Tender No. 3(15)/2004-CERT-In Vol.VIII (part)

Tender Document

For
Procurement/Installation of Software and Hardware for Cyber Security Assurance Lab at CERT-In

Issued by:

Director General,
CERT-In

Government of India
Ministry of Electronics and Information Technology
Indian Computer Emergency Response Team (CERT-In)
Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi-110003

TENDER DOCUMENT

CERT-In has been set up to enhance the Cyber Security in Indian Cyber Space. It mainly serves as a central point for responding to Cyber Security Incidents as and when they occur. CERT-In operations are carried out on 24X7 basis.

Director General, CERT-In, invites Sealed Tenders valid for 90 days from date of tender opening for procurement of hardware and software for cyber security assurance lab at CERT-In.

All the items as mentioned above are required for use at Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, New Delhi. Following instructions should be carefully noted and followed by the bidders:

GENERAL TERMS & CONDITIONS

1. Bidders can download the tender document free of cost from website (https://eprocure.gov.in), Tenders by Organization, "Indian Computer Emergency Response Team".

2. Bidders have to submit Technical bid as well as Commercial Bid in Electronic format on Central Public Procurement Portal (CPPP) (https://eprocure.gov.in) website till the Last Date & Time for submission.

3. Bidders who wish to participate in online will have to procure/ should have legally valid Digital Certificate as per Information Technology Act-2000 using which they can sign their electronic bids. Bidders can procure the same from any of the license certifying authority by Government of India.

4. A Bid should be digitally signed, details regarding digital signature certificate are available at https://eprocure.gov.in/.

5. Offers in physical as well as electronic submission have to be submitted before the closing time and date of the tender.

6. The tenderer should invariably submit their tender in three sealed covers separately namely
   a. E.M.D.
   b. Technical bid and Supporting Documents Cover
   c. Commercial Bid

7. The cover for the bids should bear the following inscription.

"Quotation for Software and Hardware for Cyber Security Assurance Lab at CERT-In"
Tender No. 3(15)/2004-CERT-In Vol.VIII (part)
Closing date & Time for submission of bids: 17/01/2018 upto 1400 hrs

8. EMD Fee
    a. Payment should be made by Account Payee Demand Draft, Fixed Deposit Receipt from a commercial bank, Bank guarantee from a commercial bank, payable at New Delhi.
    b. Payment should be made in favour of "**Pay & Accounts Officer,MeitY,New Delhi**.
    c. Payment made towards EMD will not be refunded unless bid is accepted.
    d. Non- payment of the EMD will make the tenderer liable for disqualifications.
    e. Wrong/ Fraudulent data submission may lead to disqualification / debar. Please ensure that you furnish correct data.
    f. Those tenderers who are exempted for payment of EMD must enclosed necessary documents like SSI Registration etc. along with NSIC/DGS&D/CSPO Registration.

9. Technical Bid Submission

    a. The envelope should be marked as "Technical Supporting Documents".
    b. If the suppliers fail to submit the supporting documents offline within time limit, the bidder is liable for immediate disqualification.
    c. The bids should be submitted on or before the time stipulated in Tender notice at the website https://eprocure.gov.in. The technical supporting documents in physical form may be submitted at the following address:

(Administration), CERT-In
Ministry of Electronics and Information Technology
Ground Floor, Opp. Bank of India Electronics Niketan, 6 CGO Complex,
Lodhi Road, New Delhi 110003
Telefax: 011-24366791
Email: admcert@cert-in.org.in

10. Commercial Bid Submission

    a. The commercial bid submission should be done on the website.
    b. The bids should be submitted on or before the time stipulated in tender notice at the website.

11. No tender will be accepted after prescribed closing time for submission of the same. The delay will not be condoned for any reason whatsoever including postal/transit delay. However, if the last date of submission of tenders is declared as a holiday by the Government, the last date of submission of tenders will be extended to the next working day at same time.

12. The bidder must be a reputed manufacturer or his authorized representative of the type of product offered.

13. The tenders will be opened online on the date, time specified in tender notice.

14. In the first instance, only "Technical bid" will be opened online on the date of opening the tender and taken into consideration for finalization. Subsequently, the "Commercial bid" will be opened online only of those tenderers whose quotations satisfy the technical requirement of the indenter and are otherwise acceptable. The date of opening of commercial bid will be intimated to the qualified bidder.

15. Back out from tender at any interim level during tender processing :- Once the tenders is submitted it will be the responsibility of the tenderer not to escape halfway directly or indirectly by way of raising any problems.

16. The technical scrutiny of the items will be carried out by a committee of experts nominated by the DG CERT-In which may also include demonstration / sample testing and the report of the scrutiny

committee shall be final and binding upon the tenderer. In case there is a discrepancy in the claim made by the tenderer and the specifications shown in the product literature / circuit diagram / photograph, reliance will be placed on the specifications shown in the product literature / circuit diagram photograph, ignoring the claim of the tenderer. Any change or alteration in the product literature / circuit diagram/ photograph must be authenticated by the manufacturer and an affidavit from the manufacturer for supplying the item as altered or changed should also be submitted failing which such changes / alterations will be ignored.

