Headquarters Supreme Allied Commander Transformation Norfolk Virginia

REQUEST FOR INFORMATION
RFI-ANNEX-ACT-SACT-22-05

This document is the ANNEX for the Request for Information (RFI) Call for Nations and Industry input to NATO's IT Modernisation (ITM) Capability.

Suppliers wishing to respond to this RFI should read this document carefully and follow the guidance for context on the ITM capability.

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

Contents ITM RFI

VISION FOR INFORMATION TECHNOLOGY–MODERNISATION (ITM) – INCREMENT 2 & 3

1. **NATO IT:** In the past, NATO capabilities were 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.

2. **ITM Objective**. The architectural objective of the programme is to 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. Within this, the ITM project is focused on consolidation of hardware and centralisation of existing applications, reducing the IT footprint of local installations, and providing improved tooling to manage the new environment.

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 2 (PBN) capability is of increasing urgency.

4. **Scope and Scale.**

    a. **Increment 2, Protected Business Network (PBN).** Increment 2 (PBN) will deliver mobility at the NATO Restricted (NR) and NATO Unclassified (NU) levels in support of business processes. It will provide a federation of services within the NATO Enterprise to improve collaboration across NU and existing NR domains before 2025.

    b. **Increment 3, Data Processing and Storage.** In capability terms, data processing and storage will be required to meet the large rise in capacity and demand for compute, storage, backup, recovery and archive that are forecast due to the very significant increase of users, data sets and applications capacity requirements. This includes the capability requirement for new sites and the need for increased resilience and fully synchronous data replication.

STRATEGIC DRIVERS

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. **NATO Command Structure-Alignment (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.

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 endeavor 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.

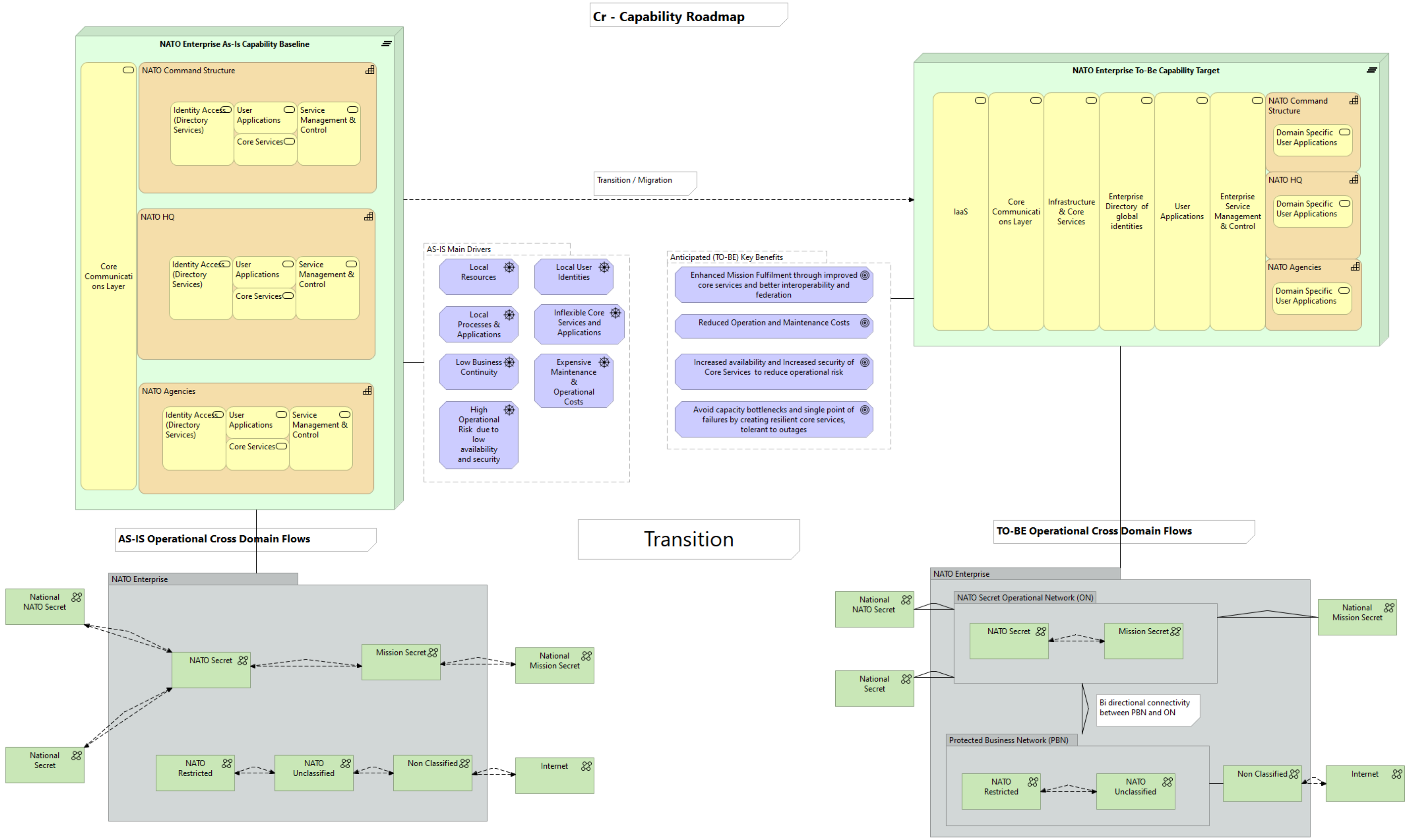
4. **NATO's Warfighting Capstone Concept (NWCC).** The NWCC describes the Allies' agreed 'North Star' vision to develop their joint forces. Foundational to deliver this data enabled transformation is the ability to exploit data through a resilient, coherent and unified information infrastructure and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

