality of Service (QoS) parameters.

6. In order to expedite the migration process; have you achieved the capability to reuse outputs from preceding site or service increments to automate subsequent sites' migration efforts? Include the role of Infrastructure as Code (IaC) in this process?
7. How did your company strategize and oversee migration phases to optimize automation, reduce timelines, and efficiently utilize resources? With respect to cloud automation capabilities, include the level of reusability was attainable during the migrations in your response? Arrange the migration-related questions in the order of service complexity.

**PRIVATE CLOUD TRANSFORMATION/DEFINING THE CLOUD ITSELF:**

1. Regarding the transformation of current static nodes, including Data Centres (DCs) how has the solution improved the specified quantification criteria to enable the conversion of each node into a cloud node?
    a. Elaborate on the enhancements made in Quality of Service (QoS) services
    b. Provide your interpretation of the cloud, highlighting five key characteristics:
        - On-demand Self Service
        - Broad Network Access
        - Resource Pooling
        - Rapid Elasticity
        - Measured Service
2. The utilization of APIs in the merging of commercial cloud with private cloud poses the question of whether it presents a risk or an opportunity for aligning or converging commercial cloud with private cloud. How do you perceive the evolution of public cloud and private cloud service catalogues in this context?

**FACILITY DEVELOPMENT:**

1. What is your experience in supporting on premise private cloud facilities? Provide examples.

**CONTINUOUS MONITORING, COMPLIANCY CHECK, AUTONOMOUS SERVICE PROVISIONING AND ACCREDITATION CAPABILITIES:**

1. Can you provide instances of implementing cloud-native solutions with a specific emphasis on Infrastructure as Code (IaC) automation capabilities, encompassing automated service provisioning, platform setup, network configuration, and the utilization of script libraries and repositories for development? If available, provide further details
2. What is the extent of your current DEVSECOPS, continuous monitoring, and real-time compliance checking capabilities? Indicate your level of success integrating these capabilities to perform automated audit and accreditation tests for the operation and deployment of cloud services and applications.

**SECURITY POLICY ADMINISTRATION:**

1. What platform do you use for identifying, enforcing, and distributing security policies in your private cloud? Are there distinct platforms, such as Enterprise Mobility Management (EMM) for end-user devices or a centralized Service Management and Control (SMC) for back-end/front-end services, dedicated to these capabilities?

**DATA PORTABILITY:**

1. How did you go about implementing measures to ensure data portability? Were there deliberate plans and implementation efforts to transform vendor-specific data, service, or application service backups into open standards or architectures? For instance, transitioning from directory services to OPEN ID or OAUTH or converting office automation file backups into OPEN OFFICE formats. Provide insights into various scenarios, the type of artefacts used in Infrastructure as Code (IaC) for generic automation models, specific implementation plans, generic models for data portability, with a focus on the role of automation and orchestration in these processes.

**BUSINESS CONTINUITY PLANNING:**

1. Provide further details regarding your disaster recovery plans for the private cloud, specifically in terms of Business Continuity Planning (BCP) and the comprehensive planning of resources, including backup strategies?
2. Did you take into account the integrated layers of IT services for the calculation of resiliency parameters of RTO, RPO and availability?

**SCALABILITY:**

1. How do you achieve auto-scaling capability of your private cloud services?
2. If there is an increase demand for the number of users supported in terms of capacity, what is your response time for providing increased capacity and storage?
3. How does your organisation handle the upgrades to the infrastructure to maintain capacity, effectiveness and cyber-security over time?

**BUSINESS PROCESS ORCHESTRATION, PREPARATION OF SERVICE CATALOGUES, PREPARATION OF DATA CATALOGUES:**

1. Share your experience on preparation of private cloud service catalogues, data catalogues, API Mappings, and your efforts on providing service orchestration integrated with business workflow orchestration. Elaborate on the implementation steps for the end picture, AS-IS to TO-BE, such as dashboards provided to commanders/leaders tracking on-going business workflows or admins to have tracking on service workflows.