ACCEPTANCE OF TENDER

17. The tender is liable for rejection due to any of the reasons mentioned below:

    a) Non-Submission of tender within stipulated time online.
    b) Tender is unsigned OR not initialed on each page or with unauthenticated corrections.
    c) Tender not submitted in separate envelopes as per conditions and the envelopes are not superscribed with details of the tender enquiry and part enclosed.
    d) Non-payment of Earnest Money Deposit {if not exempted.}
    e) Non-submission of required documents.
    f) Conditional and / or vague offers
    g) Unsatisfactory past performance of the tenderer or any instance where bidder has been named in fraud to the government.
    h) Rates have been shown elsewhere than as asked for.
    i) Items with changes / deviations in the specifications / standard / grade / packing / quality are offered.
    j) Offering a cheaper accessory not approved / recommended by the manufacturer.
    k) Offering an accessory as optional even though it is required to operate the instrument.
    l) Submission of misleading / contradictory / false statement or information and fabricated / invalid documents.
    m) Tenders not filled up properly.
    n) Non-submission of Manufacturer's Authorization Form(MAF) in prescribed format.

18. DG CERT-In, reserves the right to consider or reject any or all tenders or close the tender enquiry without assigning any reason at any time at any stage.

19. The DG CERT-In, does not pledge himself to accept the lowest or any tender and also reserves the right to accept the whole or any part of the tender against any item at his discretion. The tender will be accepted if DG CERT, is satisfied about the production, sale, quoted price technical details, utility of products and past performances of tenderer.

20. The Cumulative turnover of the bidder should be a minimum of Rs.25 Crores for each year through sales of Hardware and Software for the last two financial years. Documentary proof of the same should be provided in the technical bid.

21. The bidder should be an authorized representative of the OEM products and should have adequate facilities, trained manpower and staff for installation, commissioning and after sales service of the equipment. Documentary proof of the same should be provided in the technical bid.

22. The bidder should submit authorization letter issued by the Manufacturer for items no. 1,2,3,5,6,7,12,13,16,17. It is to be addressed to Director General, CERT-In, Ministry of Electronics and Information Technology.

23. The Articles of Association and Memorandum of Association of the bidder are to be submitted along with the certificate of incorporation.

24. The bidder should be ISO 9000 and ISO 27000 Quality certified. Documentary proof should also be submitted in this regard.

25. The bidder should quote the products strictly as per the tendered specifications. Complete Technical details along with make, model number, complete specifications, pamphlets, and literature of the systems highlighting the special features of their offer should be supplied along with the quotation. Bidder should quote for all the items.

26. It is must for the bidder to bid for the hardware & software warranty/license renewal subscription, manpower as per provided BOQs. Bids received without the complete quotes will be summarily rejected.

27. The bidder must quote for all the items as per provided BOQs.

28. Total cost will be calculated in BOQ1 from total costs quoted in BOQ2, BOQ3, BOQ4. This total cost will be considered for calculating the L1 bidder.

29. The bidder's bid for the software, as selected to bid, must be for its latest version only as, released by the OEM at that time. Software Version / Equipment Make & Model must be clearly stated by the bidder in bid.

30. The hardware and license for the Software should be procured by the qualified bidder in name of "Director General, CERT-In " and relevant document for the same is required to be delivered to CERT-In along with the media with installable software for the softwares, as selected to bid, including the preinstalled softwares.

31. The equipment / item / software to be supplied should be supported by a Service / Support Centre manned by the technical service / support engineers authorized by OEM.

32. The qualified bidder shall supply all the spares and accessories for installation & commissioning, as may be required during erection, initial operation of the facility till successful commissioning at CERT-In. The bidder will have to arrange / provide for all the testing equipment & tools required for successful installation, testing & acceptance, maintenance etc.

33. At the time of installation of software tools and license the vendor must provide authenticated file checksum of the software/security tools from the OEM for the verification purpose. The security tools shall be installed only after verification of the checksums.

34. The Bidders should give clause-by-clause compliance for the detailed technical specification of the equipment's/software applications/tools in their technical bids as per Annexure-II. Compliance of all the terms & conditions, as stated in the Tender document, should also be given. An unpriced 'Bill of Material' for all items as mentioned in the Annexure-I of tender should be submitted for compliance of the specifications and configurations of each of the items as part of technical bid.

35. The bidder shall furnish a compliance statement of specifications & features of offered equipment/items in the Technical Bid. Deviation on lower side of specifications will not be

considered. In case, CERT-In is not satisfied with proposed product the bidders must arrange for demonstration of building lab scenarios as suggested by CERT-In, failure of doing so will lead to rejection of bid. Quotes for the latest versions of products only, as available on the closing date, shall be considered. No deviations in terms & conditions of the tender document will be accepted in any case. Complete Technical literature for each of the quoted item from OEM along with make, model number, specifications, configurations, product brochures etc of the systems/software / equipment highlighting special features of their offer should be supplied by the bidder along with the quotation/ technical bid.

36. A certificate on company letterhead, stating that the bidder hasn't been blacklisted or indulged in any controversy by any institution/ organization/ society/ company of the central/ state government ministry/department, or its public sector organizations during the last three years, with company stamp and signed by authorized signatory should also be submitted.

37. The bidder should have adequate facilities, trained manpower and staff for installation, commissioning and providing maintenance support service after the sales of the equipment's in India.

38. The bidder will deploy their own manpower for the installation/ integration of the equipment's and should not be outsourced to any third party.

39. For a bidder, who has submitted the tender bids, it will be automatically assumed that he has accepted all the terms and conditions of the tender. A statement specifying that the quotations are strictly as per the terms and conditions of the tender, should be enclosed with the bids. No request for deviation in the terms and conditions of the tender will be entertained. If there is any deviation from the terms and conditions of the tender or the tenderer has submitted conditional bids, the bid will be summarily rejected

40. Bids should be valid for a minimum period of 90 days after the tender opening date.

41. In case of untoward delay, if any, tenderers may be requested by CERT-In to submit their willingness in writing to extend the validity of the bids for the requested period.

