Headquarters Supreme Allied Commander Transformation Norfolk Virginia

REQUEST FOR INFORMATION
RFI-ACT-SACT-21-65

This document contains a Request for Information (RFI) Call for NATO Nations and Industry to provide inputs to NATO's NATO Enterprise Wide Core Communications Multimedia Access Services (NEW Core Comms MMAS) Capabilities.

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

HQ Supreme Allied Commander Transformation RFI 21-65 General Information	
Request For Information No.	21-65
Project Title	Request for Nations and Industry to provide inputs to NEW Core Comms MMAS Capabilities
Due date for submission of requested information	11 June 2021
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. Jens Weber e-mail: jens.weber@act.nato.int Tel: +1 757 747 4358 2. Klean Xhelilaj e-mail: klean.xhelilaj@act.nato.int Tel: +1 757 747 4204

1 - INTRODUCTION

1.1. **Summary**. Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with NATO Nations and Industry. The intention is to establish the art-of-the-possible and state-of-the-art with respect to technologies, products and services in the area of NATO Enterprise Wide Core Communications and Multimedia Access Services Capabilities in order to support NATO Governance decision-making on Common Funded Capability Development.

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 existing and available capabilities related to Core Communications. 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 the 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.

3 - DESCRIPTION OF THE PROGRAMME

3.1. **Programme Vision**

3.1.1. NEW Core Comms MMAS capability represents the Command & Control core communications backbone of the NATO Enterprise, the essential and critical IT infrastructure for Enterprise customers, the main critical and resilient collaboration services of NATO and necessary access to the Internet service for all NATO Enterprise users. This capability will enable a more survivable NATO command network by reducing the network attack surface to a minimum, sustainable footprint, enabling a wider Alliance and Coalition Federation in the strategic domain and ensuring evolving technological progress over time.

This programme through its future projects, will update NATO's Communications Infrastructure in support of political consultation, decision-making, and command and control, across the joint land, air and maritime domains to developing in the near future into a more resilient and survivable "NATO Command Network" (C2, C4ISR, NC3) and a Business as Usual "General Purpose Network" network with less critical performance requirements. It will introduce a paradigm shift in the way network services and network infrastructure are provisioned and sustained. This new architectural approach will adopt a service oriented perspective, following industry innovations and foster the implementation of services on infrastructure that can independently evolve, be upgraded or replaced, wholly or partly, without the constraints of today's vendor-specific environments.

3.1.2. The main capability is clustered as below:

a. Core Communications Infrastructure Services:

(1) Protected Core Services;

(2) Coloured Cloud Services.

b. Communications and Collaboration Services:

(1) Unclassified Voice Service;

(2) Secure Voice Services;

(3) Studio VTC Services.

c. Enterprise Internet Services:

(1) Internet Access Services;

(2) Internet Hosting Services.

This programme will focus on reducing the NATO Enterprise network footprint by decreasing the number of interconnection points between the NATO Enterprise and members of the Alliance Federation and Coalition Federation from existing 600+ to around 100 in the future. This clear delineation will improve the cybersecurity posture by reducing the attack surface. This stable baseline after full NCI implementation will provide for future self-contained, service-oriented architectures for the communications network infrastructure and the collaboration services. Using this approach, individual Service Level Agreement (SLA) specifications, thresholds, and targets for service levels for all self-contained services can be defined. The Programme will create more standardised, self-contained and agile services definitions.

In this context, the NEW Core Comms MMAS programme endeavours to outfit capability within the NATO Enterprise. This RFI relates specifically to communications infrastructure and multimedia services maintenance and development for the NATO Enterprise. It includes addressing lifecycle issues such as obsolescence and ensuring the Enterprise (including Allied Operations and Missions [AOM]) has critical CIS communications capabilities required to keep pace with the current operational requirements and consolidate the NATO Communications Infrastructure (NCI) with the Alliance Federation Participants (AFPs).

