بسم الله الرحمن الرحيم

National Center for Security & Crises Management

المركز الوطني للأمن وإدارة الأزمات

اعلان طرح عطاء رقم (م وأز/ادارة/ل/٢٠٢٥/ع ١٤)
لتطوير الشبكات العاملة بالمركز وتحديث الأنظمة الأمنية الخاصة بها للمرحلة الثانية
NCSCM NETWORKS DEVEL OPMENTAND SECURITY ENHANCEMENT PROJECT (PHASE2)

١. يعلن المركز الوطني للأمن وادارة الازمات عن حاجته لتطوير الشبكات العاملة بالمركز وتحديث الأنظمة الأمنية الخاصة بها للمرحلة الثانية NCSCM NETWORKS DEVEL OPMENTAND SECURITY ENHANCEMENT PROJECT (PHASE2) وحسب المتطلبات المبينة بالملحق (أ) المرفق ، فعلى الراغبين بتقديم عرض سعر معفي من الضريبة العامة على المبيعات وأية رسوم وضرائب أخرى علماً بأن مشتريات المركز خاضعة بنسبة الصفر استنادا لنص المادة (٢٢/أ) من قانون الضريبة العامة على المبيعات موافاتنا بعروض بالمغلف المختوم معزز بالسجل التجاري ورخص المهن مبيناً الرقم الوطني للشركة جميعها سارية المفعول في المركز الوطني للأمن وادارة الازمات/سكرتير لجنة الشراء الرئيسية (خلف متحف السيارات الملكي) .

٢. آخر موعد لبيع المناقصات يوم الخميس الساعة (١٢٠٠) الموافق ٢٠٢٥/٠٨/١٤.

٣. الزيارات الميدانية للموقع خلال الفترة من الاحد الموافق (٢٠٢٥/٠٨/١٧) ولغاية يوم الاثنين الموافق (٢٠٢٥/٠٨/٢٥) بالتنسيق مع المهندس حمزة الفوارس على الرقم المباشر (٠٦٥٧٧٧٣٨٨) أو (٠٦٥٧٧٧٣٧٠) فرعي (٣٣٠٢) (٣٣٣٧) أو خلوي (٠٧٩٢١٢٢٢٧١).

٤. ارسال الاستفسارات من قبل المناقصين اعتباراً من يوم الثلاثاء الموافق ٢٠٢٥/٠٨/٢٦ ولغاية الساعة ١٢٠٠ يوم الخميس الموافق ٢٠٢٥/٠٨/٢٨ على E-mail التالي:

FROM: hfawaress@ncscm.gov.jo.
CC: tenders@ncscm.gov.jo.

٥. الرد على الاستفسارات خلال الفترة من ٢٠٢٥/٠٨/٣١ ولغاية الساعة ١٢٠٠ يوم الخميس الموافق ٢٠٢٥/٠٩/٠٤.

٦. أخر موعد لتسليم المناقصات الى لجنة الشراء الرئيسية / سكرتير اللجنة يوم (الاثنين) الساعة (١٢٠٠) الموافق ٢٠٢٥/٠٩/١٦ بالتنسيق مع سكرتير لجنة الشراء الرئيسية على الرقم المباشر (٠٦٥٧٧٧٨٧٠) أو (٠٦٥٧٧٧٣٧٠) فرعي (٣٢٠٧) أو خلوي (٠٧٩٢١٢٢٢٦٨).

بسم الله الرحمن الرحيم

National Center for Security and Crises Management

(NCSCM)

RFP NO. (.....)

