ΑΔΙΑΒΑΘΜΗΤΟ
ΚΑΝΟΝΙΚΟ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Μόνιμη Αντιπροσωπεία της Ελλάδος
στο NATO

Aikaterini Nikaki
16.12.2021 17:58

Αρμόδιος: Ασμχος (ΜΕ) Δημήτριος Κανταρτζόγλου
Τηλ.: +32 2 707 6734
e-mail: d.kantartzoglou@grdel-nato.be

Βρυξέλλες, 16 Δεκεμβρίου 2021
Α.Π.: 6578

ΠΡΟΣ: **ΥΠΟΥΡΓΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ**
- ΓΔΑΕΕ/ΔΑΕΤΕ *(μ.η.)*

ΚΟΙΝ.: **ΥΠΟΥΡΓΕΙΟ ΕΞΩΤΕΡΙΚΩΝ**
- κ. Δ' Γενικό Διευθυντή
- Δ2 Διεύθυνση

ΓΕΕΘΑ
- Γ2 Διεύθυνση

ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ
- Γενική Γραμματεία Εμπορίου *(μ.η.)*
- Γενική Γραμματεία Βιομηχανίας/ Διεύθυνση Διεθνών Βιομηχανικών Σχέσεων (*μ.η.)*

ΤΕΧΝΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΕΛΛΑΔΟΣ
- Διεύθυνση Επαγγελματικής Δραστηριότητας (*μ.η.)*

ΘΕΜΑ: Αίτηση για Παροχή Πληροφοριών RFI-ACT-SACT-21-86 για το Αντικείμενο: "NATO's IT Modernisation (ITM) Capability)"

Διαβιβάζεται, συνημμένως, αίτηση Συμμαχικής Διοίκησης Μετασχηματισμού (ACT) για συμμετοχή Βιομηχανίας σε έρευνα και παροχή πληροφοριών (Request for Information/RFI) για εν θέματι αντικείμενο.

Καταληκτική ημερομηνία υποβολής προτάσεων ενδιαφερομένων ορίζεται η **31η Ιανουαρίου 2022.**

Ενδιαφερόμενες εταιρίες δύνανται αναζητήσουν πληροφορίες μέσω καθοριζομένων σημείων επαφής (Point of Contact/POC, βλ. σελ. 2 αιτήσεως).

Παρακαλούμε για τις ενέργειές σας προς ενημέρωση Βιομηχανίας και Ακαδημαϊκών Ιδρυμάτων.

Λ Α Μ Π Ρ Ι Δ Η Σ

Συν. σελ.: 16
Ηλεκτρονικό αρχείο φύλλων δεδομένων : 1

ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ
Η υπάλληλος της Μ.Α. ΝΑΤΟ
Αικατερίνη Νικάκη
Τμηματάρχης Α' ΕΠ & ΠΛ

Headquarters Supreme Allied Commander Transformation
Norfolk Virginia

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

This document contains a 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 responding.

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

HQ Supreme Allied Commander Transformation RFI 22-05 General Information	
Request For Information No.	22-05
Project Title	Request for Nations and industry input to NATO's ITM Capability.
Due date for submission of requested information	31 January 2022
Contracting Office Address	NATO, HQ Supreme Allied Commander Transformation (SACT) Purchasing & Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490
Contracting Points of Contact	1. Ms Tonya Bonilla e-mail : tonya.bonilla@act.nato.int Tel : +1 757 747 3575 2. Ms Catherine Giglio e-mail : catherine.giglio@act.nato.int Tel :+1 757 747 3856
Technical Points of Contact	1. Dr Arnau Pons, e-mail : arnau.pons@act.nato.int Tel : +1 757 747 3876 2. Philip Deans e-mail: Philip.deans@act.nato.int Tel: +1 757-747-3746

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 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. Further, 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.