C&I VISION STATEMENTS

1. ICT services are provided that are fit for purpose and satisfy the needs of Enterprise Users.
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. All NATO Enterprise organisations will converge by 2025 towards consumption of a standardised set of ICT applications and services. All networking infrastructures will converge towards a single NATO Enterprise network that integrates different user communities and fulfils all security requirements.
4. All NATO Enterprise entities will use standardised ICT services provided to all users within its scope.
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)).
6. All services delivered will be protected against cyber-attacks to a level commensurate with the assessed risk.
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.
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.

HQ Supreme Allied Commander Transformation

DIAGRAM OF TRANSITION, CAPABILITY DRIVERS, AND ROADMAP


Cr - Capability Roadmap
NATO Enterprise As-Is Capability Baseline
Core Communications Layer
NATO Command Structure
Identity Access (Directory Services)
User Applications
Service Management & Control
Core Services
NATO HQ
Identity Access (Directory Services)
User Applications
Service Management & Control
Core Services
NATO Agencies
Identity Access (Directory Services)
User Applications
Service Management & Control
Core Services
Transition / Migration
AS-IS Main Drivers
Local Resources
Local User Identities
Local Processes & Applications
Inflexible Core Services and Applications
Low Business Continuity
Expensive Maintenance & Operational Costs
High Operational Risk due to low availability and security
Anticipated (TO-BE) Key Benefits
Enhanced Mission Fulfilment through improved core services and better interoperability and federation
Reduced Operation and Maintenance Costs
Increased availability and Increased security of Core Services to reduce operational risk
Avoid capacity bottlenecks and single point of failures by creating resilient core services, tolerant to outages
NATO Enterprise To-Be Capability Target
IaaS
Core Communications Layer
Infrastructure & Core Services
Enterprise Directory of global identities
User Applications
Enterprise Service Management & Control
NATO Command Structure
Domain Specific User Applications
NATO HQ
Domain Specific User Applications
NATO Agencies
Domain Specific User Applications
AS-IS Operational Cross Domain Flows
Transition
TO-BE Operational Cross Domain Flows
NATO Enterprise
National NATO Secret
National Secret
NATO Secret
Mission Secret
National Mission Secret
NATO Restricted
NATO Unclassified
Non Classified
Internet
NATO Enterprise
National NATO Secret
National Secret
NATO Secret Operational Network (ON)
NATO Secret
Mission Secret
National Mission Secret
Bi directional connectivity between PBN and ON
Protected Business Network (PBN)
NATO Restricted
NATO Unclassified
Non Classified
Internet

DEFINITIONS

Infrastructure as a Service

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
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.
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.

Satellite Infrastructure as a Service

4. 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. While centralizing infrastructure services, the Satellite Infrastructure as a Service Pattern provides a means of safeguarding minimum availability and performance levels.
6. 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.
7. 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.
8. 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

9. 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.

Platform as a Service

10. 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.
11. 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.

FEDERATED MISSION NETWORKING (FMN)

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.
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.
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.
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.
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. 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.
7. More information on FMN can be found at:
   - FMN Profiles
   - FMN Spiral 3
   - FMN Spiral 4