Acquisition Office

Boulevard Léopold III
B-1110 Brussels, Belgium

NCIA/ACQ/2025/07623
09 December 2025

Market Survey - Request for Information

SD-WAN - Requirements for Dynamic Overlay and Multi-Bearer Connectivity on NATO Deployable CIS (DCIS) Transport Network

NCI Agency Reference: MS-424320-SD-WAN

NATO Communication and Information Agency (NCIA) is seeking information from Nations and their Industry regarding the existing SD-WAN solutions including both the functional and technical specifications. Furthermore, Nations are asked to provide information regarding integration with NATO's DCIS infrastructure, meeting military-grade requirements, and innovative features that add operational resilience, security, and performance.

NCI Agency Point of Contact (POC) for this Market Survey:

Ms. Estefania Nunez, Principal Contracting Assistant,
E-mail: estefania.nunez@ncia.nato.int

NCIA/ACQ/2025/07623

NATO Communications and Information Agency

To : See Distribution List

Subject : NCIA Market Survey - Request for Information
MS-424320-SD-WAN

Reference(s) :
A. NCIA/TR/SEA/2018/02530 DCIS CUBE ARCHITECTURE DEFINITION DOCUMENT
B. FMN Spiral 6, Service Instructions for Protected Core Networking, Oct 2024
C. STANAG 5638 - Protected Core Networking (PCN) Core Specifications

1. The NCI Agency requests the assistance of the Nations and their Industry to identify potential existing solutions to identify SD-WAN solutions integrated with NATO DCIS infrastructure.

2. This Market Survey aims to apply due diligence by 'testing the market' to:

   a. Determine the relevant existing technologies and products which may provide the basis for the identification of suitable SD-WAN solutions integrated with NATO DCIS infrastructure.

   b. Identify a development strategy, while also evaluating the potential solutions available to NATO which may include "Adopt"-ing (an existing solution already in-service by Nations), commercial "Buy"-ing (acquiring a solution from industry), or a combination thereof.

3. Respondents are requested to reply via the questionnaire at Annex B. Other supporting information and documentation of current products catalogue is also welcome (technical data sheets, marketing, brochures, non-binding catalogue price lists, descriptions of existing installations, etc.).

4. The NCI Agency reference for this Market Survey Request is **MS-424320-SD-WAN**, and all correspondence and submissions concerning this matter should include this number.

5. Responses may be issued to the NCI Agency directly from Nations or from their Industry (to the staff indicated at Paragraph 8 of this Market Survey Request). Respondents are invited to carefully review the summary of requirements in Annex A to determine interest.

6. Responses shall in all cases include the name of the firm, telephone number, email address, designated Point of Contact, and a description of the capability available and its functionalities (not above NATO Unclassified). This shall include any restrictions (e.g. export controls) for direct procurement of the capability by the NCIA.

7. Responses are requested to reach the NCI Agency no later than by **12:00 Brussels** time on **31.01.2026.**

NCIA/ACQ/2025/07623

8. Please send all responses via email to the following NCI Agency Point of Contact:

To Attention of:	Ms. Estefania Nunez, Principal Contracting Assistant,
E-mail:	estefania.nunez@ncia.nato.int

9. Meetings with industry may take place only following the submission of responses, with the purpose of clarifying or further augmenting those responses where required.

10. This Request for Information (RFI) does not constitute a commitment to issue a future request for proposal (RFP).

11. Note that this RFI is not a formal request for submissions as part of an active procurement; but rather a general request intended to determine whether any possible solutions exist that should be considered or included in evaluating the options as part of the system requirements development for future procurements.

12. Respondents are requested to await further instructions after submission of their responses regarding any potential future bidding process, and are requested to contact only the NCIA POC identified above in Paragraph 8 above with any further requests for information or clarification.

13. Any response to this request shall be provided on a voluntary basis. Responses to this request will help identifying and selecting firms eligible for any future procurement that may arise from this Market Survey. The result of this Market Survey might be used for selecting purpose.

14. In accordance with the NATO Management of Non-Classified NATO Information policy (C-M(2002)60), this **MS-424320-SD-WAN** shall not be published on the internet.

15. Responses to this request, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as informational only and will not be construed as binding on NATO for any future acquisition.