تطوير شبكات المركز الوطني للأمن وإدارة الأزمات وتحديث الأنظمة الأمنية الخاصة بها (مرحلة ٢)

NCSCM NETWORKS DEVELOPMENT AND SECURITY ENHANCEMENT PROJECT (PHASE2)

(2025/2026)

VOLUME II

TECHNICAL SPECIFICATIONS

DISCLAIMER

THIS DOCUMENT IS A REQUEST FOR PROPOSAL (RFP), AND SHALL NOT BE CONSIDERED IN WHOLE OR PART AS A DIRECT OR INDIRECT ORDER. IT SHALL NOT BE CONSIDERED AS A REQUEST OR AUTHORIZATION TO PERFORM WORK AT THE EXPENSE OF THE NCSCM. THE INFORMATION IN THIS RFP IS INTENDED TO ENABLE THE RECIPIENT TO FORMULATE A PROPOSAL IN RESPONSE TO THE PROJECT REQUIREMENTS SET FORTH. ALTHOUGH THIS RFP CONTAINS SUCH ENABLING INFORMATION, BIDDERS MUST MAKE THEIR INDEPENDENT ASSESSMENTS AND INVESTIGATIONS REGARDING THE SUBJECT MATTER OF THIS RFP. THE BIDDER REMAINS RESPONSIBLE FOR IDENTIFYING ANY FURTHER INFORMATION THAT IT REQUIRES TO PREPARE THE PROPOSAL. THIS RFP SHALL CONSTITUTE PART OF THE CONTRACT THAT WILL BE SIGNED BETWEEN THE NCSCM AND THE WINNING BIDDER.

1.0 INTRODUCTION

1.1 RFP Purpose

The purpose of this Request for Proposal (RFP) is to provide a proposed solution from qualified bidders (either alone or having a joint venture with local/international firms) to execute the implementation of The National Center for Security and Crises Management NCSCM networks development and security enhancement project (Phase2).

NCSCM is seeking proposals from qualified bidders (partners) for the design, supply, Engineering, implementation, and supporting of a modern Core Network Infrastructures. This new infrastructure will replace the current system, which has reached its end-of-life and no longer meets our growing business needs, business continuity insurance, and compliance with local and national regulations.

We are looking for a reliable, scalable, high-performance, and secure Core Network Infrastructure that aligns with industry best practices and supports our ICT strategy, Information Security Strategy, and business-critical applications and services.

2.0 PROJECT DEFINITION AND OVERALL DESCRIPTION

2.1 Current status

NCSCM currently operates a Data Center & Campus network infrastructure built primarily on Cisco hardware, including Nexus 7K, 5K, 2K switches, Catalyst 6513-E for core and data center layers, 2960 S series, and 3750 Series switches for access layer, Nexus Fabric Interconnect Switches for Cisco UCS Servers with Cisco Hyperflex system connected to IBM SAN storage, and HPE HCI simplivity servers system, other rack servers from different vendors. The infrastructure is end-of-life (EOL), and we need to transition to a modern, scalable, secure, and high-performance system. We are considering Cisco, HPE Aruba, Juniper vendors only with a preference for a unified system that reduces complexity and integrates well with existing systems and future requirements.

Therefore, NCSCM intends to replace the existing Core Network Infrastructures to resolve all issues (performance, security, reliability, availability, manageability, and scalability) to ensure a future-proof system that can meet the growing demands of NCSCM.

2.2 Description of the Project

The bidders should re-design, re-assemble, and re-build the existing NCSCM Core Network infrastructures as a single and unified platform. (As shown in Annex (A)).

Understanding and engineering the current HLD (As shown in Annex (A)), figuring out the optimal (best practice) deployments for the new solution components, defining NCSCM requirements/specifications, and planning the implementation methodology.

Supplying, Delivering, Installing, Configuring, Integrating and testing the project components.

3.0 SCOPE OF THE PROJECT

3.1 Core Network Infrastructure

NCSCM is embarking on a critical evolution of its core network infrastructure to support the increasing demand for advanced applications and services for its users. This initiative necessitates the acquisition and implementation of a modern, scalable, highly available, and high-performance core network solution.

Furthermore, recent compliance assessments against ISO 27001 and pertinent local regulations have highlighted the urgent need to integrate robust security controls within the network's design and architecture. This includes, but is not limited to, micro-segmentation, Zero Trust Security principles, and advanced security automation and orchestration capabilities. Therefore, the implementation of a suitable Core Network Infrastructure is essential to meet both current operational demands and evolving security and compliance mandates.