42. All prices have to be quoted with taxes as final price. No enhancement will be permitted once the order has been awarded.

43. The registration number of the firm along with the GST No. Allotted by the sales tax department, as well as the pan number of the firm allotted by the income tax department should be submitted, failing which bidder's bid may be rejected,. The bidder should be registered with service tax department of the government of India and copy of the valid service tax registration no. should also be enclosed.

44. **Pre-bid Meeting:** CERT-In shall hold a pre-bid meeting with the prospective bidders on 05th January 2018 at 3:00 PM in the CERT-In conference room. Queries received, from the bidders, two days prior to the pre-bid meeting shall be discussed.

45. Tenderer is duty bound to observe all the laws, rules, regulations, policies, procedures and guidelines of the central vigilance commission and government of India as in force from time to time.

46. CERT-In reserves the right to accept or reject any bid or cancel tender proceedings without assigning any reason whatsoever.

47. CERT-In reserves the right to change (increase/decrease) the quantity of items to be procured or to place Purchase Order for selected items only, that is, some of the items may be omitted from procurement in entirely.

48. Rates quoted by the bidder shall be final and no negotiation will be held.

49. Incomplete quotations are liable to be rejected.

50. All the pages and drawings forwarded with the quotation should be sequentially numbered and shall be signed by authorized signatory with organization's rubber stamp.

51. In case of any discrepancy between rates mentioned in figures and words, the latter shall prevail.

52. Conditional tenderers, on whatsoever ground, shall not be accepted and summarily rejected.

53. Any attempt of direct or indirect negotiation on the part of the tender with the authority to whom tender bids to be submitted; or with the authority who is competent to finally accept it after the submission of the tender; or any other endeavor to secure any interest or any influence by the tenderer any means for acceptance of a particular tender will render the tenderer liable to be excluded from consideration.

54. The rates are to be quoted by the bidders in Indian Rupees only and payment shall be made to successful bidders in Indian Rupees only. The quotes should be inclusive of all taxes for delivery at the premises of the CERT-In, MeitY, New Delhi. All prices shall be fixed and shall not be subject to escalation of any description.

SUPPLY

55. All the items will be supplied at CERT-In, MeitY for inspection and installation by bidder. All the expenses involved in shipping the equipment to the CERT-In will be borne by the bidder. All aspects of safe delivery shall be the exclusive responsibility of the bidder. CERT-In will have the right to reject the component/equipment's supplied, if it does not comply with the specifications at any point of installation/inspections.

56. All licenses for the software and software subscriptions, if any and as applicable, should in the name of Director General, CERT-In. All the licenses should be generated after hardware installation only.

57. Technical hands-on workshop for 5 CERT-In officials for 5 days on supplied solution to be arranged by bidder and to be provided at bidder expenses with no additional cost to CERT-In.

INSPECTION

58. CERT-In or its representative shall have the right to inspect or to test the items to confirm their

conformity to the ordered specifications. The supplier shall provide all reasonable facilities and assistance to the inspector at no charge to CERT-In. In case any inspected or tested goods fail to conform to the specifications, CERT-In may reject them and supplier shall either replace the rejected goods or make all alterations necessary to meet specification required free of cost to CERT-In.

59. **EARNEST MONEY DEPOSIT (EMD)**

The bid must be accompanied by Earnest Money Deposit of Rs. 50 lakhs/- (Rupees Fifty lakhs only) in the form of a Demand Draft/Pay Order/Bank Guarantee/Fixed Deposit Receipt drawn on any Indian Nationalized Bank/Commercial Banks in favour of Pay & Accounts Officer, MeitY, New Delhi. Bank Guarantee should be valid minimum for a period of 90 days from the opening date (original) of the tender. **Quotations received without Earnest Money Deposit or not confirming to the above and /or with short period of validity are liable to be rejected.**

(a) Earnest Money is liable to be forfeited and bid is liable to be rejected, if the tenderer withdraw or amend, impairs or derogates from the tender in any respect within the period of validity of the tender.

(b) The earnest money of all the unsuccessful tenderers will be returned as early as possible after the expiration of the period of the bid validity but no later than 30 days of the issue of the purchase order. No interest will be payable by CERT-In, on the Earnest Money Deposit.

(c) The Earnest Money of successful bidder shall be returned after acceptance of the material subject to submission of Performance Bank Guarantee of the amount equivalent to 10% of the total price of the items supplied as per the purchase order placed.

60. The Financial Bids of only technically qualified bidders will be opened **online** (only of those tenderers whose quotations satisfy the technical requirement of the indenter and are otherwise acceptable). The date of opening of commercial bid will be intimated to the qualified bidder

61. **WARRANTY**

(a) All the items must be quoted with minimum one year onsite warranty period; or above, if so supplied by the OEM. Warranty period shall commence from the date of completion of – supply, successful installation & commissioning and acceptance by CERT-In; 45 days after the date of complete delivery, if installation is somehow delayed by CERT-In only; whichever is later.

(b) Warranty shall include free maintenance of the whole equipment/ software supplied including free replacement of parts. The defects, if any, shall be attended to on immediate basis but in no case any defect should prolong for more than 120 hours. The on-site comprehensive warranty period will commence from the date of acceptance of the equipment by CERT-In.

(c) The bidder shall submit an assurance that for maintenance of the supplied item, inventory of spares will be maintained at least for next five years from the date of supply of the hardware/equipment/software to CERT-In.