16. The NCIA is not liable for any expenses incurred by firms in conjunction with their responses to this Market Survey, and this Survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

17. Your assistance/participation in this Market Survey request is greatly appreciated.

FOR THE CHIEF OF ACQUISITION:

Estefania Nunez

Digitally signed by Estefania Nunez
Date: 2025.12.09 16:12:00 +01'00'

Estefania Nunez

Principal Contracting Assistant

NCIA/ACQ/2025/07623

Enclosures :

Annex A: Summary of Requirements

Annex B: Questionnaire

Annex C: Distribution List

Annex D: Potential Industrial Suppliers

Annex A

Requirements Summary

Technical Architecture and Capabilities

The technical architecture of NATO's DCIS is an advanced interoperability of a number of communications technologies running in a variety of operational environments. The DCIS infrastructure sets a wide range of communications services including IP routing and switching, multimedia services for voice and video transport, and varied transmission technologies bound both wireline and wireless systems, Line of Sight (LOS) and Beyond Line of Sight (BLOS) capabilities. The system's infrastructure services deliver critical business support functions and military applications accessed through or hosted on the DCIS network. Another important characteristic of DCIS is that it is Federated Mission Networking (FMN)-aligned to promote interoperability across NATO and national systems to support effective communication across operations, missions, and exercises.

The Need for SD-WAN in NATO's DCIS Infrastructure

NATO Deployable Communications and Information System (DCIS) is trying to ensure secure, stable, and high-performance communications in increasingly complex operating environments. Software-Defined Wide Area Network (SD-WAN) technology adoption in DCIS has become essential since NATO expeditionary operations necessitate greater network agility, enhanced security, and bandwidth optimization within distributed deployment settings. The current DCIS architecture, while functioning, cannot adequately respond to the intense growth in data traffic because of multiple heterogeneous transmission bearers (PACE model), multimedia communications, and real-time sharing of intelligence between coalition forces. SD-WAN's ability to form virtual network overlays concealing the underlying connections would provide DCIS with very much improved traffic management capabilities enabling dynamic routing of mission-critical communications over available transport means. This is particularly significant to NATO's forward-deployed forces that have to operate in areas of degraded or contested network environment, where continuity of Command-and-Control communications is paramount to the success of operations.

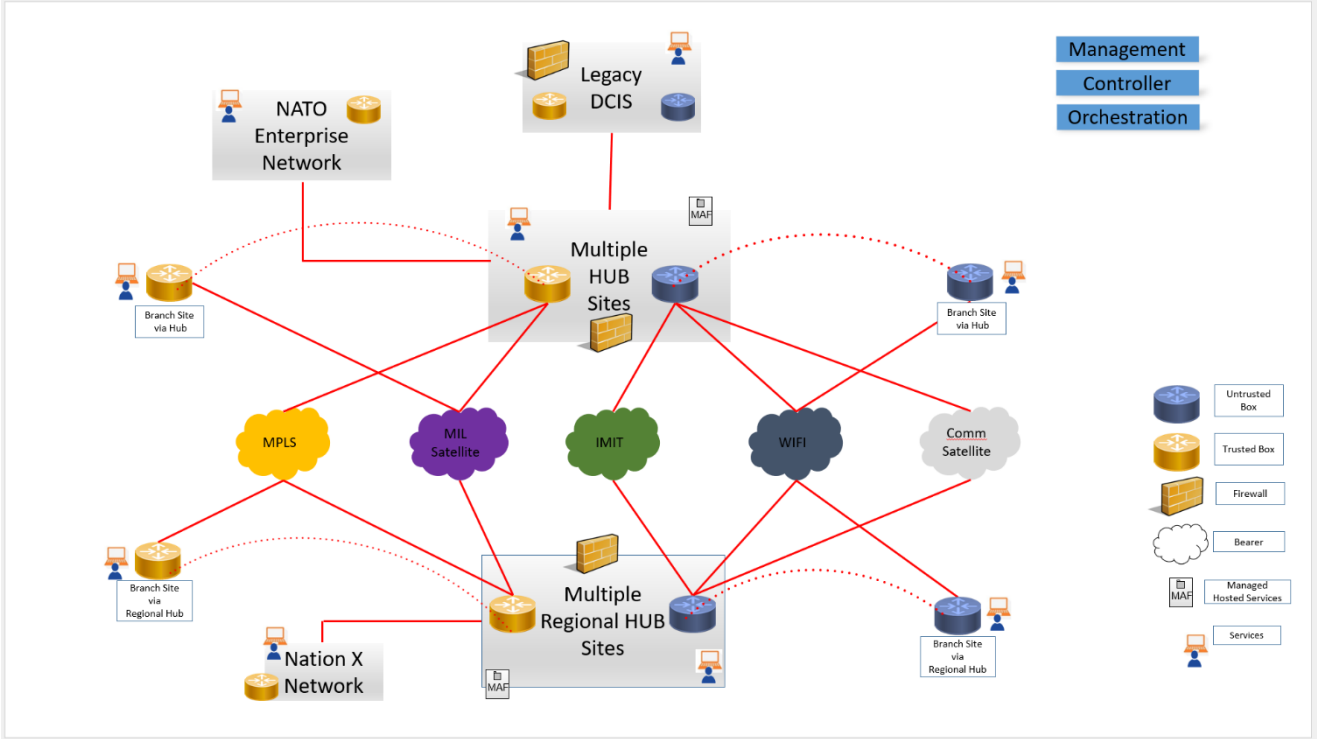
Greater Operational Capabilities by SD-WAN