**SERVICE MANAGEMENT AND CONTROL (SMC):**

1. Where have you positioned the Service Management and Control (SMC) function within your private cloud infrastructure? Include in your response if the SMC solutions are implemented at Enterprise level globally or at an elemental level.
2. Does your enterprise-wide SMC solution offer centralized management and monitoring for network data flows across various classification levels, or is it federated with local SMC instances?
3. Explain how the federation with major service providers is achieved to monitor service level agreements (SLAs), ensuring the delivery of end-to-end services, and managing incidents, among other aspects?
4. Analysis of service/application over-classification: Shifting workloads from Classified to Unclassified networks involves a series of steps that necessitate a gap analysis. Do you have any insights or experience with this process?
5. What is your familiarity with Service Management and Control (SMC) and data exchange standards in relation to their implementation between the Classified and Unclassified networks?

**IDENTITY AND ACCESS MANAGEMENT:**

1. Explain the connection with IAM integration of your private cloud IAM services within the perspective of Federated Identity and Access management.
2. Have you deployed solutions that facilitate role-based or attribute-based dynamic authorization with respect to data-centric security? Give a detailed answer with examples.
3. Elaborate on the significance and interdependence of NPKI (Non-Public Key Infrastructure) and federated authentication solutions in relation to your centralized Identity Management solutions?
4. From a data-centric security perspective, what is considered the optimal approach for authentication and authorization solutions?

**CLOUD CONNECTIVITY:**

1. How did you evaluate your on-premises cloud connectivity options? On your assessment of the best cloud connectivity option, did you use the following evaluation criteria, if so describe for each:
    - Business Needs
    - Application Requirements
    - Network Geography
    - Site Distribution
    - Security and Compliance
    - Budget and Cost
2. Have you used recent developments of satellite technologies (satellite as a service) as primary transport option or secondary (as a redundant)? If used as

primary transport option, have you achieved auto transformation of static/deployable nodes into cloud nodes by leveraging benefits of low latency and high bandwidth?

**ZERO-TRUST ARCHITECTURE:**

1. Elaborate on your solutions for your implementation of Zero-Trust Architecture, aligned with defence in depth approach?

**DATA CENTRIC SECURITY:**

1. Describe your overarching objective to create data-centric networks with data itself serving as the primary determinant of its classification, thereby eliminating the necessity for distinct classification networks. Elaborate on the integration of data lakes, data labelling, API utilization, application/service updates, and warehouses of analytic/reporting databases.
2. What steps would be involved in the migration and transition of sites towards establishing a data-centric security environment? How do you propose to implement data labelling?
3. What previous experience has your IT capability had with NATO, a national Government or military? Does your solution have a track record of handling sensitive or classified information?

**DATA SOVEREIGNTY/DATA RESIDENCY:**

1. How did you achieve your private cloud data sovereignty/data residency requirements in terms of preventing replication/exposure of your data to specific regions?
2. How would you avoid transferring service desk and monitoring functions to locations outside NATO operation area?

**CLOUD FINOPS (FINANCIAL OPERATIONS):**

1. How do you perform your private/commercial cloud financial operations (FINOPS)?
2. Do you have platforms to monitor and avoid over allocation and underutilization of purchased cloud services?
3. What level of automation have you reached in terms of applying proactive solutions to prevent overbilling of cloud services?
4. Have you managed to integrate your FINOPS capabilities with your global SMC platform?

**PRIVATE CLOUD DEVELOPMENT TEST ENVIRONMENT:**

How do you create a test environment for the development of the private cloud services including COTS and non-COTS services and applications?

# ANNEX B: RFI-Goals and Vision-SACT-24-44

## 1. GOALS FOR INFORMATION TECHNOLOGY–MODERNISATION (ITM) – INCREMENT 3

1.1 **NATO IT:** In the past, NATO capabilities has delivered as a collection of self-contained, individual systems. Separate projects procured all the necessary hardware, software and services required to implement a required capability, which operated within its own information silos. They shared information between themselves in an ad-hoc manner, in addition to certain features and functionality being recreated time and again. These characteristics of systems do not take advantage of economies of scale or the rationalisation of IT Infrastructure that NATO is capable of leveraging.

1.2 **ITM Programme Objective**. The ITM programme is to designed transform the way IT services are provided to users across the NATO enterprise by modernizing, consolidating, and centralising the infrastructure and service management, pooling resources, and delivering services at a higher quality, more flexibly, and at lower cost.