The consolidation and segmentation of a high-availability, high-scalability Communication and Collaboration capability for both unclassified and secure voice and VTC, strictly allocated to support a command network with C3 activities within the NATO Command Structure (NCS) and in HQ, including all COIs (Core Services, AirC2, Alliance Federation, Cyber Defence, etc.). This capability will be interconnected with the digital collaboration platforms predominant in the non-C3 business domain, in the framework of Core Enterprise Services and projects dealing with collaboration services and digital workspaces in general.

3.1.3. The NEW Core Comms MMAS Programme is currently at the stage to develop a consolidated, comprehensive programme plan that will deliver a required capability as detailed in the Capability Requirements Brief (ref. ACT/CAPDEV/REQS/TT-3409/SER:NR:0172). This plan will direct the necessary actions across the NATO-recognised lines of development including: Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability. This is NATO's Capability Programme planning stage within the new NATO Common Funded Capability Delivery Governance Model. The new NATO Common Funded Capability Delivery Governance Model includes decision points on the:

- Requirement (via the Operational Requirements Statement) – the Programme Mandate;
- Viability of a capability-based programme to satisfy the requirement (via the Capability Requirements Brief) – the Programme Brief and Vision; and
- Establishment of a programme to deliver capabilities and to drive the transformational change – the Capability Programme Plan.

3.1.4. Amongst other aims, the Capability Programme Plan is intended to determine alternatives through an analytical comparison of the operational effectiveness and life cycle costs of different alternatives under consideration to satisfy the requirements. The Analysis of Alternatives (AoA) also includes consideration of the possibility of "Adopt"-ing a solution (from Nations), "Buy"-ing (acquiring a solution from Industry), or "Create"-ing (developing a solution bespoke to NATO). The AoA will assist decision makers to identify alternatives that offer the Alliance value.

3.1.5. To achieve the aims of the Capability Programme Plan, a Request for Information is necessary to determine relevant technologies, products and services that exist within NATO Nations (as part of the consideration of "Adopt"-ing a solution from Nations) or that are available on the commercial market (as part of the consideration of "Buy"-ing a solution from Industry). This request intends to identify prospective solutions, implementation and approaches, for which the team may need to conduct additional in-depth discussions. This is not a formal request for submissions as part of a procurement; it is intended to conduct an additional in-depth survey to determine possible solutions, implementations and approaches, which should be identified in the development of the Capability Programme Plan.

3.2. **Intent/Objectives.**

To support the transformational change and future development of NEW Core Comms MMAS capabilities, a Capability Programme Plan needs a robust Analysis of Alternatives, notably from the "Adopt" and "Buy" perspectives. This Request for Information is intended to provide NATO Nations and Industry an opportunity to provide information that would allow NATO to determine potential benefits they might receive from adopting or buying an existing solution. As part of this process, Nations may rely on information from Industry.

3.3. **Expected benefits to respondents.**

NATO Nations and Industry will have the chance to expose NATO core communications and multimedia services subject matter experts to existing technologies, products and services.

3.4. **Expected input from Nations and Industry**.

Expected input to this RFI is the perspective from Nations and Industry on relevant and existing solutions and approaches responding to NATO requirements.

4 - REQUESTED INFORMATION

4.1. **Intent.**

The information collected with this survey (please see enclosed Excel spreadsheet) will be used in support of the AoA for NEW Core Comms MMAS capability programme that will be conducted by HQ Supreme Allied Commander Transformation's Analysis of Alternatives Branch. To enhance understanding of NATO needs, HQ SACT will conduct two GoToMeeting collaborative question and answer (Q & A) sessions with NATO subject matter representatives on 19 May 2021, First Session: 0730 - 0900 EST | 1230 - 1400 GMT | 1330 - 1500 CET and Second Session on 24 May 2021 0930 - 1100 EST | 1430 - 1600 GMT | 1530 - 1700 CET). These sessions will enable participants to interact with ACT Programme Team and POCs. If you want to participate, please send your contact details e-mail, nation you represent, name, function and the date you prefer to participate on 19th (Session 1) or 24th (Session 2) of May to jens.weber@act.nato.int and klean.xhelilaj@act.nato.int and you will be invited in one of the following sessions:

- The first session 19th of May (0730 - 0900 EST | 1230 - 1400 GMT | 1330 - 1500 CET).
- The second session 24th of May (0930 - 1100 EST | 1430 - 1600 GMT | 1530 - 1700 CET).

