RFI: RFI-ACT-SACT-24-44. INFORMATION TECHNOLOGY MODERNISATION

Reference: Q&A #1

Date of Issue: 12 JUNE 2024

The following questions were raised with respect to subject **RFI-ACT-SACT-24-44-INFORMATION TECHNOLOGY MODERNISATION.** Responses are to provide clarification.

Questions	Responses
1. Can NATO extend the deadline to this RFI for 14 calendar days/	1. Yes, HQ SACT will extend the RFI deadline until 28 June, 2024 via amendment 1 to the RFI posted on Contracting - NATO's ACT.
2. How does NATO envision implementing artificial intelligence or machine learning (AI/ML) capabilities as managed services across a NATO-Secret cloud environment? Examples include federating ML models across a distributed command network, sharing AI/ML models between NATO members and non-NATO partners, or workflow tasking and knowledge management capabilities (e.g., AI FELIX).	2. AI/ML model-sharing: NATO also envisions the ability to share AI/ML models between member nations and partners, which would enable more collaboration and knowledge-sharing. Workflow tasking: NATO envisions the ability to use AI/ML capabilities to automate and streamline workflow tasks, improving efficiency and reducing errors. Knowledge management capabilities: NATO envisions the use of AI/ML capabilities like AI FELIX to manage and organize knowledge within the cloud environment, making it easier for NATO personnel to access and use relevant information.
3. How will NATO ensure data sovereignty for NATO-Secret workloads? For example, requiring dedicated infrastructure to be located within NATO member states and data residency within NATO countries.	3. Data residency: This task will provide storage of ON-X data within a specific NATO geographic boundary preventing data flow and replication through a non-NATO region. ON-X's commercial cloud hosted global services will be configured to avoid replication of NATO data across non-NATO countries, addressing the fact that commercial cloud global services' data are being replicated across the whole world.
4. How does NATO envision data-sharing between NATO members and non-member partners, both within NATO-Secret resources and across data classification boundaries?	4. Allied Federated Services is the underlying, enabling framework, creating a layer of federated network and core services, upon which multiple Communities of Interest can operate, and involves not only the NATO Enterprise, but all the nations and Non-Federated Services.
5. How will NATO ensure operations sovereignty, such that NATO-Secret workloads can only ever be operated, managed, and observed by NATO-cleared personnel physically located within NATO member countries?	5. Regarding ON-X, background checks and personnel security clearances will be expected for all of the cloud provider personnel.
6. How will NATO ensure security of consumption monitoring and invoicing in the NATO-Secret environment?	6. Establish centralized cost management and billing platform for cloud services4: This task will deliver a cost Management + Billing platform that will provide analysis, management, and optimization the costs of ON-X cloud workloads. This platform will use the Enterprise to take advantage of the benefits provided by the cloud while rationalising cost and providing transparent costing of services. Billing tool will

	provide the centralized Enterprise wide invoicing capability for the commercial cloud services specific for each of the sites. Together with the billing tool, the cost management tool will enable reporting, monitoring, forecasting and analysis of a site's or the whole Enterprise's cost and usage patterns of commercial cloud services with advanced analytics. In addition, this platform will bring NATO the flexibility (Through dynamic pricing / SLA capability) to allow cloud pricing to fluctuate based on market pricing. The FinOps function group will monitor and operate this platform. Except CSP baseline SLAs, which are fixed in cost, FINOPS will avoid underutilization of cloud services by prevention of static costing SLAs. FinOps will provide a cost control mechanism to supervise service managers by manually or automatically shutting down/decommissioning services that are not needed/used anymore.
7. How does NATO envision deploying NATO-Secret cloud resources to the tactical edge, to enable distributed mission command? For example, what cloud resources should be available on NATO Enhanced, Standard, and Remote Nodes?	7.Not yet determined, is subject for internal analysis
8. How does NATO envision Enhanced, Standard, and Remote Nodes to operate in a distributed mission command, or Denied, Disrupted, Intermittent, and Limited (DDIL) communications environment?	8. NATO envisions Enhanced, Standard, and Remote Nodes to operate in a distributed mission command, or Denied, Disrupted, Intermittent, and Limited (DDIL) communications environment by utilizing a variety of technologies and techniques. Enhanced Nodes are designed to provide the highest level of connectivity and redundancy, and can operate in a variety of environments including DDIL. They are typically used in fixed locations or as part of a larger network infrastructure. Standard Nodes are designed to provide reliable connectivity in a variety of environments, but may not have the same level of redundancy as Enhanced Nodes. They are typically used in mobile or tactical environments where portability is important. Remote Nodes are designed to provide connectivity in remote or austere environments where infrastructure is limited or non-existent. They are typically used in expeditionary or special operations environments. To operate in a DDIL communications environment, NATO employs a variety of techniques such as adaptive networking, dynamic spectrum management, and advanced encryption. These technologies help to ensure that critical communications can be maintained even in the face of disruptions or interference. **NOTE: ON-X looks to restructure this concept but what that concept looks like is unknown at this time.**