1.3 **Operational Imperative.** While the agreed requirements remain extant, the COVID19 crisis has demonstrated how the operational context has changed. Moreover, all indications are that this change and the need to be prepared for increasing uncertainty in terms of the strategic environment are unlikely to diminish. A flexible, agile, mobile force is critical to the success of NATO. Additionally, the large rise in data due to the very significant increase of users, data sets and applications capacity requirements and the new sites supported is yet another critical enabler to mission success. The imperative to meet the information and data needs of an increasingly distributed and mobile workforce through a protected Enterprise solution is a key operational driver. Therefore, the Increment 3 (Operational Network-Extension) capability is of increasing urgency.

1.4 Scope and Scale.

1.4.1. **Increment 3, Operational Network Extension (ON-X).** Increment 3 (ON-X) is poised to enhance mobility at NATO Secret (NS) levels, supporting operational processes. By 2027, it aims to foster improved collaboration across NS by delivering a federation of services within the NATO Enterprise. ON-X's data processing and storage capabilities are crucial to meet the anticipated surge in demand for compute, storage, backup, recovery, and archive. This surge is expected due to a substantial increase in users, data sets, and application capacity requirements. The expansion also necessitates the incorporation of new sites and a heightened emphasis on resilience and fully synchronous data replication.

## 2. STRATEGIC DRIVERS

2.1 **Communication and Information (C&I) Vision 2025.** The C&I Vision foresees Information and Communications Technology (ICT) services that are fit for purpose and satisfy the needs of the Enterprise users. As such, ICT services are critical enablers of the NATO Enterprise and at the same time support the Alliance needs for interoperability with Nations, Partners, Coalitions and other organizations through federated and public networks. Of critical relevance, the C&I Services are to be 'evergreen' and evolve continuously to ensure relevance to the needs of users.

2.2 **NATO Command Structure-Assessment and Adaptation (NCS-A).** The key implications for Cyberspace are the need to support the key principles of Persistence, Centralisation and Proactivity. These in turn drive specific requirements for persistent federated networking, persistent cyber defence and sufficient levels of resilience within CIS infrastructure to ensure that static Bi-Strategic Commands (Bi-SCs) elements can operate as warfighting HQs. Bi-SCs elements will no longer deploy as full HQs but have the capacity to operate in place as static warfighting HQs. The shift to predominant use of static NCS HQs to anchor C2 of operations will drive an increase for the capacity, resilience and survivability of the supporting CIS and cyber defence infrastructure, including its interfaces to national CIS infrastructures. Completion of ITM is essential to provide the necessary resilience and capacity to the NATO Enterprise. It is therefore expected that the associated capacity, processing and storage requirements will increase in the data centers and nodes in order to maintain and improve the business continuity, efficiency and effectiveness.

2.3 **NATO 2030.** At the June 2021 NATO Summit in Brussels, leaders agreed to chart the Alliance's course over the next decade and beyond. This included agreement to invest more across people, processes and technology including accelerating digitalisation (including in the classified domain). At the core of this intent is the need to build a secure and resilient Enterprise infrastructure and platform. Core Services and Core Communication Capability Packages (and their successor programmes) are at the heart of this endeavour to deliver NATO's 'central nervous system'. In the near and medium term, successful delivery of the existing programmes is foundational to the delivery of NATO's digital ambition in the 2030 timeframe and beyond.

2.4 **NATO's Warfighting Capstone Concept (NWCC).** The NWCC describes the Allies' agreed 'North Star' vision to develop their joint forces. Foundational to deliver this data enabled transformation is the ability to exploit data through a resilient, coherent and unified information infrastructure and platform. This places Core Services, its successor programme and the current ITM Project as a critical interdependency with the NWCC.

## 3. C&I SERVICE REQUIREMENTS

3.1 ICT services are provided that are fit for purpose and satisfy the needs of Enterprise Users.

3.2 ICT services are seen as a critical enabler of the NATO Enterprise. NATO Enterprise C&I will fully support Alliance needs for interoperability with Nations, Partners, Coalitions and other organisations through federated and public networks.