SD-WAN technology offers DCIS significant performance enhancements directly translated to greater operational capabilities. With intelligent traffic steering and bandwidth shaping, SD-WAN can prioritize mission-critical applications for best-available network resources, guaranteeing Quality of Service even during tough network conditions. The fact that the technology can detect automatically in milliseconds any outages and redirect traffic as needed is invaluable network resiliency for NATO operations in contested environments. Further, SD-WAN enables the aggregation of several paths of communication - e.g., satellite, cellular, and terrestrial networks - into redundant connectivity paths that significantly enhance overall network dependability. This multi-path feature is particularly valuable for NATO's expeditionary forces, which must maintain constant communications across diverse geographic areas while being vulnerable to potential jamming or interference by the adversary Scope of Information Requested.

NCIA/ACQ/2025/07623

SD-WAN Conceptual Topology

The diagram below illustrates a conceptual SD-WAN topology for reference purposes only. This conceptual architecture is intentionally non-prescriptive and does not bind vendors to any specific design approach or implementation.



Within the Transmission layer, two fundamental elements are defined:

- An Untrusted Box (ETM) for Internet-of-opportunity bearers
- A Trusted Box (PCA) for managed bearers

Vendors have full flexibility in their proposed architecture, including the option to introduce additional SD-WAN overlay networks, modify the illustrated boxes, or propose alternative designs that incorporate these transmission elements. The diagram serves solely as a discussion framework to facilitate understanding of the integration requirements with NATO's DCIS infrastructure and the general solution objectives.

The requested information in this RFI must cover both the functional and technical abilities of your SD-WAN solution. Furthermore, please provide information regarding integration with NATO's DCIS infrastructure, meeting military-grade requirements, and innovative features that add operational resilience, security, and performance.

NCIA/ACQ/2025/07623

Annex B

Questionnaire

Organisation Name :

Contact name & details within organisation:

Notes

- Please **DO NOT** alter the formatting. If you need additional space to complete your text then please use a 'Continuation Sheet' which you can append at the end of this Annex and please reference the question to which the text relates to.
- Please feel free to make assumptions, *HOWEVER* you must list your assumptions in the spaces provided.
- Please **DO NOT** enter any company marketing or sales material as part of your answers within this market survey. But please **DO** submit such material as enclosures with the appropriate references within your replies. If you need additional space, please use the sheet at the end of this Annex.
- Please **DO** try and answer the relevant questions as comprehensively as possible.
- All questions within this document should be answered in conjunction with the summary of requirements in Annex B.
- All questions apply to Commercial or Government responders as appropriate to their Commercial off the Shelf (COTS) or Government off the Shelf (GOTS) products.
- Cost details required in the questions refer to Rough Order of Magnitude (ROM) Procurement & Life Cycle cost, including all assumptions the estimate is based upon:
  - Advantages & disadvantages of your product/solution/organisation,
  - Any other supporting information you may deem necessary including any assumptions relied upon.