9. How will NATO ensure supply chain security for its NATO-Secret infrastructure? For example, hardware that does not originate (sourced or produced) from adversary nations?	9. NATO polices are currently being established to address supply chain security.
10. How will NATO ensure supply chain security of the underlying source code of its NATO-Secret cloud environment? For example, relying upon cloud service providers that have clouds in adversary nations and may have previously shared source code, detailed design documents, and other compromising cloud platform information with adversary nations?	10. NATO polices are currently being established to address source code sharing / review.
11. How will NATO ensure its NATO-Secret cloud environment includes the same services on an on-going basis as the corresponding commercial cloud offerings?	11. NATO-Secret cloud services are based on operational requirements that are continually assessed. These requirements may necessitate more or less services than commercial cloud offerings.
12. How will NATO ensure its NATO-Secret cloud environment is mission-ready as soon as possible; for example, would NATO want mission-ready NATO-Secret cloud capabilities as soon as 2026?	12. Not yet determined, is subject for internal analysis at this point.
13. To ensure NATO's Secret-level cloud environment receives timely continuous innovation and security updates, what are NATO's cross-domain solution (CDS) design requirements?	13. Not yet determined, is subject for internal analysis at this point.
14. What security governance and compliance frameworks does NATO require for its NATO-Secret cloud solution?	14. NS Cloud directive discussions are currently underway, but there is no set directive for this classification network level at this point. There is governance of NS on-premises capabilities.
15. Why is the RFI referring to nations bidding? Is this a reference to where the provider my host their capability from a particular region?	15. NATO has various measures in place to ensure data sovereignty for NATO-Secret workloads. One such measure is requiring dedicated infrastructure to be located within NATO member states. This means that any infrastructure used for NATO-Secret workloads must be physically located within a NATO member state to ensure that the data is subject to NATO's jurisdiction and control. Additionally, data residency within NATO countries is also required to ensure that the data is subject to NATO's legal and regulatory framework. This helps to ensure that NATO-Secret workloads remain secure and protected from unauthorized access or compromise.
16. What software or applications does NATO envision consuming on the NATO-Secret platform?	16. Not yet determined, is subject for internal analysis at this point.
17. How will NATO ensure the infrastructure underlying its NATO-Secret workloads cannot be re-tasked to non-NATO cloud customers?	17. As the provider of future services, we expect the provider to answer this question and make recommendations for a solution.

