RAJASTHAN RAJYA VIDYUT PRASARAN NIGAM LIMITED
(An ISO 9001-2015 Certified Company)
Corporate Identity Number (CIN): U40109RJ2000SGC016485
OFFICE OF THE SUPERINTENDING ENGINEER (MIS&IT)
IT CENTRE, Chambal Power House Premises, Hawa Sarak
Sodala, Jaipur-302006 Email: se.mis@rvpn.co.in

No./RVPN/SE (MIS&IT)/XEN-I/AEN/F.71( ) / D. 482 dt. 14/9/21

CLARIFICATION & CORRIGENDUM IN E-BID NOTICE BID SPECIFICATION NO SE/MIS_IT/9024002105

Clarifications were sought during Pre-Bid meeting held on 12th Aug 2021 in the bidding documents under Bid Specification No: SE/MIS_IT/9024002105 (UBN No: VPN2122A0289) for **"Implementation of Cyber security and ISO 27001-2013 Readiness in RVPN"** and accordingly the clarifications and corrigendum issued in Bid Document are enclosed as follows:

1) Clarification in Bid Document- **Annexure-"A"**
2) Corrigendum in Bid Document- **Annexure-"B"**
3) Tentative List of Asset-**Annexure**-"LA"

The above documents are also available on departmental website https://energy.rajasthan.gov.in/rvpnl and the other contents of the Bid Specification remain the same.

(A K Gupta)
Superintending Engineer (MIS&IT)
RVPN, Jaipur

Copy submitted/forwarded to the following for information.
1. Additional Chief Engineer (IT), RVPN, Jaipur.
2. Sr. AO (Civil/PPD), RVPN, Jaipur.

Superintending Engineer (MIS&IT)
RVPN, Jaipur

384

Annexure-A

Clarifications under Bid Enquiry No SE/MIS&IT/9024002105 Implementation of Cyber Security and ISO 27001:2013 Readiness in RVPN

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
1	BEL	2.3 (Sl.No:5)	11	The Bidder must have experience of providing ISO27001 consultancies to Organization in India leading to successful ISO: 27001 certification/re-certification of its datacenter Or DRsite.	Our team has an experience in providing the Internal consultancy to get the ISO27001:2013 certification for Our Facility/Units/SBU. Whether providing the consultancy to the internal units and Stragic Business Units (SBU) of our own oragniazation is considered as the eligiblity for this bid. Please confirm?	Consultancy to own oragnization may not be considered as a experience. Provision of bid document shall be adhered
2	BEL	4.1	44	1. Identification of Critical infrastructure Information of RVPN. 2. Preparation of Cyber Crisis Management Plan 3. Readiness for ISO 27001:2013	It is understood that few activites of SOW like preparation of Cyber crisis Management Plan, Documentation of ISO 27001 and etc will be done at the bidder premises. There is no requirment of continuous deployment of man power at RVPN during the project. Please confirm.	This clause is regarding deployment of software and hardware in RVPN premises. Resouce personell is as and when required adhering to the time line of VAPT Reporting.
3	BEL	3.iii.d	46	Awareness session to Senior Management of RVPNwith respect to ISO 27001:2013 standard.	Please specify the days of training program is being envisaged?	Half Day Training Programme
4	BEL	3.iii.k	46	Training to RVPN IT personnel on implementation and maintenance of ISO: 27001-2013 standard of approx. 3 days and Awareness training to RVPN Employees on ISO 27001: 2013 Standard in 2 sessions {Offline/Online} by ISO 27001 Lead Auditor and bidder shall award the participation/pass Certificateto the participants.	Please specify the no of trainees expected for the each of training program?	Approx 50 Employees are need to be given training for implementation and maintenance of ISO: 27001-2013 standard
5	BEL	Annexure-X	73	Technical Specification of the Software Tool for Vulnerability assessment	What is the deployment duration (in years) of the vulnerability Assessment solution in the RVPN Network.	2 Years
6	BEL	Annexure-X	73	Technical Specification of the Software Tool for Vulnerability assessment	Please provide the approximate no of servers, Desktops, Switches, Firewall, web application and oT Devices to be assessed by the vulnerablity assessment tool to calculate the license requirement.	**List of asset is enclosed at Annexure "LA"**
7	BEL	Annexure-X	73	Technical Specification of the Software Tool for Vulnerability assessment	It is understood that after completion of project, the vulnerability assessment solution can be taken back from the RVPN Network. Please confirm.	Yes bidder can take back the VA software