Questions

Please provide detailed responses to the following questions:

1) Dynamic Overlay Network

How does your SD-WAN solution manage the dynamic overlay network information? In other words, how do you share connectivity, policy, and routing information between edge devices and central controllers?

2) Overlay Fabric

How your solution builds and sustains an overlay fabric? We'd like to know how it builds a secure, dynamic, and scalable network layer that enforces policy consistently and optimizes routing across distributed nodes?

3) Integration with Geo Satellite Bearers

a) How the SD-WAN solution overcomes latency, signal variability, and network interruption inherent in satellite communication?

b) Provide use cases for remote or unreachable locations where satellite connectivity is mission-critical.

4) MEO/LEO Satellite Connectivity

a) How Medium Earth Orbit (MEO) and Low Earth Orbit (LEO) satellites can be combined with the SD-WAN solution to maximize the network coverage and reduce latency?

b) Address use cases for remote or mobile use cases where MEO/LEO satellites deliver stable connectivity, and how challenges such as dynamic routing and signal instability can be addressed.

5) xG/5G Connectivity:

a) Does your solution provide interfaces to enable connectivity via ITU IMT based 4G/5G? Kindly describe the precise mobile connectivity features, how these interfaces are integrated into your SD-WAN solution.

b) Give scenarios where 4G/5G networks serve as primary connectivity, especially in mobile or temporary deployments.

c) Explain how your solution addresses possible concerns like handoff between networks and maintaining quality of service consistency.

d) Does your solution optimize the use of 4G/5G connectivity in dual-WAN setups, given its inherent limitations such as throttling? How does your system ensure that 4G/5G - designed for bursty, low-volume data transfers - is maintained as a backup transport, only activated when the primary WAN link fails, to prevent unnecessary charges and optimal performance?

e) Does your SD-WAN product guarantee backup WAN connectivity through cellular networks as a fall-back method? Exactly how does your system determine that all primary overlay tunnels across wired WAN links are down and, subsequently, activate a local cellular interface as a fall-back?

6) Dynamic Path Selection and Traffic Steering

a) Does your solution intelligently steer traffic over different bearers (e.g., MPLS, broadband, satellite, 4G/5G) based on real-time network conditions?

b) Does your solution ensure that business-critical applications always take the best path considering factors like latency, jitter, and packet loss?

7) Handling Latency Variation among Bearers

a) How does your solution manage large disparities in latency between transport types (e.g., satellite vs. Fiber) without affecting application performance?

b) Does your solution provide techniques such as packet/stream level Forward Error Correction (FEC), jitter buffering, and TCP optimization for providing seamless user experiences.

8) Interruption of Underlay Network Connectivity

Does your SD-WAN solution react to underlay connectivity breaks to the Hub/Regional Hub? Explain how these breaks are detected, what failover processes are followed, and what redundancy measures are taken in an effort to maintain the network in operation and functional availability during these events.

9) Loss of Controller Connectivity

a) What is the behaviour of your SD-WAN solution in cases where connectivity to the controllers is completely lost? Outline the fullback processes, local decision-making strategies, and redundancy mechanisms in place to ensure network performance and maintain operational continuity when the controllers are unavailable.

b) What is the duration that SD-WAN ecosystem supports for a disconnected node to remain operational and manageable until joining back to the SD-WAN?

10) Dual Transport Domains (Trusted vs. Untrusted Bearers)

a) Describe architectural designs that segregate bearers in to a trusted and untrusted solution.

b) How do you address security policies, performance isolation, and failover between the two domains?

11) Controller Deployment Mode

a) Could you please explain your controller deployment strategy? We are interested in knowing whether your solution supports both centralized and distributed controller topologies, and how you provide scalability, redundancy, and failover.

b) Can you provide details regarding the process of configuration management and interoperability with other network devices? This will allow us to assess how well controllers can be deployed, upgraded, and scaled in our production environment.

NCIA/ACQ/2025/07623

12) AI/ML Features for Predictive Analytics and Automated troubleshooting

a) Provide in-depth explanation of how your solution leverages innovation AI/ML for predictive analytics and automated troubleshooting. Specifically, we are interested in understanding how your system uses AI/ML algorithms to forecast potential network issues, optimize performance, and reduce downtime.

b) Additionally, outline the data inputs, model training processes, decision models, and any mechanisms for continuous improvement and integration with existing network management systems. This understanding will enable us to evaluate the proactive capability of your solution in managing and mitigating network problems.