The requested information is embedded in the attached spreadsheet: *RFI-ACT-SACT-21-65 NEW Core Comms MMAS – RFI Questions and Requirements Assessment.xlsx*.

4.2. **Answers to the RFI**.

The answers to this RFI may be submitted by e-mail to the contracting and technical Points of Contact listed above. Sensitive information can also be forwarded to the POCs, who have information access up to NATO Secret. Further instructions will be provided upon such a request.

Nations and Industry respondents indicating that a solution could be adopted or bought are expected to provide Rough Order of Magnitude (ROM) costing. The ROM costing shall not be considered as an offer or commitment from the respondent. In case Nations or Industry respondents do not want to document this, one on one discussion can be set up to discuss only about proposals and costing.

4.3. **Follow-on**.

4.3.1. The data collected in response to this RFI will be used to develop a report to inform the NEW Core Comms MMAS Programme. The data collected will notably be used to provide an assessment to support a decision as to whether NATO should pursue an Adopt/Buy approach to NEW Core Comms MMAS capabilities and follow one of the following acquisition models:

a. NATO Owned, NATO Operated (NO-NO)

b. NATO Owned, Contractor Operated (NO-CO)

c. Contractor Owned, NATO Operated (CO-NO)

d. Contractor Owned, Contractor Operated (CO-CO)

4.3.2. 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.

4.4. **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. **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.

4.6. **Response Date**. 11 June 2021.

4.7. Summary. **This is a RFI only. The purpose of this RFI is to involve Nations and Industry, through collaboration,** in an examination of existing capabilities related to NEW Core Comms MMAS capability. 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. 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.

Enclosure to
RFI-ACT-SACT-21-65

Please use the Excel file *RFI-ACT-SACT-21-65 NEW Core Comms MMAS - RFI Questions and Requirements Assessment.xlsx*, “1. Capability Overview” tab to answer the questions. Below requirements are provided for easy reading and reference.

Purpose:

This survey allows nations to offer potential alternative solutions for consideration to meet the operational requirements for NEW Core Comms MMAS (NATO Enterprise-Wide Core Communications MultiMedia Access Services) capability programme. The information collected in this survey will be used in support of the Analysis of Alternatives (AoA) for NEW Core Comms MMAS by HQ Supreme Allied Commander Transformation’s Analysis of Alternatives Branch.

Prioritised Requirements:

Core Communications Infrastructure Capability

Protected Core Services

Coloured Cloud Services

1. The Core Communications Infrastructure Capability shall provide communications services to the strategic segment of the NATO Enterprise.

a. The Core Communications Infrastructure Capability shall enable communications between the strategic segment of the NATO Enterprise and other parties in the wider Alliance Federation[1] and Coalition Federation(s)[2] realms.

b. Core Communications Infrastructure Capability shall support all Core Entities[3] of the NATO Enterprise, as well as any customer-funded entities qualifying as Standard Entities[4] of the NATO Enterprise.

c. The implementation of communications services supporting connectivity within the NATO Enterprise, and towards the wider Alliance Federation and Coalition Federation realms, shall adhere to Protected Core Networking (PCN) principles (STANAG 5637).

d. The strategic portion of the NATO Enterprise shall rely on Protected Core Services delivered by the Protected Core Segment[5] of the NCI (NATO Communications Infrastructure).

[1] NATO Nations, most of the NATO Force Structure.

[2] NATO Nations and Approved Partner Nations or entities in Alliance-authorised missions.

[3] - that are defined as part of the NATO Enterprise. This includes the NATO HQ (both IS and IMS), the NATO Command Structure, the NATO Agencies (e.g. NCI Agency, NSPA, etc.) and the National Points of Presence.

[4] - are those that Allies choose to get Enterprise standardised services. These entities pay for access to all (or a subset of) NATO Enterprise services and are subject to the mandatory body of policy, directives and guidance, applicable within the NATO Enterprise. Roles and responsibilities of security and legal nature, where appropriate, need to be clearly determined and officially acknowledged before Enterprise services are provided to these entities.