62. **DELIVERY & INSTALLATION**

All the items must be delivered and installed/commissioned within 8 weeks of placement of the Purchase Order. Any delay by the supplier in the performance of delivery of items shall render the supplier liable to imposition of liquidated damage as per the respective Clause (next)

63. **LIQUIDATED DAMAGES (LD)**

If the supplier fails to either deliver any or all of the goods or do not complete the installation within the period as specified in the purchase order, CERT-In shall without any prejudice to its other remedies, deduct liquidated damage at the rate of point one percent (0.1%) of the quoted price for the delayed goods for every week or part thereof. Maximum limit of such deduction will be 10% of the cost of delayed goods.

64. **PAYMENT**

(a) A pre-receipted bill in triplicate in the name of Director General, CERT-In duly supported by purchase order, Delivery Challan, Inspection/Acceptance Certificate after installation, commissioning and testing of the items at site may be submitted to CERT-In for processing of the documents for making the payment

(b) **In Case of Software:** 90% of payment shall be made by CERT-In, MeitY after delivery and satisfactory completion of installation, commissioning, testing and acceptance of the software and equipment as well as receipt of pre-receipted bills in duplicate. Bidder may submit the bills after all the software and equipment are installed, commissioned, tested and accepted. Payment may be made by CERT-In, MeitY after all the software and equipment are installed, commissioned, tested and accepted. Balance 10% payment will be released after expiry of warranty of one year or against Performance Bank Guarantee of the amount equivalent to 10% of quoted price, which should be valid for the 60 days beyond the duration of the warranty period.

(c) **In case of Hardware** : 90% payment shall be made by CERT-In, MeitY after delivery and satisfactory completion of installation, commissioning, testing and acceptance of the equipment as well as receipt of pre-receipted bill in duplicate. 10% payment would be released after expiry of the warranty period of 36 months or 100% on satisfactory completion of installation, commissioning, testing and acceptance of the equipment if the firm submits the Performance Bank Guarantee of the amount equivalent to 10%, of quoted price, which should be valid for the 60 days beyond the duration of the warranty period.

(d) **In case of Resident Engineer**: Payments for resident engineer services will be made on quarterly basis, subject to satisfactory services provided by the vendor.

(e) AMC for 4th and 5th Year will be included in calculating L1 but AMC will be awarded separately.

65. **PERFORMANCE SECURITY**

In case, supplier either fails to deliver the items within delivery period or do not provide satisfactory maintenance during the warranty period, the Performance Security or 10% of quoted price, as case may be, submitted by the firm is liable to be forfeited. Performance Security shall be released immediately after the warranty period is over. No interest will be payable by CERT-In on the Performance Security.

66. **FORCE MAJEURE**

During Force Majeure i.e. Acts of God, War, Floods, Riot, Earthquake, General Strike, Lock ants, Epidemics, Civil Commodities, the bidder shall provide their best possible service in given circumstances.

67. **ARBITRATION**

In the event of any dispute or disagreement under or in relation to this agreement or over the

Interpretation of any of the terms herein above contained or any claim or liability of the party, the same shall be referred to the Sole Arbitrator to be nominated by mutual consent of both parties therein. The intending party will serve notice in writing up on the other party notifying its intension for appointment of Arbitrator should both parties fail to agree on by mutual consent, then CERT-In will appoint the Sole Arbitrator. The provisions of Arbitration and conciliation Act 1996 shall apply. The Arbitration proceedings shall be held in New Delhi. The Arbitrator will give reason for his award and the award passed by the Arbitrator shall be final and binding upon both the parties herein. Such reference shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation Act 1996, or of any modifications or re-enactment thereof including the rules framed there under.

NOTE

1. Quoted price bid including taxes and AMC of 4th and 5th year (Total of BOQ2, BOQ3 and BOQ4) will be considered for calculating the L1 Bidder.
2. Bill of Material is available as the Annexure-I.
3. The bidder should do Online Enrolment in the Central Public portal and the digital signature enrolment has to be done with the e-token. The e-token may be obtained from one of the authorized Certifying authorities.
4. The e-token that is registered should be used by the bidder and should not be misused by others.
5. DSC once mapped to an account cannot be remapped to any other account.
6. The Bidders can update well in advance, the documents such as certificates, purchase order details etc., under *My Documents* option and these can be selected as per tender requirements and then attached along with bid documents during bid submission. This will ensure lesser upload of bid documents.
7. After downloading / getting the tender schedules, the Bidder should go through them carefully and then submit the documents as per the tender document; otherwise, the bid will be rejected.
8. The BOQ templates (BOQ1, BOQ2, BOQ3, BOQ4) must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for that tender. Bidders are allowed to enter the Bidder Name and Values only.
9. If there are any clarifications, this may be obtained online through the e-Procurement Portal, or through the contact details given in the tender document. Bidder should take into account of the corrigendum published before submitting the bids online.
10. Bidder, in advance, should prepare the bid documents to be submitted. If there is more than one document, they can be clubbed together.
11. Bidder should arrange for the EMD as specified in the tender. The original should be posted/couriered/given in person to the Tender Inviting Authority, within the bid submission date and time for the tender.
12. The bidder reads the terms and conditions and accepts the same to proceed further to submit the bids
13. The bidder has to submit the tender document(s) online well in advance before the prescribed time to avoid any delay or problem during the bid submission process.
14. It is important to note that, the bidder has to Click on the *Freeze Bid Button*, to ensure that he/she completes the Bid Submission Process. Bids which are not Frozen are considered as Incomplete/Invalid bids and are not considered for evaluation purposes.
15. At the time of freezing the bid, the e-Procurement system will give a successful bid updation message after uploading all the bid documents submitted and then a bid summary will be shown with the bid no, date & time of submission of the bid with all other relevant details. The documents submitted by the bidders will be digitally signed using the e-token of the bidder and then submitted.