13) SD-WAN in Deployable and High Mobility Environments

a) Provide use cases for rapidly deployable networks in emergency, military, or event settings.

b) Does your solution maintain stability and performance under constantly changing network conditions?

14) Management and Orchestration

a) How do you ensure centralized management features to monitor and improving performance in real-time over different bearers?

b) Automation and policy management for integrating different transport types in a seamless fashion.

15) Routing Protocols Support

Can you list the routing protocols your solution accommodates?

16) TCP Sequence Synchronization across Bearers with Different Latency

a) Does the SD-WAN solution keep TCP sequence numbers in sync when traffic is divided across a number of bearers with dissimilar latency profiles?

b) Do you use techniques such as buffering, sequence number mapping, or sync algorithms that are employed to realign packets that arrive out of order due to latency differences?

c) Provide details on the impact of these techniques on maintaining stable layer 3 cryptographic protocols in the presence of heterogeneous network environments.

d) The Multiple Sequence Number Space (MSNS) feature addresses the issue of packet delivery out of order due to Quality of Service (QoS) mechanisms like Low Latency Queuing (LLQ), which can cause IPsec replay failures. By mapping different sequence number spaces to different QoS traffic classes for a given SA, MSNS helps in maintaining the integrity of the data stream. How does your SD-WAN solution implement anti-replay protections within its IPsec framework? Additionally, please explain how your solution supports multi-SNS configurations, including any mechanisms or features that ensure secure and efficient management of multiple security networks or service segments.

17) Certificate-Based Encryption for All Tunnel Types

a) Do you use certificate-based encryption for various tunnel types (VPN, IPsec, SSL/TLS) within the SD-WAN solution.

b) Do you use certificate-based encryption in support of Enterprise PKI option, revocation, and renewal in dynamic multi-bearer settings?

18) Traffic Flow Confidentiality (TFC)

a) What are your ways to maintain confidentiality of traffic flow patterns to keep sensitive information such as packet sizes and timing concealed?

b) Do you use techniques like traffic padding, header encryption, and obfuscation methods to resist traffic analysis attacks?

19) Controllerless SD-WAN Architecture

a) Do you use controllerless design model that doesn't need a control plane, and possibly reduce single points of failure?

b) How your controllerless solution interacts with other management and orchestration platforms to ensure seamless operation under dynamic network conditions?

20) Application Experience Assurance

a) Please explain mechanisms to manage real-time monitoring and optimization of the end-user experience of data across the network. This involves collecting and analysing some of the most important performance indicators - such as latency, jitter, packet loss, and throughput - to see how data flows are running across the network in real time. Ideally by tracking these measures, the system can dynamically reallocate traffic management policy, prioritize mission-critical applications DSCP based, and even redirect traffic to avert performance degradation. This ensures that regardless of the underlying technology, the network delivers high performance and reliability for mission-critical applications and actionable intelligence for proactive optimization.

21) Bidirectional Forwarding Detection (BFD)

a) What are the Fast link failure detection mechanisms used and how BFD is integrated to ensure high availability?

22) Quality of Service (QoS)

a) Describe if traffic prioritization is addressed by the solution and how it ensures predictable performance across several links.

b) Does your SD-WAN solution ensure consistent Quality of Service across an SD-WAN deployment with heterogeneous transmission bearers

23) Forward Error Correction (FEC)

Describe the proactive error correction techniques used to maintain data integrity.

24) Packet Duplication

Identify if and how the solution makes use of packet duplication to improve reliability without incurring unnecessary overhead.

25) Fragmentation Avoidance

Describe techniques for avoiding packet fragmentation, which has a detrimental impact on throughput and performance.

26) Intelligent Application Routing

Describe techniques for directing network traffic that is founded on real-time application performance and network conditions (DSCP based). By monitoring each application's specific needs and the real-time performance of the links, this system streamlines the process of path selection to deliver minimum latency and maximum throughput, and therefore the optimal overall user experience.

27) TCP Flow Optimization

What evaluating techniques to optimize TCP flows across a number of transport media of varying latency profiles do you use?