[5] A PCS is a network built on the principles of PCN as described in section 1.4 and designed to work seamlessly with other PCS-s in a federation of systems.

e. Protected Core Network Services shall provide Alliance-wide resilient connectivity to multiple Coloured Clouds[6] operating within the NATO Enterprise and extending into the Alliance and Coalition Federation environments.

f. The static portion of the NATO Enterprise shall rely on ON (NS)[7], and PBN (NU and NR)[8] Coloured Clouds, supported by the Protected Core Segment of the NCI.

g. Protected Core Services shall be present and available to connect Coloured Clouds across the NATO Enterprise.

h. Coloured Cloud Services shall provide Alliance-wide connectivity to the various eligible Communities of Interest (COI) of the NATO Enterprise at different levels of security and enable wide area connectivity to non-eligible entities.

i. Protected Core Services shall be able to scale and adapt their capacity and/or resilience to changing operational requirements driving changes in traffic volumes and/or availability.

j. Protected Core Services serving NATO Enterprise entities other than the NCI Core Nodes shall feature sufficient capacity to adequately support the traffic flows generated by the COIs served by the connected Coloured Clouds.

k. The Core Communications Infrastructure shall be centrally managed from the primary and alternate Service Operations Centres (SOC).

l. NATO CIS Provider Service Management shall control all the services provided under the Core Communications Infrastructure capability.

m. Protected Core Services and Coloured Cloud Services shall rely on a dedicated Network Management and Cyber Defence capability (NMCD), existing and operated within the NCI.

n. The Core Communications Infrastructure capability shall feature facility, physical link, and physical node redundancy and diversity when the sought availability levels equal or exceed 99.99%.

o. Protected Core Services shall guarantee transport performance and availability for different traffic flows, end-to-end, as delivered by the connected Coloured Clouds or by any federated Protected Core Segments which shall be handled in accordance with their precedence levels, in the event of network congestion and/or underperformance affecting the Protected Core.

p. Coloured Cloud Services shall guarantee transport performance and availability for different traffic flows, end-to-end, as delivered by the connected COI or by any federated Coloured Clouds which shall be handled in accordance with their precedence levels, in the event of network congestion and/or underperformance affecting the Coloured Cloud.

q. The Core Communications Infrastructure capability shall feature northbound interfaces to connect to the Enterprise-wide Service Management System (ESMS).

r. Protected Core Services shall provide connectivity to the Protected Core Segments of Alliance Federation Participants, and to their Coloured Clouds.

[6] A CC is a cloud of a specific information (security) domain. If information confidentiality for the traffic transported between CC-s is needed, crypto devices shall be used to tunnel traffic via the protected core segment.

[7] ON – Operational Network, NS – NATO Secret

[8] PBN – Protected Business Network, NU – NATO Unclassified, NR – NATO Restricted

s. Protected Core Services shall individually authenticate and authorize the connectivity of Coloured Clouds and Protected Core Segments of Alliance Federation Participants operating outside the NATO Enterprise.

t. Protected Core Services shall be able to reach and connect to the Protected Core Segment(s) of Alliance Federation Participant(s), either through collocation at a NATO Enterprise site, or over long-haul transmission media terminating at the site, when no collocation exists.

u. Coloured Cloud Federation Services shall be able to reach and connect to the Coloured Cloud(s) of Alliance Federation Participant(s), either through collocation at a NATO Enterprise site, or over a Protected Core, and through the use of interoperable cryptos (NINE[9]), when no collocation exists.

v. Federating the NCI with the Protected Core Segments or the Coloured Clouds of NATO nations shall be possible over redundant and geographically diverse interconnection points, enabling resilient and/or load-balanced connectivity to the NATO Enterprise or to other Alliance Federation Participants.

w. Protected Core Network Services shall prevent the analysis of traffic flows and patterns generated by the Coloured Clouds of the NATO Enterprise, through the application of Traffic Flow Confidentiality (TFC) measures.

x. The NATO Enterprise CIS Provider, hereafter referred as the "CIS Provider" shall conduct Cyber Security Monitoring Services to monitor the Core Communications Infrastructure Capability.

y. The Core Communications Infrastructure Capability shall provide capturing probes for full packet capture.

z. The Core Communications Infrastructure Capability shall support dual-stack IP standards (IPv4 and IPv6).