Annexure I

Bill of Material
List of Equipment, Software & Services

Technical Specifications

I. Hardware

S.No.	Items Description	Qty.
1.	**Server (type-1: rack mountable - (2U)** • Rack Mounted with railing (2U) • Dual processor - Intel Xeon E5-2600 v4, 22 core per processor with 2.5MB per core cache or higher • Chipset Intel C610 series • Memory : 512 GB or higher DDR4 RAM with upgrade option upto 1.5 TB • DVD+/-RW Drive • Internal storage at least 18TB, 10K rpm SAS HDD hot plug • Integrated 4 port 10 Gigabit Ethernet (GbE) • At least 2 USB Port, 1 serial port • Redundant Power Supply	10
2.	**Server (type-2: rack mountable - (2U)** • Rack Mounted with railing (2U) • Dual processor - Intel Xeon E5-2600 v4, 10 core processor with 2.5 MB cache per core. • Chipset Intel C610 series • Memory :256 GB or higher DDR4 RAM • DVD+/-RW Drive • Internal storage atleast10TB, 10K rpm SAS HDD hot plug or higher • RAID Controller with 12 Gbps SAS, RAID levels 0, 1, 5, 6, 50 • Integrated 4 port 10 Gigabit Ethernet (GbE) • At least 2 USB Port, 1 serial port • Redundant Power Supply • Windows Server 2016 Datacenter edition preloaded	3
3.	**Network Packet Capture and analytic appliance :** • The Packet capture appliance should have a throughput of 1 Gbps. • The Storage capacity for retention should be atleast 50 TB. • Appliance Network interfaces 2 X 1 Gb and 2 X 10 Gb Copper. • CPU/Memory: at least Intel xeon series 6 Cores CPU with 128 GB Memory. • The solution should support Easy-to-use dashboards for analysts for threat hunting and investigation. • The Packet capture appliance should support high-speed packet capture with deep packet inspection capabilities. • Capability of analysis of logs and packets. • Capability for data enrichment and application of threat intelligence to raw data	1

	• Should monitor a line rate of 20 Mbps perspective and should capture 15 Days of RAW Data and 30 Days META Data. • Capability of network performance monitoring for Packet Capture. • Security analytics for Logs & Packets. • Interoperability, XML WSDL API, SNMPv2 MIB, SNMP traps, Syslog, TACACS+, SMTP • Device Management, Console access, HTTP, HTTPS, Telnet + SSH CLI, SNMP • Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay, page reconstruction, image views, artifact & raw packet extractions. • The solution should support session reconstruction. • The solution architecture should be multi-tiered with the raw data capture and management capability in two different distinct appliances. • Should support automated analytics. • The solution should support session reconstruction for session size atleast 30 MB and object extractions from sessions like zip, office documents, media, attachments etc • Solution should support creating additional parsers for protocols and object analysis without any additional license • Solution should creates session meta data at the point of capture (i.e. while held in memory) for near realtime creation and increased performance. • Solution should have filtering capabilities to drop or truncate certain traffic to maximize performance and storage use. • Solution should support native SSL decryption for HTTPS protocol • QoS (Quality of Service) monitoring • In order to optimize the data store for captured traffic, the solution must: a) Filtering off network traffic to discard unwanted traffic based on filtering conditions using OSI Layers 2-7. b) Truncate traffic based on filtering conditions using OSI Layers 2-7. c) Solution should provide options to choose which alerts to remove and which to keep. • Capability of Specific Service monitoring.	
4.	**Network Cable manager** • 1 U Rack mountable • Horizontal • Deep cable compartments to allow maximum cable density • Rounded edges throughout to protect cable jackets from damage • Pass-through holes on double-sided models to protect cable while facilitating routing between front and back sides • The front side of the manager must provide support, management and high capacity for patch cords, while the back must support Cat 5e, 6, 6A and fiber optic cables.	5
5.	**Router** • Rack Mountable 1U/2U • Throughput 1.5 Gbps or higher • built-in 1 GE and 10 GE ports • Memory DRAM 4 GB (control/services plane) • Flash Memory 8 GB or higher • Redundant Power Supply • Interface management: Console,Web based, Telnet, SSH	1
6.	**Hardware based Firewall:** • Rack mountable 1U	

	• Memory 16 GB or higher • Minimum System flash: 8 GB or higher • Multiprotocol Stateful Throughput: 2 Gbps or higher • Concurrent sessions: 1,000,000 • Minimum firewall connections/Second: 50,000 • Packets per second: 1,000,000 or higher • supports SSL and IPsec VPN services • VLans: 400 or More • Maximum 3DES/AES VPN throughput: 700 Mbps or higher • 1 x management - console , RJ-45 • Dual Power Supply • Separate Console cable • IPv6 ready	1
7.	**Rack Mountable Managed Switch(1U)** • Managed Switch • Rack Mountable(1U) • Uplinks: 4 X 10 Gbe SFP Ports • 48 10/100/1000 Ethernet ports • 20 Gbps Switching bandwidth or higher • DRAM: 512 MB or Higher • Flash Memory: 256 MB hiher • Active VLans: atleast 64 • IPv4 and IPv6 routing • Remote Management Protocol(SSH,CLI,Web Based User Interface)	2
8.	**Laptops-1:** • Intel Core i7-7600U (2.8 GHz, 4 MB cache, 2 cores) or higher • RAM: 16 GB • 512 GB Solid-State Drive (SSD) • 13.3" diagonal LED, Touchscreen with Corning Gorilla Glass • 360 degree screen flexibility • 720p HD webcam • Intel Dual Band Wireless-AC 8265 802.11 a/b/g/n/ac (2x2) Wi-Fi and Bluetooth • External optical drive of laptop brand • At least 2 USB, 1 HDMI, headset jack • Sign in with IR camera and fingerprint sensor • Weight : Maximum upto 1.5 Kg • Leather Sleeve and Backpack • Stylus • Charging adapter and battery. • Windows 10 Pro 64 bits • Microsoft office 2016 professional or latest	3
9.	**Laptops-2:** • Intel Core i7-6920 (Quad Core 2.90GHz, 3.80GHz Turbo, 8MB cache) or higher	8