3.3 By 2027, all NATO Enterprise organizations are expected to adopt a uniform set of ICT applications and services on the NS network. The NS networking infrastructures will also unify into a singular NATO Enterprise network, accommodating diverse user communities while meeting all security requirements.

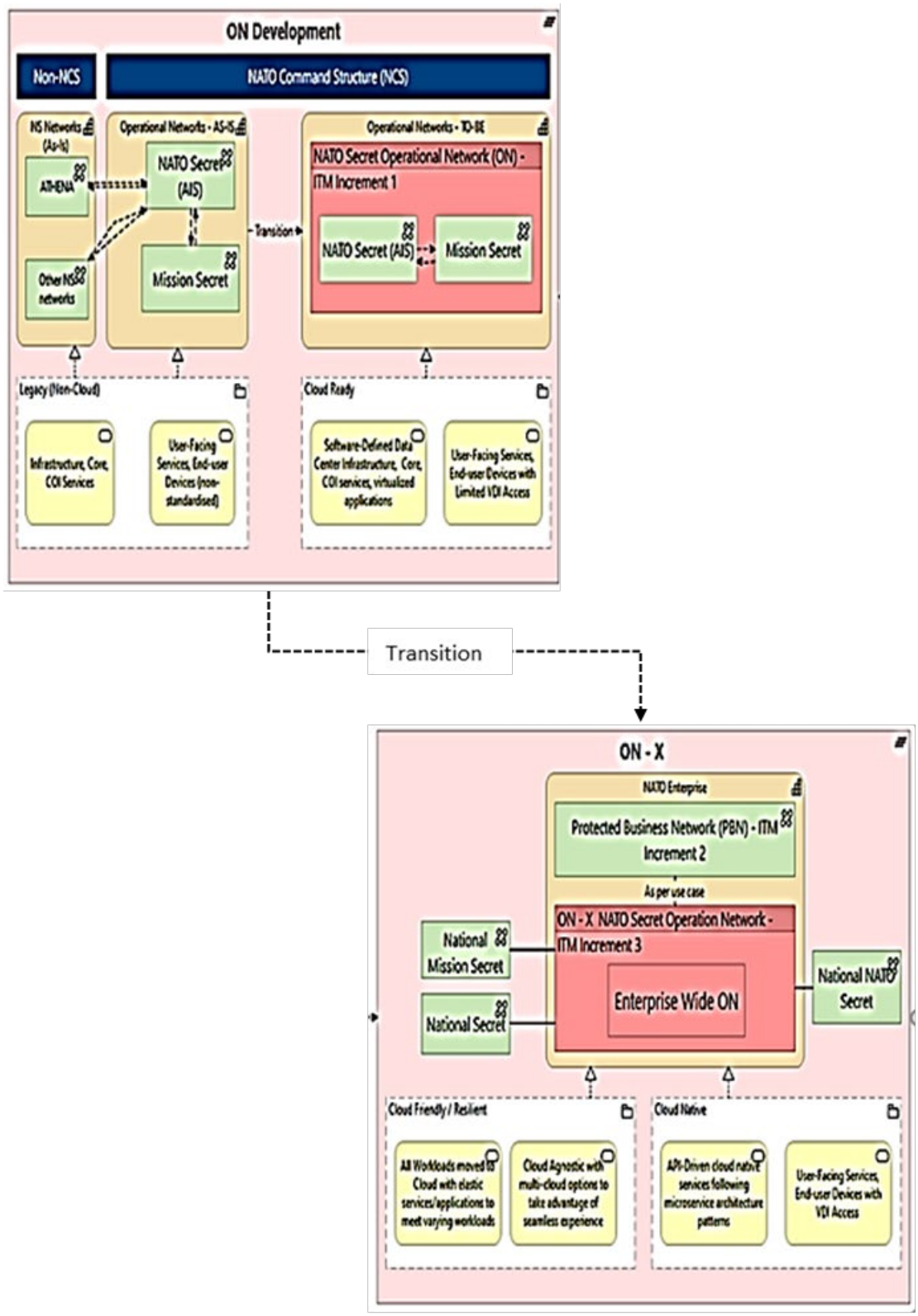
3.4 All NATO Enterprise entities will use standardised ICT services provided to all users within its scope.

3.5 All NATO Enterprise capabilities will be exposed to users as services (Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)).