The required solution is mainly divided into two main parts:

A) Data Center Core Network solution.

B) Campus Core Network solution.

3.2 Technical specifications

#	Technical Specifications	Comply
	Core Network Infrastructure	
1	The solution must provide multivendor compatibility with the current heterogeneous environment.	
2	Must be compatible, and integrated with the network and security controls that operates in NCSCM environment. (will be discussed furtherly throughout the site survey)	
3	The proposed solution must provide SDN (Software-Defined Networking) capabilities for network automation, centralized control and granular security enforcement.	
4	The security architecture must support dynamic micro-segmentation based on application context, user identity, or workload characteristics, integrated with a centralized policy management system.	
5	Must support the Implementation of network security best practices, including micro segmentation, firewall integration, ZTNA, and secure access for remote and on premise users.	
6	The system should ensure 99.999% uptime with built-in redundancy and failover capabilities for all parts of the solution.	
7	Must support Micro-segmentation, through both network-based (Smart Switches) and through DC Firewall Integration, allowing for granular control over network traffic between individual workloads, regardless of their location	
8	The solution should be able to scale seamlessly to support future expansion, both in terms of traffic capacity and number of connections.	

9	Provide user-friendly management and effective reporting capabilities with useful user dashboards.	
10	The solution shall be offered in on premise deployment for the critical parts, the management and administrations parts are accepted to be through cloud.	
11	The solution must have the ability to ensure optimal performance for the delay and jitter-sensitive applications, such as VOIP, high definition video, and real-time sensitive applications by minimizing delay and jitter in its design and utilizing quality of service (QoS) traffic identification techniques.	
12	The solution must operate in HA mode (active-active or active-passive), HA mode of operation must be considered through the site survey.	
13	The solution must support local or centralized management (centralized management is preferred).	
14	The proposed solution must support future growth in terms of data traffic, connected devices, and the expansion of data centers and campus network. The architecture should be able to scale seamlessly without requiring significant redesign.	
15	The solution should use modern network architectures such as Leaf-Spine, Spine-Leaf, TOR (Top of Rack), EOR (End of Raw), or other suitable industry-standard designs that ensure high availability, redundancy, and low-latency operation.	
16	The proposed network infrastructure must support low-latency, high-throughput capabilities, especially for mission-critical applications (such as virtualized environments, cloud computing, and real-time communication services). It must be capable of handling up to 100GbE for data center traffic (depending on the current setup) and it should support 1G/10GbE for campus traffic, depending on the use case and required capacity (determined through the site-survey).	
17	The solution must support QoS policies to ensure that latency-sensitive applications such as VOIP, high-definition video conferencing, and real-time analytics are prioritized with guaranteed bandwidth	
18	The proposed solution should provide real-time visibility into network traffic, application performance, and security status. Tools for network management, monitoring, and analytics should be provided, enabling administrators to track performance, troubleshoot, and optimize the network.	

3.3 Winning bidder activities

- The winning bidder is responsible for removing all obsolete network equipment (servers, switches, etc.) and delivering them to NCSCM's designated storage.

- The winning bidder must redesign the server rack layout and distribution of servers within the Data Center for optimal performance and future scalability, considering power distribution, cooling, and physical security as part of the redesign, ensuring structured cable management that follows industry standards. This includes proper labeling and patching of cables and network devices.

- It is the winning bidder responsibility to install, configure and integrate and engineer the proposed solution with other solutions or systems.

- The winning bidder should abide to all terms of SLA agreement in Annex 3.