Communications and Collaboration Capability

Unclassified Voice Services

Secure Voice Services

Studio VTC Services

2. Communication and Collaboration Services (Multimedia Access Services) shall be supported by their own, dedicated Coloured Cloud Network services and supporting Coloured Clouds, yet sharing the same Protected Core Segment as the Coloured Clouds transporting data traffic.

a. Multimedia Access Services back-end, front-end and inter-connectivity components shall be self-contained with clearly defined interfaces and standards.

b. Multimedia Access Services shall allow separate life cycling of their above components for both hardware and software.

c. NATO Enterprise CIS Provider shall deliver Unclassified Voice Services to all of its users.

(1) NATO Unclassified Voice Services shall provide a minimum set of features that include: OpsLoop, conferencing, hunt groups, voice mail, phone billing service, call intercept, and call forwarding.

[9] Network and Information Infrastructure Network Encryption.

(2) NATO Unclassified Voice Services shall support the use of both desktop, mobile (handheld) and support integrated calls established from software-based applications (i.e. soft-phones).

(3) NATO Unclassified Voice Services shall include a legacy FAX transmit and receive capability.

(4) NATO Unclassified Voice Services shall centralise call processing.

(5) NATO Unclassified Voice Services shall maintain a service availability target of 99.5%.

(6) NATO Unclassified Voice Services shall allow for any site to continue using those services within the site, when the site is disconnected from the NCI Core Nodes.

(7) The Service Provider shall resolve Unclassified Voice Services incidents above critical level within 4 hours.

(8) The NATO Enterprise CIS Provider shall manage and control NATO Unclassified Voice Services (24/7/365).

(9) NATO Unclassified Voice Services shall be subject to Cyber Security monitoring, for security-related incidents.

(10) NATO Unclassified Voice Services shall be subject to SMC (Service Management and Control) monitoring, for CIS-related incidents.

(11) NATO Unclassified Voice Services shall support the federation with the unclassified voice services of Alliance Federation Participants, and implement boundary protection measures accordingly.

(12) NATO Unclassified Voice Services shall enable integration with the Unified Communications and Collaboration (UCC) capability, which encompasses voice services carried over the data network.

(13) NATO Unclassified Voice Services shall integrate with ESMS (Enterprise-wide Service Management System).

(14) NATO Unclassified Voice Services shall integrate with NPKI (NATO Public Key Infrastructure).

(15) NATO Unclassified Voice Services shall integrate with NEDS (NATO Enterprise Directory System).

(16) NATO Unclassified Voice Services shall federate with DCIS Unclassified Voice Services.

(17) NATO Unclassified Voice Services towards the public networks shall rely on global SIP trunks terminated at the NCI Core Nodes, to allow for the adoption and enforcement of centralised (vice per site) call management and security measures by the NCI.

(18) NATO Unclassified Voice Services shall comply with both IPv4 and IPv6 protocols for their equipment.

d. NATO Enterprise shall provide Secure Voice Services, available to all of its users.

(1) NATO Enterprise shall provide Voice over Secure Internet Protocol (VoSIP) to include NS via the Operational Network (ON) until SCIP is fully implemented.

(2) NATO Secure Voice Services shall be physically segregated from the data network infrastructure, in terms of applications hosting, and transport of traffic (dedicated Coloured Cloud).

(3) NATO Secure Voice Services shall allow for any site to continue using those services within the site, when the site is disconnected from the NCI Core Nodes.

(4) NATO Secure Voice Services shall provide a minimum set of features that include: OpsLoop, calls, video calls, conferencing calls, video conferencing calls, hunt groups, pick up groups, call forwarding, and extension mobility services.