18. How will NATO ensure mission-readiness of its NATO-Secret infrastructure in terms of service level agreements (SLAs), including manageability, performance, and availability of NATO-Secret resources?	18. NATO is constantly working towards ensuring that its NATO-Secret cloud environment is mission-ready as soon as possible. To achieve this goal, NATO is investing in various initiatives and programs to enhance its cloud capabilities. For instance, NATO is leveraging advanced technologies such as AI, machine learning, and automation to improve the speed and efficiency of its cloud services. Moreover, NATO is collaborating with industry partners and member countries to develop and deploy cutting-edge cloud solutions that meet its mission requirements. NATO is also conducting regular assessments and testing of its cloud environment to ensure that it is secure, reliable, and resilient.
19. How will NATO ensure its NATO-Secret data is always encrypted, both at-rest and in-transit, and in such a way that NATO-Secret cloud users cannot switch off encryption?	19. In accordance with AC/322-D(2021)0032. NATO directs that data is always encrypted.
20. How will NATO ensure that new services are made available in the NATO-Secret cloud environment, within a specified amount of time after release into public-commercial cloud offerings?	20. As the provider of future services we expect the provider to answer this question.
21. How will NATO ensure a seamless and uniform cloud environment from its core NATO-Secret cloud infrastructure across the ~100 ON-X sites?	21. As the provider of future services we expect the provider to answer this question.
22. How will NATO ensure its NATO-Secret cloud service provider enable an open-architecture ecosystem where system integrators and independent software vendors can rapidly deploy capabilities to the NATO-Secret core cloud and ON-X environment?	22. Current and future STANAGS provide guidance to prevent vendor lock in and support the use of open architecture standards.
23. Will this project require: Optimization of integration with many IT systems and/ or solutions?	23. ON network will require optimization integration with multiple community of interest functional area of interest, which will need to be cloud ready.
24. Will this project require: Exchanging data between different mediums, while unifying communication channels?	24. Yes, but it depends on use case scenarios. The vendor should expound on CDS capabilities.
25. Will this project require: Managing the distributed IT infrastructure covering network, technical services and processes?	25. Yes, the vendor should expound on SMC capabilities.
26. Will this project require: Optimization of complex procedures that require the cooperation of many systems?	26. Yes, the vendor should expound on orchestration integrated into workflows.
27. Will this project require: Automation of technical configuration procedures and operations covering repetitive, trivial actions, which distract a highly qualified employee from more important tasks?	27. Yes, “as code” services will form the basis for service provisioning.

28. Will this project require: Assuming that the solutions we would like to propose to NATO cover some parts of the requirements, should we answer all the questions mentioned in Annex A or only those that correspond to the proposed solutions?	28. Answer all question in Annex A and any recommendation that would enhance the project.
29. Will this project require: Can you briefly list the types of IT systems that should be moved to the cloud and the relations between them?	29. Not yet determined, is subject for internal analysis at this point, and pending cloud readiness assessment results.
30. What are the specific interoperability standards that proposed systems must meet to ensure seamless integration across various NATO operations and member nations?	30. NATO has established specific interoperability standards that proposed systems must meet to ensure seamless integration across various NATO operations and member nations. These standards are intended to ensure that NATO forces and member nations can communicate and collaborate effectively and efficiently in a variety of scenarios. Some of the specific interoperability standards that proposed systems must meet include: NATO Standardization Agreements (STANAGs): These are technical standards that define common procedures, protocols, and interfaces for communication and information exchange between NATO forces and member nations. Joint Tactical Data Link (JTD): These are a set of standardized data links that enable real-time communication and data exchange between NATO forces and member nations. Common Operational Picture (COP): This refers to a shared view of the operational environment that provides situational awareness to NATO forces and member nations. Proposed systems must be able to integrate with the COP to ensure seamless communication and collaboration. Multinational Interoperability Council (MIC) standards: These are technical standards developed by the MIC to promote interoperability between NATO forces and member nations. Security standards: Proposed systems must meet NATO's security standards to ensure that they are secure and can protect against cyber threats and other security risks. Federated Mission Networking (FMN) is a governed conceptual framework consisting of people, processes and technology to plan, prepare, establish, use and terminate Mission Networks in support of federated operations.
31. What configurations and deployment models (e.g., private, public, hybrid, multi-cloud) are preferred for the NATO ITM project? Are there specific cloud service providers that have already been vetted or considered?	31. Not yet determined, but is being discussed within the NATO Enterprise Cloud Operating Model, NATO is reviewing the range of models that are compliant with security policies. Currently, NATO has existing cloud initiatives with multiple vendors, but there are no specific vetted vendors.