3.4 Technical Requirements

- Bidders are required to provide details on their vendor renewal strategy for the proposed solution including :

  - End-of-Support (EOS) / End-of-Life (EOL) dates for hardware and software components,

- A clear outline of the support options available post-EOS/EOL, including access to software patches, security updates, and any extended warranty options,
- Details on the upgrade paths available to move to newer solutions after EOS/EOL, including cost estimates, migration procedures, and any risks associated with upgrading.
- Vendor's roadmap for hardware and software evolution, including planned future versions, and next-generation products.

o Bidders must provide a Total Cost of Ownership (TCO) analysis that includes the following:

- Upfront capital costs (CapEx) for hardware, software, and licenses.
- Ongoing operational costs (OpEx), including maintenance and support.
- Estimated renewal cost for the years following the initial contracted period.
- Estimated cost of upgrades once hardware or software reaches End-of-Life (EOL).

o The bidders shall provide such Hardware, software, professional services, deliverables, support, training, and warranty even if not listed in Requirements/Specifications. The cost of these requirements or activities should be included in the fixed lump sum price submitted by the winning bidder.

o Only Partners who are holding the highest partnership level (e.g., Gold, Premium, Platinum, Elite) relevant to the proposed solution are eligible to submit a bid. Bidders must attach an official, verifiable certificate or letter from the relevant vendor that indicates the partnership level and duration.

o The vendor's support (all types of support on hardware, software, license, and others) on the proposed solutions (with all components) must be available for the next 6 years (2026 to 2032), The bidder must provide NCSCM by with a guarantee certificate from the vendor shows their solution is under all types of support (EOSCR, EOS, and EOL) for the next 6 years (at least).

o NDA agreement between NCSCM and other bidders (all bidders) must be signed before the RFP documents (annexes) are delivered.

o All required information or answers could help the bidders to determine the project components or products are through:

- Contact Eng. Hamza Elfawaris through telephone: 065777370 ext. 3337 or Email: hfawaress@ncscm.gov.jo.
- Contact Mr. Ameen Azzam by telephone: 065777370 ext. 3207 or Email: tenders@ncscm.gov.jo

o Site survey visit is a must: a mandatory site survey of NCSCM's current environment must be conducted by all prospective bidders prior to the submission of proposals. This visit is essential for gaining a comprehensive understanding of the existing infrastructure and requirements to accurately scope and design, and propose a successful solution.

o Bidders are responsible for thoroughly analyzing NCSCM's stated requirements and existing network architecture, design, and configuration, then designing and accurately sizing a proposed solution to fully meet all specified technical and functional criteria, including future scalability needs, while adhering to industry best practices.

o Bidders shall include selection, design, implementation, integration, migration, and engineering of the proposed solution through the technical proposal.

o Bidders shall provide NCSCM with the vendor's recommendations and best practices for installation and management of production services and any specifics related to their proposed solution.

- All bidders shall schedule and conduct a technical meeting (after conducting the site survey) with NCSCM to present their proposed solutions and key components. This meeting must take place prior to the submission of the final technical and financial proposals. Its purpose is to ensure mutual understanding of how the proposed solution aligns with NCSCM's requirements and best practices.

- Bidder shall provide basic project management services for the implementation. Project managers shall have experience with core network infrastructure (data centers and campus) and security solutions.

- Bidder shall work closely with NCSCM IT staff regarding the configuration to ensure NCSCM business needs are met.

- The Requirements/Specifications are the minimum.
- Demonstrate the technical capability of the team who will be in charge of maintaining and supporting the solution, by providing the team qualifications and the number of people who will be dedicated to supporting and maintaining the installed platform.

- Vendors must work in such a manner that NCSCM business is not affected in any way. If emergency network downtime is inevitable to deliver the proposed solution, a written notice is required by NCSCM.

- The principal scope of work shall include engineering, design, management, coordination, assembly, software programming, installation, testing, interfacing, commissioning, documentation, and training, the remedy of defects, integration, and warranty of the solution.

- NCSCM reserves the right to accept, annul or cancel the bidding process and reject all proposals at any time without any liability to the bidders or any other party and/withdraw this tender without providing reasons for such action and with no legal or financial implications to NCSCM.

- The bidder is requested to provide options for the licenses and support for one, two, and three years.

- NCSCM reserves the right to conduct a technical audit on the project either by NCSCM resources or by a third party.