	• RAM 64 GB DDR4 2133 Mhz or higher • Screen maximum size: 43.1cm (17) touch screen • Memory: 64GB DDR4 2133MHz • HD Graphics CARD • 2 TB SATA OR SSD storage • 4 USB, 1 HDMI, 1 Headphone and microphone jack, 1 SmartCard Reader • 802.11a/b/g/n /ac wireless card • Camera 720p HD webcam • 6 cell or higher Li-Ion battery • Windows 10 Professional 64 bit • Microsoft office 2016 professional or latest • Good Quality branded Laptop bag (backpack)	
10.	**Desktop Workstations:** • Intel Xeon Processor E5-2600 64 bit at least 6 core per processor • Memory: Quad channel, atleast 128GB • Internal drives: SATA 4 TB or higher • Windows 10 Professional 64 bit • Microsoft office 2016 professional or higher • DVD RW Super Multi Drive • Monitor (19.5 diagonal, LED Backlight Technology, Contrast Ratio: 1000:1, Pixel Per Inch: 94, Height-adjustable stand ,Tilt, Swivel, Pivot) • USB Mechanical key board • Mouse USB Optical Mouse • Inbuilt speaker systems • HD Graphics card	5
11.	**MacBook Pro:** • 15.4-inch (diagonal) LED-backlit display with IPS technology. • Operating system: macOS Sierra or latest with boot camp. • Touch Bar with integrated Touch ID sensor . • 2.6 GHz quad-core Intel Core i7 processor (Turbo Boost up to 3.5GHz) with 6MB shared L3 cache or higher. • 16GB onboard memory. • 256GB SSD. • 720p HD camera. • Ethernet Adapter . • Stereo speakers,Dual microphones,3.5-mm headphone jack. • Adaptors for VGA and HDMI. • License of Windows 10 Pro 64 bit. • Microsoft Office 2016 for MAC. • Good Quality branded Laptop bag (backpack).	3
12.	**All in One Color Network printer:** • Print, copy, scan • Print and Copy Speed: 50/50 PPM (Color/B&W)	

	• Print Resolution atleast: 1200 x 1200 dpi • Scan Speed : 100 original / min. (Simplex) and 200 original/min. (Duplex) • Direct Print of Word, Excel, Power Point, PDF etc. file from USB media. • 10+ inch color Control Panel • Scan resolution 100dpi, 150dpi, 200dpi, 300dpi,400dpi,600dpi • Paper Size – Max. SRA3 and Min. A5 • Memory : min. 5 GB RAM and min. 500 GB HDD • Standard Single Pass Duplex Scanning Unit • Interface : USB 2.0 or 3.0 10Base-T/100Base-Tx/1000Base-T • Inbuilt Duplex mode	1
13.	**Rack:** • One 42U Racks for IT Devices with integrated active cooling in the cabinet • Racks should be modular, flexible and easy to expand with Fire Detection Systems • Capacity 3 KW • 1 nos of 3.5 KW Precision Air Conditioner with fixed scroll compressor 19 inch rack mountable design fits only in 6U height.Cooling units should be integrated and mounted. • Cooling unit should be mount in the botom of the cabinet ; cold Aise should have Upward airflow and Hot Aise have Downward Airflow • Useable Space 32U or higher • Atleast 2 no. of 32Amp 1Phase PDU with atleast 12 no. IEC C13 & 4 no. IEC C19 Socket • Integrated Monitoring • Temperature, Humidity, Door Switch Sensor, Access Control, Water Leak Sensor and Camera Based Local Surveillance,Events Alerts, SNMP, Email notification	1
14.	**Rack Mountable KVM switch with built-in monitor capable of connecting 16 inputs:** • 1U rack mount • 17" or 19" LED-backlit LCD monitor • BIOS-level access • Hot pluggable - add or remove computers without having to power down the switch • One console controls at least 16 computers directly • Multiplatform support: Windows, Linux, Unix, HP-UX, SUN Solaris. • Computer selection via front panel buttons, hotkeys, or On Screen Display • BIOS-level access • Auto PS/2 and USB interface detection. • Firmware upgradeable • Fully compliant with USB specification. • Dual interface – support computers with PS/2 or USB keyboard and mouse. • All necessary interface cables	1
15.	**KVM Switch(Minimum 4 Ports)** • Direct Computer Connections: 4 or more • Port Selection Hotkey, Pushbutton, on screen display (OSD) • Console Ports • 2 x USB Type ,1 x HDB-15 1 x Mini Stereo Jack ,1 x Mini Stereo Jack • KVM Ports	4