(ANSHU JAIN) AEN (MIS & IT)

(MUKESH SHARMA) XEN (MIS & IT)

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
8	BEL	Annexure-X	73	Technical Specification of the Software Tool for Vulnerability assessment	Please specify the OEM of the Vulnerability assessment software tool.	Any OEM should be in leaders quadrant of Gartner/ Forrester/IDC
9	BEL	Annexure-X (Sl.No.1)	73	The Solution should be on-premises with no dependency on the cloud and shall not rely on component / service hosted outside the RVPN premise for any feature functionality or product capability. The solution should be 100% on-premise solution.	All vulnerability software's required to be connected with their OEM to update their vulnerability signature/plugin, otherwise it will not detect the new published vulnerabilites. Hence, It is proposed to modify/revisit the requirement.	Please see amendment sheet as Annexure "B"
10	BEL	Annexure-X (Sl.No:4)	73	The solution should not have any proprietary format for logs, alerts, vulnerability storage etc. All logs, alerts, vulnerabilities, data etc. should be extractable & exportable without OEM dependent tools & techniques	All vulnerability software's stores the logs, alerts, vulnerabilities and data in their own format which can not be extracted by any other tools. It is proposed to modify/revisit the requirement.	Please see amendment sheet as Annexure "B"
11	BEL	Annexure-X (Sl.No:10)	74	The solution should be able to integrate with IT ticketing and workflowsystems to streamlineand accelerate the handover of lnformafion and to obtain visibilty into the remediation process.	Please specify the IT Ticketing software is being used in RVPN to verify the integration possiblity with Vulnerability Assessment tool.	Please see amendment sheet as Annexure "B"
12	Bosontech	1 f	10	clause 1.f Bidder must possess CERT-IN certificate at the time of Bidding	Why Cert-in when Implementation of 27001 & Readiness is required. This is restictive; removing it will allow more active participations.	Please see amendment sheet as Annexure "B"
13	Bosontech	Clause 4.1	44	Scope Of Work:All assets that are directly accessible through the above mentioned RVPN sites are under the scope of audit and ISO Readiness.	No of Assets /Approx estimate /Band 5000-7500 Not mentioned . Location mentioned Just 4 , Hence no. of GSS Covered mentioned are at how many locations Last Line All assets Directly for example no Upper Cap as 10000 mentioned. This will help in Better resource planning & helps arrive at pricing	**List of asset is enclosed at Annexure "LA"**
14	Bosontech	Para 2	48	Scanning Same Assets 4 times in 2 Years	Assets will vary or remain same in number	May vary due to addition/ deletion of asset. Bidder will scan new assets added to the system and perform the VAPT and submit report for further action.
15	Bosontech	4.3	50	Shift of DC /CoLo and DR Access	Place not specified	Jaipur/Ajmer and Jodhpur in Rajasthan

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
16	Bosontech ---- Allied Boston Consultants India Private Limited	2.3 Point No5(I). Technical Capability	11	Experience of successfully minimum one contract work prder of Cyber security in any Govt. Organization including supply, installation, testing & commissioning for cyber security solutions, appliances software tools, and Vulnerability Assessment value of which should not be ess than Rs. 32 Lakhs during best of three FY out of five FY i.e. 2016-17 to 2020-21	Experience of successfully minimum one contract work prder of Cyber security in any Govt./ listed/ leading private Organization including supply, installation, testing & commissioning for cyber security solutions, appliances software tools, and Vulnerability Assessment value of which should not be ess than Rs. 32 Lakhs during best of three FY out of five FY i.e. 2016-17 to 2020-21.	Please see amendment sheet as Annexure "B"
17	Allied Boston Consultants India Private Limited	Clause No 1 (e)	10	Self-Declaration on Rs. 1000/- Non Judicial stamp paper of Rajasthan State (Annexure-IV)	We request it Rs.100 Stamp Paper from any State of India.	Provision of bid document shall be adhered
18	Maverick Quality Advisory Services Private limited				As we have worked with few Electricity board department in India, we request you to give preference to Cert-IN Vendor to showcase the Work orders for Electricity board department at the time of bid as per Cert-IN. Also this can be preference for CERT-IN agency who will do VAPT part.	Provision of bid document shall be adhered
19	Maverick Quality Advisory Services Private limited				suggest you to please mention a point in RFP for VAPT section, CERT-IN Agency must provide the list no of Government clients details at minimum 15 to 30, if they have done Cyber security audit in last 1 year in State govt/Central Government.	Provision of bid document shall be adhered
20	Maverick Quality Advisory Services Private limited	5(I)	11		We have submission here in government sector we have done more than 100 + Cyber security audit in 1 year. But most of the Purchase order value is less than 1 lacs or so, kindly allow Cert-IN Vendor to provide multiple work orders which should cross the value of Rs 32 Lakhs with considering Private/Gov orders in 1 year.	Please see amendment sheet as Annexure "B"
21	Maverick Quality Advisory Services Private limited				suggested that consultancy for ISO 27001 for DR & DC can be considered for Private organisation work done prior by bidder.	Please see amendment sheet as Annexure "B"