28) Local Internet Breakout for SD-WAN

Can you explain how your SD-WAN solution supports local internet breakout? We are interested in learning about how your approach improves the user experience for SaaS applications in remote sites by eliminating performance degradations with regards to backhauling internet traffic to primary data centres and how it allows granular control of internet access on a per-VPN or per-site level.

29) Topology Control via Constrained Transport Classes

Describe how your solution facilitates topology control by limiting the use of specific transport classifications. How it allows operators to define and enforce policies such only specific allowed transport types are enforced on certain flows of traffic in order to maximize performance and security?

30) Hub-and-Spoke with Restricted Direct Spoke Connectivity

Would you explain how your solution enforces a hub-and-spoke topology with restricted direct tunnels among spoke nodes? How does it ensure that all inter-spoke communications are routed through the defined hub to maintain centralized control, enhance security, and optimize performance?

31) Hub/Regional Hub and Spoke Deployment with Restricted Direct Spoke Connectivity

Can you clarify if your solution supports a hub-and-spoke deployment that includes central and regional hubs? More specifically, how does it restrict direct spoke-to-spoke tunnels such that all inter-spoke traffic is off-routed via the assigned hubs and regional hubs? Further, does your system support dynamic establishment and management of hub and regional hub nodes for optimizing traffic flows?

32) Dynamic End-To-End Path Tracking

Does your solution support dynamic end-to-end path tracking for traffic engineering? Can you define the centralized control policies, routing mechanisms, and continuous monitoring processes that support the dynamic redirecting and ensure the preferred traffic path is maintained?

33) Dynamic Service Chaining

Does your solution provide for dynamic service chaining? How exactly does your solution dynamically position services such as firewalls, intrusion prevention, web proxies, load balancers, caching engines, or WAN optimizers along the data path per predefined policy? We would be interested to understand how your solution automatically advertises and orchestrates such services in the WAN.

34) Leaking in SD-WAN

Can you explain if your solution enables controlled and selective redistribution of routing information between isolated network segments or routing domains without compromising security and centralized policy control?

35) Per VPN Topologies

Can you explain if your solution supports per-VPN topologies? More significantly, does it allow each VPN to have its own independent network topology in such a way that different service VPNs take different paths in the network?

36) Dynamic On-Demand Tunnel for Direct Spoke-to-Spoke Connectivity

Could you describe if your solution provides on-demand tunnel creation for low-latency direct connectivity between remote sites? Does your system, within a hub-and-spoke architecture, determine spoke-to-spoke traffic and dynamically establish temporary secure tunnels to improve performance similar to dynamic multipoint VPN processes?

37) Application-Based Traffic Engineering and Prioritization

Does your solution enable application-based traffic engineering—otherwise referred to as application pinning - to deploy centralized data policies (DSCP based)? Does your architecture differentiate business-critical versus non-critical applications in dual-WAN environments, such as routing non-critical traffic over a best-effort Internet connection while routing business-critical traffic over a link with a guaranteed SLA? Also, what are the methods non-critical traffic is shed on an Internet link failure in order to prevent oversubscription? Does your solution ensure business-critical applications can fail over to backup transports uninterruptedly when the primary link is failed?

38) Resilient High Availability and Seamless Failover

Does your solution assure high availability in an SD-WAN deployment? Does it detect failures, ensure seamless failover across redundant elements or paths, and maintain session continuity and performance? Also, please specify the mechanisms - e.g., active-active or active-standby configuration, multi-path redundancy, and

centralized policy management - that are employed to minimize downtime and enable uninterruptible service delivery.

39) Hierarchical SDWAN Region based Architecture

Does your solution support a hierarchical SD-WAN architecture that segments the WAN into independent regions?

40) Seamless Integration with Legacy Branch Networks

Does your solution facilitate connectivity to legacy, non-SD-WAN branch networks? Specifically, does it get these legacy sites integrated into the centralized SD-WAN architecture in order to leverage unified management, consistent policy control, and assured communication across the entire network?

41) Multiple Hub/Regional Hub Scenario

Describe whether your solution supports multiple hub deployments, and regional hub scenarios? Does it handle connectivity, failover, and centralized policy enforcement between the central and regional hubs for integrated and best possible performance?