2 – GENERAL BACKGROUND: ACT Framework for Collaborative Interaction (FFCI)

2.1 ACT has implemented a Framework for Collaborative Interaction (FFCI) to increase opportunities for industry and academia to contribute to ACT capability development efforts through collaborative work. Such collaboration enables HQ SACT, and NATO as a whole, to benefit from industry/academia 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 industry / academia with an improved understanding of NATO's capability requirements and the associated issues and development challenges to be addressed by HQ SACT. 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/academia and ACT ranging from informal information exchanges, workshops, studies or more extensive collaboration on research and experimentation.

2.2 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" (NDA) for projects involving exchange of specific information to more extensive "Declaration of Mutual Collaboration" (DOMC) to address intellectual property and other issues.

2.3 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.

2.4 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**

3.1.1 The overall NATO IT Modernisation vision can be described as moving from a highly decentralized environment with each location possessing and operating their own equipment, expert servicing and capabilities, towards a centrally managed, centralized IT infrastructure providing services to Standard Nodes or consumer sites in two domains (PBN and ON), providing IaaS, utilizing centralized provisioning, a centralized Service Operations Centre(s) to manage the infrastructure, and Service Operations. The networks are described as follows:

- PBN: the Protected Business Network will enable communication of information up to NATO RESTRICTED across the NATO enterprise.
- ON: the Operational Network will enable communication of information up to NATO SECRET across the NATO enterprise.

The scope of this RFI is to provide a centralized PBN (Protected Business Network) allowing for NATO information up to NATO RESTRICTED and providing the data storage and processing capacity necessary for the network and data synchronization across applications, services, distributed across the enterprise. Initially this will impact 15 000 users at 18 main locations in 11 countries under the Strategic Commands, but shall be scalable to the entire NATO enterprise consisting of approximately 25 000 users at 32 main locations in 13 countries. Moreover, operational bases, exercises and other locations will also require ITM capabilities.

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

3.1.3 The NATO ITM 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.

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

- the identification of different available alternatives to satisfy the defined requirements.
- careful analysis to compare the operational effectiveness, risk and life cycle costs of each alternative.

3.1.5 The analysis process is designed to assist decision makers select 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).

3.2 **Intent/Objectives.**

3.2.1 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.

3.2.2 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 network and data management. 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.

3.3 **Expected benefits to respondents**

3.3.1 Nations and Industry participants will have the chance to expose NATO ITM operators and subject matter experts to state of the art technologies and products.

3.4 **Expected input from industry/academia**.
3.4.1 Expected input to this RFI is Nations and industry perspective on relevant current and future technologies and products.

4 - REQUESTED INFORMATION

The requested information is embedded in the attached excel file.

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

4.2 **Follow-on**.
4.2.1 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.

4.2.2 **Non-disclosure.** Non-disclosure principles and/or nondisclosure agreement (NDA) with third party company

4.2.2.1 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. This includes the following responsibilities and obligations:
The third party company receiving the information shall not, without explicit, written consent of HQ SACT:

- Discuss, disclose, publish or disseminate any Proprietary Information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is concluded;
- 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
- Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interviews.

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

- 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);

- 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
- 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.

4.2.2.2 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.

4.3. **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.

4.4 **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**.**

4.5 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

4.6 **Questions.** 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: www.act.nato.int/contracting-procurements.

4.7 **Response Date**. 31 January 2022

4.8 Summary. **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.

Tonya Bonilla
ACT Contracting Officer - Allied Command Transformation (ACT) NATO/HQ SACT
Tel: (757) 747-3575, **E-mail: tonya.bonilla@act.nato.int**

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.