387

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
22	Dr CBS Cyber Security Services LLP	Para 3	Page no. 8. 1.2	Successful bidders shall have to Identify Critical Infrastructure Information of RVPN, and prepare Cyber Crisis Management Plan for identified Infrastructure and readiness for ISO27001: 2013 for IT Security system.	Power Sector is already identified as critical information infrastructure by the 'Information Security Practices and Procedures for Protected System Rules, 2018' made under Indian IT Act 2000.	Please see amendment sheet as Annexure "B"
23	Dr CBS Cyber Security Services LLP	Point 2,3,4 & 5	Page no. 10 11	2. Financial Status (MAAT): For MSME of Rajasthan, Minimum Average Annual Turnover for best three (3) financial years out of last five (5) financial years, Turn over Rs. 12.80 Lacs. 3.Liquid Assets : For MSME, shall be Rs. 3.55 Lacs. 4. Net worth: The net worth of the bidder, in the last three financial years i.e. 2018-19 & 2019- 20 and 2020-21 should be Positive. (For Startup & MSME)	If the bidder is a Startup, the bidder shall be exempted from the requirement of "Bidder Turnover" criteria, "Experience Criteria" and Average Turnover" criteria. Bidder should be empanelled by Indian Computer Emergency Response Team (CERT-In), under the Department of Information Technology, Government of India. Note: No exemption w.r.t CERT-In empanelment certificate as per 1.C above shall be granted to any bidder under any circumstances. Similar Condition is made in other power sector tender documents, one such for the Reference: Bid Number: GEM/2021/B/1397715, Narmada Hydroelectric Development Corporation (NHDC) Limited Cost of the tender: 24,000,00/- If the bidder is a Micro or Small Enterprise as per latest definitions under MSME rules, the bidder shall be exempted from the requirement of "Bidder Turnover" criteria and "Experience Criteria". Similar Condition is made in other tender documents. Reference: One such standard document issued for the National Remote Sensing Centre (PMO) Reference: Bid Number: GEM/2021/B/1133763 Cost : 1,94,70000/-	As per SO134 Notification No.F2(1)/FD/ SPFC/2017 dated 28.0.2018 of RTPP Rules 2013, Auditing works and VAPT is not covered under any items listed in the schedule, although MSME related relaxation as per SO165 notification date 19 Nov 2015 has been provided in bid. Provision of bid document shall be adhered

300

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
24	Dr CBS Cyber Security Services LLP	Point No.5	Page No. 11	5. Technical Capabilities : For Audit work, no need of experience related to supply, installation, testing, software tools. (Work order of 32 Lakh)	For Cyber Security Assurance and implementation of ISO, The experience of supply, testing, installation & commissioning for cyber security solutions, appliances, software tools should not be a criteria for technical capability as cyber security assurance and audit which includes: a) Review of auditee's existing IT Security Policy & controls for their adequacy as per the best practices with established IT Security frameworks outlined in standards such as COBIT, cyber security framework, ITIL, ISO 27001etc. b) Application security assessment c) Vulnerability assessment(VA) d) Exploitation of the vulnerabilities e) Penetration Testing (PT) f) Detailed 'Risk Assessment' and mapping of all 'Vulnerabilities' of systems and networks g) Detailed 'Penetration Tests' and possible exploitation of the 'Vulnerabilities' in the systems and networks i) Network Mapping j) Review and assessment of security policies and controls as per best practices k) Malware/Backdoor detection l) Log review, incidence response and forensic auditing Reference: Guidelines For IT Security Auditing Organizations (CERT-In, v7, Jan 2020)	Please see amendment sheet as Annexure "B"
25	Dr CBS Cyber Security Services LLP	Point no. 6	Page No. 11	Certification: The bidder must possess, at Copy of a valid certificate the time of bidding, a valid ISO9001:2008.	In addition to this the bidder organization should also be a certified ISO/IEC 27001: 2013.	Provision of bid document shall be adhered
26	Dr CBS Cyber Security Services LLP	Point no. 6	Page No. 11	Employee: The bidder must have at Self-Certification by the least on an average 20 authorized signatory with Consultants in its clear declaration of Nos. of employment during last employees as enrolled three financial year i.e. staff year wise, level 2018-19 to 2020-21	As per MSME & Start Up, it is not applicable. As per CERT-In empanelment also, the minimum technical Person required for the Cyber Security Assurance work is 5. Reference: Empanelment of IT Security Auditing Organisations by CERT-In, v7, Jan 2020 Page 2, Para 2.1(b)	Please see amendment sheet as Annexure "B"