4.0 GENERAL TERMS AND CONDITIONS

- Technical and Financial proposals must be offered in separate sealed stamped envelopes.

- Proposals' contents should be organized properly and should be clear.

- Bid Bond should be offered in a separate envelope.

- Technical proposals at least must include:

  - A compliance matrix sheet to fulfill all specified technical specifications/requirements.
  - Bidder Approach for handling the project.
  - Bidder understanding of the NCSCM requirements.
  - Bidder Plan for project Delivery and implementation.

- Bidder qualifications and capabilities may be offered separately or with a Technical proposal. Bidder qualification and capabilities at least must include:

  - Bidder Financial capabilities.
  - Bidder years in Business in Jordan, with supported official Documents

- Bidder Relationship with the vendor, history brief of relation, partnership certification level with evidence, the partnership must be accessible from the vendor website (bidder must provide the online link to such evidence.
- Bidder Technical team capabilities (education, experience, date of joining the Bidder Company, and a certification summary that highlighting the certification related to the offered solution).
- Bidder References in Jordan or outside Jordan for similar projects (Installations of a similar setup must be mentioned in detail). Bidder should provide in his offer customer contact in these references, NCSCM should have the right to contact any of the provided references to get their feedback on their experience with the Bidder provided solution and services.

o Bidders are required to present a detailed support methodology and strategy within their proposal. This section should comprehensively outline the approach to post-implementation support, after-sales assistance, local and vendor-backed support like hardware replacement.....etc.

o Any additional features that can be helpful for the entire solution will be counted for the bidder as much as they are related to the NCSCM requirement.

o All prices must be in JOD clear itemized and include all licenses and taxes.

5.0 EVALUATION CRITERIA

1- The overall proposal will be evaluated according to the following criteria:

- Overall Technical Proposal 60%
- Overall Financial Proposal 40%

2- The evaluation calculation equation will be carried out as follows and will be applied based on the successful qualified Bidders only:

3-

- Total Bidder achieved Technical Score
- Bidder Offered price
- Highest Achieved Technical score for qualified offers
- Lowest Offered Price for qualified offer
- The Winning Bidder will be the bidder who achieves the highest Total score.

#	Requirements/specifications	Weight
1	**Vendor Specifics, Support, and Ecosystem**	60%
2	**Performance, Scalability, Manageability and & Resiliency**	
3	**Proposed Training Program**	
4	**Value of Money**	40%
	Total	100%

6.0 IMPLEMENTATION AND INSTALLATION PLAN

1. The bidders must provide an implementation plan. In addition, it must have milestones and a detailed project schedule.

2. The Implementation Plan should highlight pre-requests and dependencies.

7.0 TRAINING

The offer should include a certified professional training program as follows:

1) Onsite and Hands-on training for the technical staff. During installation and configuration, a knowledge transfer and a detailed education for every step of work must take place by the company team for NCSCM technical staff.

2) Professional certified training program delivered by a vendor's certified trainers in an authorized training centers for two staff includes. Training must cover the proposed solution / or something related and must focus on the following:

- Operation, Management, and administration.
- Problems and fault analysis.
- Software installation and administration.
- Engineering.
- Design and architecture.