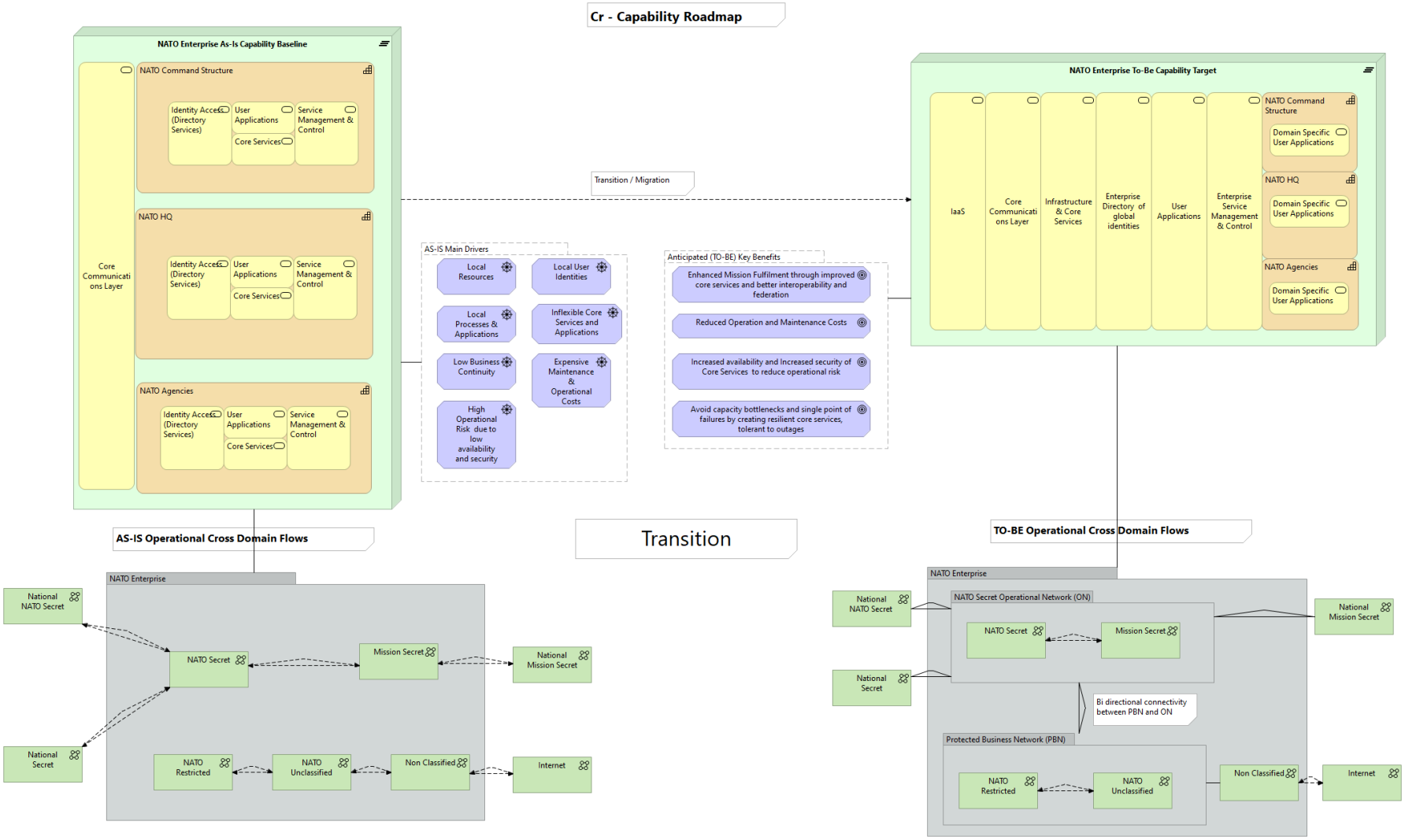
3. **NATO 2030.** At the June 2021 NATO Summit in Brussels, leaders agreed to chart the Alliance's course over the next decade and beyond. This included agreement to invest more across people, processes and technology including accelerating digitalisation (including in the classified domain). At the 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.

DIAGRAM OF TRANSITION, CAPABILITY DRIVERS, AND ROADMAP



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