32. Can you specify the cybersecurity frameworks and compliance standards that the IT solutions must adhere to? How should solutions handle encryption, secure data transfer, and access control at the NATO SECRET level?	32. AC/322-D(2021)0032 offers technical implementation guidance for protection of NATO information in the Public Cloud. However, this does not address information above NATO Restricted. AC/322-D/0048-REV3 offers additional technical implementation guidance for general CIS Security at all classification levels.
33. How open is NATO to incorporating emerging technologies such as artificial intelligence, block chain, or advanced analytics into the ITM? What are the evaluation criteria for such technologies?	33. NATO is open to incorporating emerging technologies such as artificial intelligence, block chain, or advanced analytics into the ITM. The organization recognizes the potential benefits that these technologies can bring to the table, including improved efficiency, enhanced security, and better decision-making capabilities. When evaluating emerging technologies for incorporation into the ITM, NATO considers several criteria. These include: Technical feasibility: NATO evaluates the technical capabilities of the technology to ensure that it can be integrated into the ITM without causing any disruptions or compatibility issues. Security: NATO places a high priority on security and evaluates the technology's ability to meet NATO's security requirements. Cost-effectiveness: NATO considers the costs associated with the technology, including initial investment, maintenance, and operational costs, to ensure that it is cost-effective. Interoperability: NATO evaluates the technology's ability to integrate with existing systems and infrastructure within the ITM. Ethical considerations: NATO considers the ethical implications of using the technology, including issues related to privacy, data protection, and human rights.
34. Can NATO provide specific benchmarks or performance criteria that solutions need to meet during the testing phase to be considered successful?	34. Not yet determined, is subject for internal analysis at this point. Success criteria will be presented at a later date.
35. What are the testing and validation protocols for new IT systems under the ITM project?	35. NATO has a DEVSECOPS platform that is used as a test bed for a cloud environment.
36. What common problems do you regularly find yourself having with the 5.2 Satellite Infrastructure?	36. NATO's 5.2 Satellite Infrastructure faces several common problems that can impact its effectiveness and efficiency. Some of the most common problems include: Latency: The 5.2 Satellite Infrastructure may not have sufficient capability necessary for near-real time systems. Limited bandwidth: The 5.2 Satellite Infrastructure may not have sufficient bandwidth to support the growing needs of the organization. This can lead to slow performance and delays in data transfer.

	Interference: The 5.2 Satellite Infrastructure may face interference from other satellites, which can impact its ability to transmit and receive data. Equipment failure: The equipment used in the 5.2 Satellite Infrastructure may be prone to failure, which can result in downtime and delays. Security vulnerabilities: The 5.2 Satellite Infrastructure faces constant security threats from cyberattacks and other security breaches. The organization must continuously monitor and update its security protocols to protect against these threats. Weather conditions: The 5.2 Satellite Infrastructure may be impacted by adverse weather conditions, which can affect its ability to transmit and receive data.
37. What are NATO's highest priorities relating to transiting work to the next contractor? What are the biggest concerns?	37. Amongst many issues of importance, the following are key to NATO: data portability, prevention of vendor lock in, and effective, up-to-date documentation of solution delivery.
38. What is the expected timeline for RFP due date and award date?	38. TBD
39. What are NATO's biggest pain points in their current infrastructure?	39. NATO's current network infrastructure faces several pain points that can influence its effectiveness and efficiency. Some of the biggest pain points include: Lack of automation Low resilience Legacy system management Security vulnerabilities Limited bandwidth Lack of flexibility Fragmentation of networks
40. As per 3.3, what are the biggest expected challenges with all organizations adopting a unified set of tools?	40. There are several challenges that NATO may face when adopting a unified set of tools. Some of the biggest expected challenges include: Resistance to change Integration / compatibility issues Training and support Data migration Business process / workflow adaptation and automation