42) Maritime Use Case

Can you describe in some detail how your solution addresses the special challenges of SD-WAN deployment in sea environments, on ships? Describe the failover and centralized management procedures that you have put in place to ensure continued, fault-tolerant operation in these demanding environments?

43) Management of unstable links

a) Inadequate Bandwidth Aggregation:

i) Does your SD-WAN solution aggregate bandwidth from multiple internet links?

ii) Is your solution doing actual bonding of multiple links for increased throughput, or is it just load balancing?

iii) What WAN Optimization techniques (e.g., compression, deduplication, caching) does your solution offer to increase bandwidth efficiency?

iv) Can your SD-WAN dynamically spread traffic based on real-time bandwidth availability rather than fixed policies?

b) Inadequate Path Selection:

i) Does your SD-WAN choose what the optimum path for per traffic type?

ii) Has your solution AI-based path selection or manually tuned?

iii) Can path selection rules be customized by user-specifically traffic in line with application priority needs (e.g., VoIP prefers low jitter, file transfer prefers high bandwidth)?

iv) Does your SD-WAN handle asymmetric routing and path restoration if a link is impaired but not down?

v) Does your solution allow per-application path scoring over a one-size-fits-all approach?

c) Poor User Experience for Mission-Critical Applications:

i) Does your SD-WAN prioritize critical apps over normal traffic?

ii) Does your solution use application-aware QoS with per-app bandwidth guarantees?

iii) Can policies dynamically be modified based on real-time network activity?

iv) Does your SD-WAN provide integration with SaaS apps (e.g., Microsoft 365, Zoom, Google Workspace) for cloud-based prioritization?

v) How congestion avoidance mechanism handling SD-WAN topology when all links are saturated?

d) Limited ISP Control:

i) Does your SD-WAN ensure consistent performance when leveraging best-effort internet links?

ii) Can your product dynamically monitor the performance of the ISPs and transition to a failover provider?

iii) Does your SD-WAN include cloud-based monitoring or third-party monitoring tool integration (e.g., Thousand Eyes,)?

44) SD-WAN Processing of Encrypted Traffic

a) Traffic Identification & Classification:

i) Does your SD-WAN solution classify and identify encrypted traffic (e.g., TLS, SSL, IPsec, HTTPS) for application-aware routing and QoS?

ii) Can your SD-WAN inspect encrypted traffic without decrypting it (e.g., through metadata analysis, DPI, or SNI inspection)?

b) Performance & Optimization of Encrypted Traffic:

i) What techniques does your SD-WAN use to maximize encrypted traffic (e.g., compression, deduplication, TCP optimization) without decrypting it?

ii) Does SD-WAN handle MTU size discrepancies and fragmentation of encrypted traffic in order to prevent performance loss?

c) IPsec VPN & Tunnel Security:

i) Does your SD-WAN support encrypted site-to-site VPN tunnels over multiple transport links?

ii) Does your SD-WAN support IPsec tunnel bonding for high availability and failover?

iii) Can encrypted tunnels be dynamically recreated without session drop in the event of a link failure?

iv) Which encryption standards does your SD-WAN solution support for IPsec tunnels (AES-256 CGM, Suite B, Post-Quantum Cryptography)?

d) Impact of Encryption on SD-WAN Performance:

i) Does your SD-WAN deal with CPU and memory usage when processing encrypted traffic?

ii) What is the impact of encrypted traffic on SD-WAN throughput. Are there performance benchmarks?

45) Customer Success Stories and Case Studies for Comparable Applications

a) Please present some comparable customer success stories as well as case studies illustrating how your solution has been effectively applied in scenarios comparable to our use cases? We are particularly keen on learning about measurable benefits achieved, key challenges addressed, and any specific results or measurements that pinpoint the impact of your solution.

b) Further, provide us with details on methods used, customer comments, and any lessons learned which could be applied to our setting.

46) Pricing Models

a) Please provide detailed information regarding the pricing models of your solution. We would appreciate knowing about the various pricing options offered (e.g., subscription-based, usage-based, one-time licensing, etc.) and how these models correspond to various customer sizes or deployment scales.

b) Could you provide details on any bulk/enterprise discounts, support fees, and terms of service, and provide examples of pricing structures for typical use cases? This will allow us to review the overall cost-effectiveness and scalability of your solution.