(UMESH SHARMA)
XEN (MIS & IT)

384

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
27	Dr CBS Cyber Security Services LLP		Page no. 19	2.19 Techno-Commercial Bid Evaluation: The technically qualified shall be called for making presentation of software product in order to assess the capability of bidder in the subject matter of bid.	Cyber Security Assurance including VAPT is done as per the guidelines issued by the country nodal agency CERTIn, which recommends & prefers that the security assurance including VAPT should be done Manually as well as tool based, hence only capability based on the tools (software) is contradictory with the guidelines issued by CERT-In.	Please see amendment sheet as Annexure "B"
28	Dr CBS Cyber Security Services LLP		Page No. 44	Scope of Work: 1. Identification and preparation of CII (Critical IT Infrastructure) documents: (g) Report of vulnerability assessment by a Software/ hardware tool	Non compliance of the directions, guidelines, advisories, whitepapers etc. issued by CERT-In in the matters of Cyber Security Assurance in general and CII protection in particular by the data centers, service providers, body corporate, intermediaries or any other person is punishable under section 70B (7) of IT act.	Please see amendment sheet as Annexure "B"
29	Dr CBS Cyber Security Services LLP		Page no. 42	42. Amendment in GCC S.no. 1 Joint Venture, Consortium Or Association: Joint venture, consortium is not allowed to bid although Subletting/ of work can be done as per the conditions as mentioned below: The contractor assign or sublet the contract or any part as mentioned in the scope of work for which sub-vendor/ Services are allowed for which sub-contractors are identified in the contract. Suppliers/ Sub-Contractors of the services not identified in the contract or any change in the identified sub-contractor shall be subjected to approval. The experience list of service sub-contractor under consideration by the contractor for this contract shall be furnished for approval in the bid proposal/ prior to procurement of all such Sub-letting of Services. Such assignment/sub- letting shall not relieve the contractor of any obligation, duty or responsibility under the contract. Any assignment as above, without prior written approval, shall be void.	Subletting is not permitted as per CERT-In guidelines hence this replacement proposed in GCC amendment (Page 42 S.No. 1) being contradictory to legal mandate and non compliance of CERT-In guidelines; should be with drawn. It seems that the word 'Audit' is bypassed and replaced by 'cyber security implementation'. Just to avoid the compliance of CERT-In guidelines which is a legal mandate	Provision of bid document shall be adhered

A	B	C	D	E	F	G
Sl. No.	**Bidder Name**	**ITB/GCC/Bid Specification clause No**	**Bid document Page No**	**Clause Details**	**Query/Clarification/Suggestion**	**RVPN Comments**
30	Dr CBS Cyber Security Services LLP		Page 50.	The bidder must produce VAPT report of all the critical assets identified in scope of work 4.1(1) duly approved from the CERT-In empanelled organization. In case the bidder is not empanelled with CERT then the work defined in scope of work can be sublet to the CERT-In empanelled organizations, in that case bidder must submit the name of CERT-In empanelled organization at the time of submitting bid. Any change or continuing with the proposed CERT-In empanelled organization has to be done in consultation with the RVPN before the start of VAPT. However, it is at the discretion of the RVPN to accept or reject the request of the vendor. The bidder shall furnish VAPT report as per schedule till completion of the contract.	Subletting is not permitted as per CERT-In guidelines hence this replacement proposed in GCC amendment (Page 42 S.No. 1) being contradictory to legal mandate and non compliance of CERT-In guidelines, should be with drawn. It seems that the word 'Audit' is bypassed and replaced by 'cyber security implementation'. Just to avoid the compliance of CERT-In guidelines which is a legal mandate	Provision of bid document shall be adhered