(5) NATO Secure Voice Services shall support the use of both desktop, mobile (handheld) and support calls established from software-based applications (i.e. soft-phones).

(6) NATO Secure Voice Services shall provide fax over secure data (IP) networks.

(7) NATO Secure Voice Services shall meet an availability target of 99.5%.

(8) The Service Provider shall resolve Secure Voice Services incidents above critical level within 4 hours.

(9) The Service Provider shall manage and control Secure Voice Services (24/7/365).

(10) NATO Secure Voice Services shall comply with both IPv4 and IPv6 protocols for their equipment.

(11) NATO Secure Voice Services shall support the federation with the secure voice services of Alliance Federation Participants, and implement boundary protection measures accordingly.

(12) NATO Secure Voice Services shall support the federation with the secure voice services of Coalition Federation Partners, through the Mission Anchor Function(s).

(13) NATO Secure Voice Services shall federate with DCIS Secure Voice Services.

(14) NATO Secure Voice Services shall enable integration with the Unified Communications and Collaboration (UCC) capability, which encompasses secure voice services carried over the secure data network.

(15) NATO Secure Voice Services shall support multiple COIs, in turn supported over one or more instances of Coloured Cloud Network Services, subject to COI-specific logical of physical segregation requirements.

(16) NATO Secure Voice Services shall support multiple COIs, in turn transported by the corresponding instances of Coloured Cloud Network Services.

(17) NATO Secure Voice Services shall integrate with ESMS.

(18) NATO Secure Voice Services shall support the authentication of NATO Enterprise users, through the integration with the NPKI capability.

(19) NATO Secure Voice services shall support the registration of users using their NATO Enterprise credentials, through the integration with the NEDS (NATO Enterprise Directory System) capabilities.

e. NATO Enterprise CIS Provider shall deliver Studio VTC Services, available to all of its users.

(1) NATO Enterprise CIS Provider shall provide VTC Studio equipment according to people-based room configurations outlined in the service catalogue.

(2) NATO Studio VTC Services shall support multi-user collaboration through video and audio.

(3) NATO Studio VTC Services shall support multi-location collaboration through video and audio.

(4) NATO Studio VTC Services shall support conferences involving up to 1000 high-definition endpoints.

(5) NATO Studio VTC Services shall support up to 1000 high-definition end-points operating simultaneously over multiple conferences.

(6) NATO Studio VTC Services shall support up to 1000 high-definition simultaneous conferences.

(7) NATO Enterprise CIS Provider shall physically segregate Studio VTC services from the data infrastructure.

(8) NATO Studio VTC services shall support unclassified and secure VTC connectivity from selected rooms, through separate NU and NS VTC end-points.

(9) NATO Studio VTC Services shall provide a minimum set of features that include: scheduling, VIP monitoring, conferencing, recording, playback and streaming.

(10) NATO Studio VTC Services shall allow ad-hoc user initiated sessions without requiring centralised coordination/administration.

(11) NATO Studio VTC services shall provide software for OS platforms in use in NATO.

(12) NATO Studio VTC services shall run over platform-independent software clients, including web-based applications.

(13) NATO Studio VTC services shall be capable of limiting the number of connected high definition end-points below the quantities listed above, through connection admission control mechanisms.

(14) NATO Studio VTC Services shall support priority-based pre-emption of ongoing calls, when all the capacity allocated through connection admission control mechanisms is already maxed out.

(15) The Service Provider shall resolve Studio VTC Services incidents above critical level within 4 hours.

(16) NATO Enterprise CIS Provider Service Provider shall control the Studio VTC Services (24/7/365).

(17) NATO Enterprise CIS Provider Service Provider shall manage the Studio VTC Services (24/7/365).

(18) NATO Studio VTC Services shall include functionality that allows sessions with external parties to be established through NATO Enterprise external gateways.

(19) NATO Studio VTC Services shall adhere to standard protocols to ensure interoperability with other VTC systems.

(20) NATO Studio VTC services shall enable integration with the Unified Communications and Collaboration (UCC) capability, which encompasses VTC services carried over the data network.

(21) NATO Studio VTC Services shall enable integration into the UCC capability.