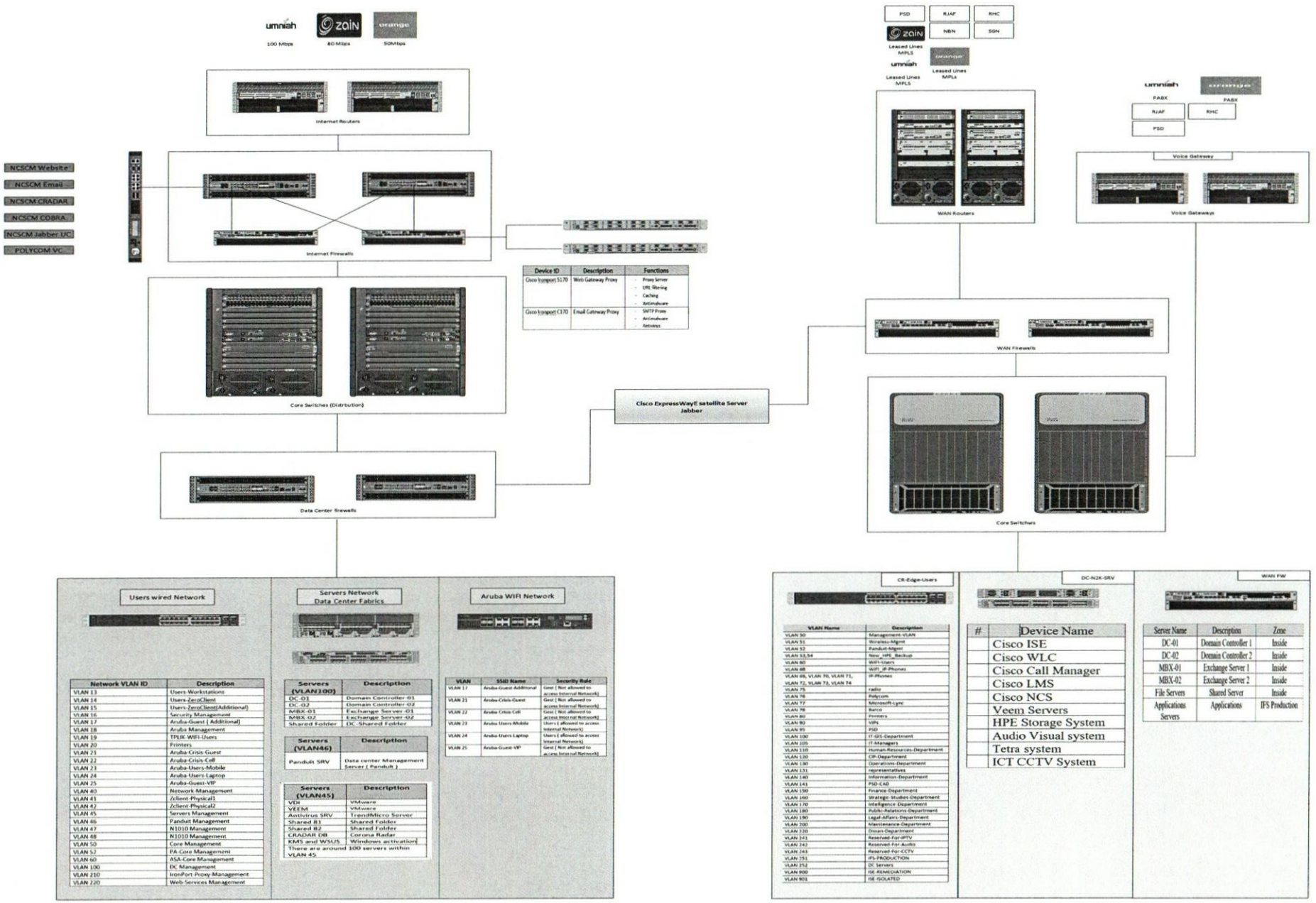
3) Bidder should explain in detail the offered training program in his proposals.

8.0 ANNEXES

Annex #	Description
A	HLD topology
B	NDA agreement
C	SLA Agreement

Annex (D) NDA Agreement (attached)

Annex (A) Current topology HLD



Device ID	Description	Functions
Cisco Ironport S170	Web Gateway Proxy	- Proxy Server - URL filtering - Caching - Antimalware
Cisco Ironport C170	Email Gateway Proxy	- SMTP Proxy - Antimalware - Antivirus