(UMESH SHARM
XEN (MIS & T

Amendment/Modification/Addition/Appended under Bid Enquiry No SE/MIS&IT/9024002105 "Implementation of Cyber Security and ISO 27001:2013 Readiness in RVPN"

S. No	Clause No	Existing Clause/Provision	Appended/Amended/Deletion of Clause (Applicable to all firms)
1	Section I 1.2 Objective	Successful bidders shall have to Identify Critical Infrastructure Information of RVPN, and prepare Cyber Crisis Management Plan for identified Infrastructure and readiness for ISO 27001:2013 for IT Security system.	Existing clause is amended as under: Successful bidders shall have to provide consultancy and assistance in Identifying Critical Infrastructure Information of RVPN (CII), and preparation of Cyber Crisis Management Plan (CCMP) for identified Infrastructure and readiness for ISO27001: 2013 for IT Security system of RVPN.
2	2.3-1 (f)	Bidder must possess CERT-IN certificate at the time of Bidding	This clause is hereby deleted.
3	2.3 Point No. 5 Technical Capability	(i) Experience of successfully minimum one contract / work order of Cyber security in any Govt. Organization including supply, installation, testing & commissioning for cyber security solutions, appliances software tools, and Vulnerability Assessment value of which should not be less than Rs. 32 Lakhs during best of three FY out of five FY i.e. 2016-17 to 2020-21. **and** ii) The Bidder must have experience of providing ISO:27001 consultancies to Organization in India leading to successful ISO: 27001 certification/ re-certification of its datacentre or DR site	Existing clause is amended as under: Experience of successful implementation of Cyber security in any Govt./Public/Private sector organization which includes consultancy/ preparation of ISO Readiness 27001:2013 during last three FY i.e. 2018-19 to 2020-21, with two contracts with combined contract value of more than Rs. 10.67 Lakhs in Govt/PSU organization or single contract value of more than 10.67 Lakhs in Private Sector Organization.
4	2.3 Point No.7.Employee	The bidder must have at Self-Certification by the least on an average 20 authorized signatory with Consultants in its clear declaration of Nos. of employment during last employees as enrolled three financial year i.e. staff year wise, level 2018-19 to 2020-21	The bidder must have at least on an average 5 technical Consultants in its declaration of Nos. of employment during last three financial year, employees as enrolled in i.e. staff year wise, level 2018-19 to 2020-21.
5	2.19	Before, the Techno-commercial Bid evaluation committee, the technically qualified bidder shall be called for making presentation of software product in order to assess the capability of bidder in the subject matter of bid.	Existing clause is amended as under: In order to assess the competency of bidder, the bidders shall be called for making presentation of their technical capability, their understanding of our scope of work, methodology to be adopted by them, the past experience and quality of their consultants before the technical evaluation committee.

Amendment/Modification/Addition/Appended under Bid Enquiry No SE/MIS&IT/9024002105 "Implementation of Cyber Security and ISO 27001:2013 Readiness in RVPN"