	• Console Keyboard Connector:1 x USB • Console Mouse Connector- 1 x USB • Console Video Connector- 1 x VGA-15 pin female(2048 x 1536; DDC2B) • Console Audio Connectors- 1 x Mini-DIN Speaker Port, 1 x Mini DIN Microphone port • 4 KVM Cables with each Switch	
16.	**Backup storage solution** • Rack mountable: 1U/2U • Capacity: Minimum 30 TB usabale capacity (300 TB logical capacity) or higher • Atleast one quad port 10 GbE, one 16 GBPS dual port FC card and dual port 1 GbE card • Protocol support: NFS, CIFS, OST, VTL • Deduplication and compression ratio of 10:1 • Throughput: 20TB/hr • Backup solution should be image level backup solution specifically designed for Virtual Environments. • Proposed backup appliance should have single deduplication pool across all protocols, data types and backup softwares to achieve maximum storage optimization. • Proposed backup appliance should have RAID 6 and hot spare. • Backup solution should be totally agentless but should support application aware backup processing including truncation of MS MS SQL, Exchange transaction logs. • Backup solution should be Hardware Agnostic Solution and it should support any type of storage for storing the Backups. • Backup solution should store a backup recovery point as a single file. • The proposed backup solution must support at least AES 256-bit encryption capabilities. • Backup solution should include inline de duplication and compression of backup files. • Backup files should be self-sufficient and recovery should not depend on files catalog or indexing. • Backup solution should support file level recovery from an image level backup of Windows\Linux\ Solaris guest file systems. • Backup solution should provide the RTO equal to High Availability and be able to boot the Virtual Machines directly from the Backup to reduce the downtime. • Backup solution should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO. • Solution shall have native feature for Automated Backup Verification. • Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency. • Solution should provide instant server recovery in the Sandbox for server testing purposes. • Solution should provide Backup and Replication capabilities in one console. • The solution should support Windows as well as Linux different flavors • The Solution should support varieties of backup mechanisms like Full, Incremental, Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly. • Replication should include failover and failback capabilities • Solution should be Agentless and should not require license, deploy, manage or monitor on hosts or VMs. • Solution should support 24x7 real-time monitoring and views of health, performance and workload of the virtual hosts. • The proposed Backup Solution must Allow to configure the maximum acceptable I/O latency level for production datastores to ensure backup and replication activities do not impact storage Availability to production workloads.	1 No.

II. Software/Tools

S.No.	Name Of the Software	Featured Required in the Software	Qty
17.	**Software defined infrastructure solution: Cloud solution including computing, network & storage virtualization and Management Server.**	• All components must integrate into single solution and setup as a single solution on the rack mountable servers specified at S.No. 1 above. **1. Cloud & Virtual Server management Capabilities** • The cloud solution should support Heterogeneous virtual environment provisioning. • The solution should also automate and provision data-center services such as compute, storage, networking, backup, replication, load balancing, fault tolerance, security and firewall. • The solution should provide resource reclamation functionality which identifies and reclaims inactive and abandoned resources by automating the decommissioning and reuse of retired resources. • The solution shall provide automated provisioning of infrastructure, applications and custom services through a unified, web-based, multi-tenant self-service IT service catalog to reduce IT service delivery times. • The solution shall allow authorized administrators, developers or business users to request new IT services and manage specific cloud and IT resources, while ensuring compliance with policies. • The solution shall support creation of services such as 'Single VM' and a 'Multi-tier application infrastructure (including software based constructs such as load balancers)' as part of a standard template and also provide ready integration with the proposed platform to automate delivery of networking & security services such as switching, routing, load balancing and firewalling. • The solution shall support multiple levels of approval integrated with email notifications such that approvals/rejections can be done without having to login to the self-service portal. • The solution shall support extensibility capabilities to customize machine configurations and integrating machine provisioning /management with other enterprise-critical systems such as load balancers, configuration management databases IP address management systems, or Domain Name System (DNS) servers. • The solution shall extend operations capabilities to the requestor of the service (eg. ability to start/stop/suspend virtual machines, request additional resources and access the VM using RDP/SSH protocols) through the self-service portal based on entitlement. • The solution shall support granular role-based access control and entitlements of infrastructure services to consumers and allow administrators to manage and reserve (allocate a share of the memory, CPU and storage) resources for a group to use. • Solution should offer leases (time-limited provisioning of resources). • The solution should be able to define multiple tenants which would enable the administrators to create a secure multitenant infrastructure. • The solution should have the ability to create custom workflows to automate the delivery of anything as a service - XaaS (for example Email, Storage as a Service, Network as a	20 CPU License (10 servers dual CPU)

		Service , Backup as a Service etc.) • The Solution should provide Infrastructure as a Service support for multi hypervisor environment including vSphere, Hyper-V, RHEV and XEN etc. and support provisioning of infrastructure in public , private and hybrid cloud etc. • The solution should provide abstraction of application-specific deployment logic from the underlying cloud infrastructure which would allow true separation between applications and infrastructure and would enable reuse of the same blueprint on multiple virtual and cloud infrastructures. • The solution should provide Simple and Automated Application Provisioning capabilities along with the graphical drag-and-drop canvas for creating application blueprints that would make planning and deploying complex applications easily. • The solution provided automation of operations such as provisioning a virtual machine or adding storage capacity should cover peripheral systems such as a configuration-management database, IP address management, load balancing, monitoring and other management systems. As a result, the entire process can be automated without necessitating any manual cycles. • Should be able to integrate with Vmware ESXi platform. • The solution should provide complete visibility into all levels of infrastructure and applications through a single management console for multiple hypervisors, plus physical and cloud environments. • The solution should be able to monitor the performance and health of underlying hypervisor and physical environment. • The solution should provide templates to ensure the hypervisor hardening, change, configuration and regulatory compliance, capability to automatically name and continuously update application components and version numbers, infrastructure & operations analytics and also policy-based configuration management which would assure compliance for virtual and physical environment. • The solution should have deep configuration data collection, change tracking, compliance assessment and remediation of noncompliant configurations across virtual & physical infrastructure and also provide unified reporting of configuration data and compliance assessment results for virtual & physical environment. • The solutions should provide Monitoring of OS level resources (CPU, disk, memory, network) for Windows and Linux OS and physical hardware resources of the hosts. • The solution should provide flexible group policies which would let admin to define specific health, risk and capacity thresholds, alert types and notifications, business hours and many other configuration settings at a group level to prioritize operational activities for business critical applications, production workloads or business units. • The solution should provide self-learning performance analytics and dynamic thresholds which can adapt to the environment to simplify operations management and eliminate false alerts and based on Historical data and trending, solution should be able to send proactive smart alerts to avoid potential downtime. **2. Computing/Server Virtualization** • Bare Metal Solution: Install directly on the bare metal server hardware with no dependence on a general purpose OS.	