47) Authorized Access Control for New SD-WAN Router Integration:

How does your SD-WAN solution control and manage approved access to the SD-WAN fabric when adding a new SD-WAN router? Describe the authentication, role-based access control, and audit logging processes in place to guarantee that only approved devices can join and communicate with the network fabric, thus ensuring its security and integrity.

48) Controller Scalability and Regional Hub Resiliency

a) Is your SD-WAN solution capable of supporting the installation of an additional controller at each regional hub for purposes of resiliency? Please provide further information on how the solution can support multiple controllers, including procedures for controller coordination, failover management.

b) Describe how the SD-WAN fabric in the Regional Hub region behaves when connectivity to the Hub is lost.

49) IPv6 Capability

a) Does the proposed SD-WAN solution provide full dual-stack (IPv4/IPv6) capability for control, management, and data planes?

b) Can the SD-WAN overlay operate natively over IPv6 transport under both static and dynamic routing?

c) Does the system support IPv6 route-advertisement, summarization, and redistribution between overlay and underlay domains?

d) Can IPv6 routes participate in path-quality measurements (loss, latency, jitter) like IPv4?

50) RIPng Capability to Support E-Node Capability

a) Does the SD-WAN solution support RIPng for dynamic routing within the overlay or in the non- SDWAN interfaces?

b) Is route redistribution supported between RIPng of the non-SDWAN interface to SDWAN Control Plane?

c) Can RIPng routing information be monitored through the SD-WAN management?

d) Can you describe how the RIPng – Auto Configuration is working in a non-SDWAN interface of your SDWAN Solution?

d) Can the solution automatically discover and form RIPng and GRE adjacencies without manual configuration?

e) Is there a mechanism to limit or control RIPng auto-discovery (e.g., interface whitelists, policy-based routing)?

51) Color Cloud – Bearer Change Detection & Capacity Adaptation

a) Describe how your solution enables the Colour Cloud (CC) node (CC connects as a service to SDWAN box via military grade encryption) to detect a change of bearer in SDWAN Transport router.

b) Which control or telemetry mechanisms are used to signal bearer change events toward the CC (e.g., BFD, SLA probes, controller API, event subscription)?

c) Describe any testing procedure or available best practices for simulating bearer transitions and verifying CC adaptive behaviour.

NCIA/ACQ/2025/07623

Please feel free to add any information you may think that may be of value to NCI Agency in the space provided below. Should you need additional space, please copy this page and continue with the appropriate page numbers.	Page __ Of __

NCIA/ACQ/2025/07623

Annex C

Distribution List for Market Survey

MS-424320-SD-WAN

NATO Delegations (Attn: Investment Committee Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czechia	1
Denmark	1
Estonia	1
Finland	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
Netherlands	1
North Macedonia	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Sweden	1
Türkiye	1
United Kingdom	1
United States	1

Belgian Ministry of Economic Affairs 1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czechia	1
Denmark	1
Estonia	1
Finland	1

France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
Netherlands	1
North Macedonia	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Sweden	1
Türkiye	1
United Kingdom	1
United States	1

NATEXs

All NATEXs	1 Each

NCIA/ACQ/2025/07623

ANNEX D

Potential Industrial Suppliers

MS-424320-SD-WAN

Vendor	NATO Nation
AIRBUS DEFENCE AND SPACE AS	Norway
AIRBUS DEFENCE AND SPACE SAS	France
CISCO Systems, Inc	United States
CLOUD JUNXION INC	United States
ERICSON/CRADLEPOINT	United States
FAIRWINDS TECHNOLOGIES	United States
FORTINET Inc	United States
Global RadioData Communications Ltd.	United Kingdom
GREY ZONE SERVICES LTD.	United Kingdom
L3 HARRIS TECHNOLOGIES INC	United States
MARLINK	France
MEDIA BROADCAST SATELLITE GmbH	Germany
MILDEF	Sweden
NETWORK INNOVATIONS	United Kingdom
NEXAT	Belgium
ULTISAT INC	United States
USEI-TELEPORT INC	United States
VERSA Group	United States
VIASAT INC	United States
WORLD WIDE TECHNOLOGY	United States