Network VLAN ID	Description
VLAN 13	Users-Workstations
VLAN 14	Users-ZeroClient
VLAN 15	Users-ZeroClient(Additional)
VLAN 16	Security Management
VLAN 17	Aruba-Guest (Additional)
VLAN 18	Aruba Management
VLAN 19	TPLR-WIFI-Users
VLAN 20	Printers
VLAN 21	Aruba-Crisis-Guest
VLAN 22	Aruba-Crisis-Cell
VLAN 23	Aruba-Users-Mobile
VLAN 24	Aruba-Users-Laptop
VLAN 25	Aruba-Guest-VIP
VLAN 40	Network-Management
VLAN 41	Zclient-Physical1
VLAN 42	Zclient-Physical2
VLAN 45	Servers Management
VLAN 46	Panduit Management
VLAN 47	N1010 Management
VLAN 48	N1010 Management
VLAN 50	Core Management
VLAN 52	PA-Core Management
VLAN 60	ASA-Core Management
VLAN 100	DC Management
VLAN 210	IronPort-Proxy-Management
VLAN 220	Web Services Management

Servers (VLAN100)	Description
DC-01	Domain Controller-01
DC-02	Domain Controller-02
MBX-01	Exchange Server-01
MBX-02	Exchange Server-02
Shared Folder	DC-Shared Folder

Servers (VLAN46)	Description
Panduit SRV	Data center Management Server (Panduit)

Servers (VLAN45)	Description
VDI	VMware
VEEM	VMware
Antivirus SRV	TrendMicro Server
Shared 81	Shared Folder
Shared 82	Shared Folder
CRADAR DB	Corona Radar
KMS and WSUS	Windows activation

There are around 100 servers within VLAN 45

VLAN	SSID Name	Security Role
VLAN 17	Aruba-Guest-Additional	Guest (Not allowed to access Internal Network)
VLAN 21	Aruba-Crisis-Guest	Guest (Not allowed to access Internal Network)
VLAN 22	Aruba Crisis Cell	Guest (Not allowed to access Internal Network)
VLAN 23	Aruba-Users-Mobile	Users (allowed to access Internal Network)
VLAN 24	Aruba-Users-Laptop	Users (allowed to access Internal Network)
VLAN 25	Aruba-Guest-VIP	Guest (Not allowed to access Internal Network)

VLAN Name	Description
VLAN 50	Management-VLAN
VLAN 51	Wireless-Mgmt
VLAN 52	Panduit-Mgmt
VLAN 53,54	New_HPE_Backup
VLAN 60	WIFI-Users
VLAN 68	WIFI_IP-Phones
VLAN 69, VLAN 70, VLAN 71, VLAN 72, VLAN 73, VLAN 74	IP-Phones
VLAN 75	radio
VLAN 76	Polycom
VLAN 77	Microsoft-Lync
VLAN 78	Barco
VLAN 80	Printers
VLAN 90	VoPs
VLAN 95	PSD
VLAN 100	IT-GIS-Department
VLAN 105	IT-Managers
VLAN 110	Human-Resources-Department
VLAN 120	CIP-Department
VLAN 130	Operations-Department
VLAN 131	representatives
VLAN 140	Information-Department
VLAN 141	PSD-CAD
VLAN 150	Finance-Department
VLAN 160	Strategic-Studies-Department
VLAN 170	Intelligence-Department
VLAN 180	Public-Relations-Department
VLAN 190	Legal-Affairs-Department
VLAN 200	Maintenance-Department
VLAN 220	Dioan-Department
VLAN 241	Reserved-For-IPTV
VLAN 242	Reserved-For-Audio
VLAN 243	Reserved-For-CCTV
VLAN 251	IPS-PRODUCTION
VLAN 252	DC Servers
VLAN 900	ISE-REMEDIATION
VLAN 901	ISE-ISOLATED

#	Device Name
	Cisco ISE
	Cisco WLC
	Cisco Call Manager
	Cisco LMS
	Cisco NCS
	Veem Servers
	HPE Storage System
	Audio Visual system
	Tetra system
	ICT CCTV System

Server Name	Description	Zone
DC-01	Domain Controller 1	Inside
DC-02	Domain Controller 2	Inside
MBX-01	Exchange Server 1	Inside
MBX-02	Exchange Server 2	Inside
File Servers	Shared Server	Inside
Applications Servers	Applications	IFS Production

Annex (B) The Unified Network HLD