(22) NATO VTC Studio Services shall provide desktop-based software clients to be integrated with room-based systems.

(23) NATO Studio VTC Services shall allow dial-in from unclassified voice services.

(24) NATO Studio VTC Services shall allow dial-in from secure voice services.

(25) NATO Studio VTC Services shall support the federation with the secure VTC services of Alliance Federation Participants, and implement boundary protection measures accordingly.

(26) NATO Studio VTC Services shall support the federation with the secure VTC services of Coalition Federation Partners, through the Mission Anchor Function(s).

(27) NATO Studio VTC Services shall federate with DCIS VTC Services.

(28) NATO Studio VTC Services shall provide interoperation with other video collaboration services.

(29) NATO Studio VTC Services shall integrate with ESMC.

(30) NATO Studio VTC Services shall support the authentication of NATO Enterprise users, through the integration with the NPKI capability.

(31) NATO Studio VTC Services shall support the registration of users using their NATO Enterprise credentials, through the integration with the NEDS (NATO Enterprise Directory System) capabilities.

(32) NATO Studio VTC Services shall comply with both IPv4 and IPv6 protocols for their equipment.

Enterprise Internet Capability

Internet Access Services

Internet Hosting Services

3. NATO Enterprise shall feature an Enterprise-wide Internet Access capability, available to all of its users.

a. NATO Enterprise CIS Provider shall provide centralised Internet access for all eligible NATO Enterprise entities.

b. NATO Enterprise CIS Provider shall provide Internet access services to all NATO Enterprise users through wired access capability.

c. NATO Enterprise Internet services shall provide a minimum of 3 Mbps throughput per user.

d. NATO Enterprise Internet services shall provide hosting for NATO websites.

e. NATO Enterprise Internet services shall provide Internet access scalable to increasing demand of network traffic.

f. Enterprise Internet services shall provide enough capacity for mobile users, predicting situations that most of NATO workforce might work remotely.

g. Enterprise Internet services shall provide load sharing/balancing of traffic towards one of the three main Internet entry points.

h. NATO Enterprise Internet services shall provide centralised Internet access services in Europe and North America.

i. NATO Enterprise Internet services shall provide Internet access for guest users.

j. NATO Enterprise Internet services shall connect to Tier-1 service providers.

k. Approved NATO Enterprise users shall be able to access the Internet anonymously.

l. Approved NATO Enterprise users shall be able to access the Internet unfiltered.

m. NATO Enterprise Internet services shall provide protected Internet access.

n. NATO Enterprise Internet services shall provide same Internet user experience regardless of user location in the NATO Enterprise.

o. NATO Enterprise users shall be able to access the Internet 24/7/365.

p. NATO Enterprise CIS Provider shall provide Internet access with a minimum of 99.5% availability.

q. NATO Enterprise Internet services shall provide a service desk that monitors the NATO unclassified and secured Internet (24/7/365).

r. NATO Enterprise Internet services shall provide full security suite at the entry point in the network.

s. NATO Enterprise Internet services shall provide controlled Internet access based on site categorisation (black or white list).

t. NATO Enterprise CIS Provider shall conduct Cyber Security Monitoring Services to monitor websites and email traffic.

u. NATO Enterprise Internet services shall provide secure exchange of information between internal sites (i.e. hosted in NATO data centres) and external sites (i.e. hosted in public clouds) to comply with NATO regulations.

v. NATO Enterprise Internet services shall provide boundary protection against external adversaries.

w. NATO Enterprise Internet services shall provide unified threat management capability to protect user online activity.

x. NATO Enterprise Internet services shall allow remote access to NATO Enterprise services in the Protected Business Network (PBN).

y. NATO Enterprise Internet services shall be integrated with NATO Public Key Infrastructure (NPKI).

z. NATO Enterprise Internet services shall be integrated with NATO Computer Incident Response Centre (NCIRC).

aa. NATO Enterprise Internet services shall comply with both IPv4 and IPv6 protocols and services.

bb. NATO Enterprise Internet services shall support Mobile Device Management (MDM).