3.6 All services delivered will be protected against cyber-attacks to a level commensurate with the assessed risk.

3.7 Enterprise C&I services will be ‘evergreen’, continuously evolving and kept relevant as the needs of the users’ evolve to reflect new threats, new possibilities enabled by technology or new missions.

3.8 At all times, an accurate knowledge of the state of the Enterprise C&I will be known and communicated, such that Commanders and other stakeholders can make informed operational decisions.


ON Development
Non-NCS
NATO Command Structure (NCS)
NS Networks (As-Is)
ATI-ENA
Other NS networks
Operational Networks - AS-IS
NATO Secret (AIS)
Mission Secret
Transition
Operational Networks - TO-BE
NATO Secret Operational Network (ON) - ITM Increment 1
NATO Secret (AIS)
Mission Secret
Legacy (Non-Cloud)
Infrastructure, Core, COI Services
User-Facing Services, End-user Devices (non-standardised)
Cloud Ready
Software-Defined Data Center Infrastructure, Core, COI services, virtualized applications
User-Facing Services, End-user Devices with Limited VDI Access
Transition
ON - X
NATO Enterprise
Protected Business Network (PBN) - ITM Increment 2
As per use case
ON - X NATO Secret Operation Network - ITM Increment 3
Enterprise Wide ON
National Mission Secret
National Secret
National NATO Secret
Cloud Friendly / Resilient
All Workloads moved to Cloud with elastic services/applications to meet varying workloads
Cloud Agnostic with multi-cloud options to take advantage of seamless experience
Cloud Native
API-Driven cloud native services following microservice architecture patterns
User-Facing Services, End-user Devices with VDI Access

## 4. DIAGRAM OF TRANSITION, CAPABILITY DRIVERS, AND ROADMAP

4.1 NATO Digital transformation is now being implemented by the ITM (IT Modernization) programme, which is composed of three increments. This RFI's focus area is Increment 3 ON-X. Currently, NATO has an operational network for both the NATO Command Structure and the non-NCS running separately. Increment 1, ON will transition the AS-IS NATO Secret (AIS) with cloud capabilities at the maturity level of 'Cloud Ready'. Increment 3 implementation will start from the end of the ON development, to consolidate all NATO Secret Networks into one Enterprise level Operational Network called the ON-X. ON-X will also exchange information with other national secret networks and with the Protected Business Network – PBN (up to NATO Restricted classification) supporting limited use cases. ON-X's cloud maturity will be both cloud friendly/resilient and cloud native (for some re-architected / SaaS services/applications).

## 5. DEFINITIONS

5.1 Infrastructure as a Service

5.1.1. The Infrastructure as a Service Pattern provides for the delivery of infrastructure resources through Services based on the priorities and needs of the of the governing organisation and/or Consumers. This pattern provides access to the following infrastructure resources:

- Storage
- Networking
- Processing

5.1.2. This pattern requires the pooling of these resources, where feasible, in one physical location where they can be managed, and provisioned, efficiently and effectively.

5.1.3. Demand for infrastructure resources may be elastic and such elasticity should be leveraged to improve resource delivery while maintaining cost-effective solutions. Managing elastic demand is a key feature of the Infrastructure as a Service Pattern.

5.2 Satellite Infrastructure as a Service

5.2.1. The Satellite Infrastructure as a Service Pattern is an extension to the core "Infrastructure as a Service Pattern". It provides the Satellite location with a minimal footprint to support designated local only services. The Satellite infrastructure is maintained by automation and/or central service management and control. Therefore no, or minimal, support personnel are required on site to administer the infrastructure services. The user-facing support personnel could handle tasks that require manual intervention.

5.2.2. While centralizing infrastructure services, the Satellite Infrastructure as a Service Pattern provides a means of safeguarding minimum availability and performance levels.

5.2.3. Local only services like printing, e-mail and file-storage are hosted on minimal footprint locally. Local infrastructure is self-sufficient for this limited set of services in case of communication failure. Local support is for client devices and applications only.