6	4.1 Scope of Work	Scope of work for which bidder shall be broadly responsible for carrying out various aspects of Cyber Security of RVPN Infrastructure are as follows: 1. Identification of Critical infrastructure Information of RVPN 2. Preparation of Cyber Crisis Management Plan 3. Readiness for ISO 27001:2013	Existing clause is amended as under: Scope of work for which bidder shall be broadly responsible for carrying out various aspects of Cyber Security of RVPN Infrastructure are as follows: 1. **Providing Consultancy and assistance in** Identification of Critical infrastructure Information of RVPN 2. **Providing Consultancy and assistance in** Preparation of Cyber Crisis Management Plan 3. Readiness for ISO 27001:2013
7	4.1 Scope of Work 1.0	Identification and Preparation of CII (Critical information infrastructure) Document.	Existing heading is amended as under: **Providing Consultancy and assistance in** Identification of Critical infrastructure Information of RVPN
8	4.1 Scope of Work 1. Deliverables	Identification of Critical Assets in RVPN for the sites mentioned in the scope of work using as Risk Based approach and as per guidelines of NCIIPC and CERT-In	Existing clause is amended as under: Assistance in Identification of Critical Assets in RVPN for the sites mentioned in the scope of work using as Risk Based approach and as per guidelines of NCIIPC and CERT-In
9	4.1 Scope of Work 2. Deliverables	Compilation of Information Assets Inventories	Existing clause is amended as under: Assistance in Compilation of Information Assets Inventories
10	4.1 Scope of Work 3. Deliverables	VAPT report of **Critical information infrastructure** identified and patching of the vulnerabilities	Existing clause is amended as under: VAPT report of RVPN **Critical IT infrastructure** and patching of the vulnerabilities
11	4.1 Scope of Work 2.0	Preparation of Cyber crisis management plan (CCMP)	Existing heading is amended as under: **Providing Consultancy and assistance in** Preparation of Cyber Crisis Management Plan
12	4.1 Scope of Work 2.0 Deliverables	Cyber Crisis management plan incorporating all the defined activities as above	Existing heading is amended as under: Assistance in preparation of Cyber Crisis management plan incorporating all the defined activities as above
13	Annexure-X (Sl.No.1)	The Solution should be on-premises with no dependency on the cloud and shall not rely on component / service hosted outside the RVPN premise	This clause is hereby deleted.

(ANSHU JAIN)
AFN (MIS & IT)

Amendment/Modification/Addition/Appended under Bid Enquiry No SE/MIS&IT/9024002105 "Implementation of Cyber Security and ISO 27001:2013 Readiness in RVPN"

		for any feature functionality or product capability. The solution should be 100% on-premise solution.	
14	Annexure-X (Sl.No:10)	The solution should be able to integrate with IT ticketing and workflow systemsto streamline and accelerate thehandover of information and to obtain visibility into the remediation process.	This clause is hereby deleted.
15	Annexure-X (Sl.No:4)	The solution should not have any proprietary format for logs, alerts, vulnerability storage etc. All logs, alerts, vulnerabilities, data etc. should be extractable & exportable without OEM dependent tools & techniques	This clause is hereby deleted.

(ANSHU JAIN)
AEN (MIS & IT)

List of IT Assets of RVPN under the Scope

Name of Location	Asset Type	Count of item
CCC,AJMER	Firewall	1
	Router	1
	Switch	4
CCC,AJMER Total		**6**
CCC,HEERAPURA	Advanced Threat Persistent	4
	Core Switch	4
	Firewall	4
	NMS Hardware	2
	On Premise Threat Analysis (Sandboxing)	1
	Router	4
	Switch	5
	Web Proxy Server	1
CCC,HEERAPURA Total		**25**
CCC,JODHPUR	Advanced Threat Persistent	2
	Firepower Manager Chassis	1
	Firewall	2
	Router	3
	Switch	6
CCC,JODHPUR Total		**14**
REMC-OSI- Heerapura	Firewall	4
	NAS	1
	SAN	2
	Server	24
	Switch	13
REMC-OSI- Heerapura Total		**44**
SCADA- HEERAPURA JAIPUR	Firewall	4
	Router	9
	SAN	1
	Server	22
	Switch	19
	tape library	1
	Terminal Server	24
	Workstation	10
SCADA- HEERAPURA JAIPUR Total		**90**
STOMS- Heerapura, Jaipur	Firewall	1
	Router	1
	SAN	1
	Server	8
	Switch	2
STOMS- Heerapura, Jaipur Total		**13**
sub-sldc KOTA	Router	1
	Switch	2
	Terminal Server	3
	Workstation	1
sub-sldc KOTA Total		**7**
SUB-SLDC-RATANGARH	Router	1
	Switch	2

(ARVIND JAIN)
XEN (IS & IT)

(UMESH SHARMA)
XEN (IS & IT)

SUB-SLDC-RATANGARH	Terminal Server	4
	Workstation	1
SUB-SLDC-RATANGARH Total		**8**
URTDSM- Heerapura	Firewall	3
	GPS	3
	Print Server	1
	Router	6
	Server	11
	Storage	9
	Storage server	4
	Switch	14
	Workstation	5
URTDSM- Heerapura Total		**56**
VB 101-DC- Jaipur	Router	24
	Server	11
	Switch	31
VB 101-DC- Jaipur Total		**66**
Grand Total		**329**

(ANSHU JAIN)
AEN (MIS & IT)