5.2.4. Characteristics of the Branch/Satellite HQ pattern:

- Branch/Satellite HQ infrastructure is logical and physical extension of NATO IaaS.
- Branch HQ infrastructure can support limited information services in absence of connection with NATO IaaS. (resiliency) These services are grouped into two as
- Common services for all sites (local e-mail etc.)
- Site-specific/Mission Critical services
- Branch HQ infrastructure is managed by central SMC.
- Local support personnel for local backend is very small or none.
- Data and applications are synchronized with NATO IaaS.
- Several legacy services/applications are hard or impossible to be provisioned from central data centres. Until those services are modernized, IaaS have to provide a solution to deliver them to end users. Applications should be profiled to develop a strategy for delivery to User Nodes.
- Services like printing or client update services require components needs to be hosted locally for user sites. They need to be orchestrated with enterprise wide services.

5.2.5. Particular applications/data are required to be hosted locally on specific sites for operational resiliency in case of communication disruption. Data integrity and bandwidth provisioning for distribution and synchronization of these applications/data is should be handled in coordination with Communication Services **Distributed Infrastructure as a Service**

5.3 Distributed Infrastructure as a Service

5.3.1. The Distributed Infrastructure as a service pattern establishes two or more instances of the Infrastructure as a Service Pattern that are geographically separated. These instances are inter-connected using a reliable high performance networks creating multiple paths between services and resources. Infrastructure services and resources can be accessed from any instance of the Infrastructure as a Service Pattern even if residing at another physical location. The Distributed Infrastructure as a Service Pattern has the ability to route service and resource requests optimally. The Distributed Infrastructure as a Service Pattern also provides the ability to instantiate multiple authoritative copies of

infrastructure services and resources and disperse them geographically. Redundancy and geographic dispersal are mechanisms used to minimise the impact of the network interruption or physical loss of an Infrastructure as a Service Pattern instance on the organisation.

5.4 Platform as a Service

5.4.1. The Service Oriented Architecture and Identity Management (SOA & IdM) platform (henceforth referred to as the “Platform”) is a Platform-as-a-Service (PaaS) offering reusable middleware services based on standardized best of breed technology.

5.4.2. The strategic goal of The Platform is to help transform a silo-based IT landscape into an efficient and standardized NATO Enterprise IT landscape that is able to swiftly respond to future customer demands.

## 6. FEDERATED MISSION NETWORKING (FMN)

6.1 Federated Mission Networking (FMN) is a governed conceptual framework consisting of people, processes and technology to exchange information and/or services among federated mission participants including but not limited to the use of a set of interconnected autonomous computer networks for the conduct of coalition operations and exercises.

6.2 FMN is built on lessons learned from the Afghanistan Mission Network (AMN) implementation and on the NATO Network Enabling Capability (NNEC) Programme. It is based on trust, willingness and commitment.

6.3 Facilitated by NATO, the *FMN Framework* is providing a permanent ongoing foundation to ensure that mission networks are established and managed efficiently for the purpose of operations, exercises, training or interoperability verifications. It's a governed, managed, all-inclusive structure providing processes, plans, templates, enterprise architectures, capability components and tools needed to plan, prepare, develop, deploy, operate, evolve and terminate Mission Networks in support of Alliance, and multinational operations in dynamic, federated environments.

6.4 The aim of the FMN Concept is to provide overarching guidance for establishing a federated Mission Network (MN) capability that enables effective information sharing among NATO, NATO Nations, and/or Non-NATO Entities participating in operations. A federated MN will be based on trust and willingness and will enable command and control (C2) in future NATO operations.

6.5 The FMN Concept describes the FMN as a capability consisting of three components: (1) Governance (2), FMN Framework, and (3) Mission Network. The FMN is founded on a seamless information exchange between NATO, NATO Nations and Non-NATO Entities participating in operations based on requirements.

6.6 Within the context of ITM, FMN provides a set of standards, processes, information exchange mechanisms, and overall framework for ensuring compatibility and interoperability of the Protected Business Network with Mission Networks.

6.7 More information on FMN can be found at:

- FMN Profiles: https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/volume2/ch04.html
- FMN Spiral 3: https://storage.nisp.nw3.dk/20181118_Final_FMN_Spiral_3_Standards_Profile_Bun dle.pdf
- FMN Spiral 4: https://storage.nisp.nw3.dk/Final_FMN_Spiral_4_Standards_Profile.pdf