		• Guest OS: Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc. • VM Capability: Create Virtual machines with up to 120+ virtual processors, 2+ TB virtual RAM and 2+ GB Video memory in virtual machines for all the guest operating system supported by the hypervisor. • VM Live Migration: Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option, no disruption to users or loss of services. • Storage Live Migration: Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS. • High Availability: In case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software and also should be able to proactively identify the capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs. • On the fly resource addition: CPU, Memory & devices to virtual machines can be added when needed without disruption in working for both windows and Linux based VMs. • VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components. • Enforcing security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits. • Support boot from iSCSI, FCoE, and Fibre Channel SAN. • Integrate with NAS, FC, FCoE and iSCSI SAN infrastructure leveraging high performance shared storage to centralize virtual machine file storage for greater manageability, flexibility and availability. • Virtual Switch: Span across a virtual datacenter and multiple hosts should be able to connect to it. In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details. • Replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level. • Backup and recovery for virtual machines should allow admins to backup virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability. **3. Network Virtualization** • Logical Switching – Reproduce the L2 and L3 switching functionality in a virtual environment, decoupled from underlying hardware. • Logical Routing – Routing between logical switches, providing dynamic routing within different virtual networks • Logical Firewall – Distributed firewall, kernel enabled line rate performance, virtualization	

		and identity aware, with activity monitoring. • Logical Load Balancer – Solution should provide a server load balancer with features like SSL offload. • Logical VPN – The solution should provide L2VPN, SSLVPN, site-to-site IPSEC VPN services. • It should support deployment of multiple instances of virtual networks independent of each other. • The solution shall provide a networking & security virtualization layer that allows delivery of network services in software. • On-demand network creation, define routed, NAT or Private network profiles based on application topology, creation of security groups based on existing security policies. • The solution should enable integration of third-party network and security solutions & and offer logical switches on virtualize infrastructure. • The virtualization solution should offer to bridge VXLAN layer2 Networks and VLAN based networks • The Solution should offer Centrally managed distributed L2-L4 stateful firewall that is kernel-level integrated into the virtualized host architecture. • The distributed firewall should be embedded in-kernel in host architecture and should provide atleast 15 Gbps or better performance per host • The solution should offer to Integrate with solutions for antivirus, malware, and intrusion prevention. • The solution should offer to Create, change, and manage security policies across all Virtual Networks. • The solution should provide industry-standard IPSec and SSL VPN capabilities that enables securely extending the virtual datacenter. • The solution should provide support for the Netflow. • The Platform should model the entire Data Center and tie together visibility across the domains of compute, network and security for physical, virtual and cloud. • The software should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting. • The Platform should be able to generate report that includes amount of traffic that's East-West, Internet, VM to VM, VM to Physical, Hair-pinned and Unprotected. • The Users should be able to monitor all the virtual as well as physical hops on the path between two machines. • The Platform should be designed for agentless deployment. **4. Storage Virtualization** • Software defined Storage. • Solution should be capable to pools together server-attached flash devices and hard disks to provide shared datastore. • Combine storage capacity available with rack mountable servers mentioned at S.No.1 and allow the combined storage to use as Storage Area Network. • Storage should be available to VMs running in virtual environment.	

		• Storage should be managed by cloud and management server • Support deduplication and compression. • Scalability of solution. • Policy based automation of the jobs. • Tight Integration with complete solution.	
18.	**Adobe Media Server Professional 5 64-bit**	• On-demand packaging for HTTP • Robust media origin services • Adobe Access DRM Support • Application-level multicast • Studio-grade DRM packaging • Advanced disk management for HTTP.	1 License
19.	**Print2Flash Commercial 3.4 [Server Mode] 64-bit**	Server mode 64 bit	1 License
20.	**Microsoft Office 2016 Professional Plus 64 bit**	Professional Plus 64 bit or latest	5 Licenses
21.	**Windows Server 2016 with downgradable option 64 bit**	Datacenter edition	1 License
22.	**Microsoft Windows Server 2016 64 bit(Standard Edition)**	standard edition	4 Licenses
23	**Microsoft Windows Server 2016 64 bit(Datacenter Edition)**	Datacenter Edition	5 Licenses
24.	**Acrobat Pro DC**	• Compatible with Windows 7, 8 and 10 or Mac OS X v10.9 and v10.10. • Edit or export PDFs to Office. • Add audio and video files to PDFs.	2 Licenses
25.	**Microsoft Visio Professional 2016 or Latest 64 bit**	It should be Professional 2016 64 bit or latest version	2 Licenses
26.	**Microsoft Windows 10 Professional 64 bit**	Professional 64 bit or latest	2 License
27.	**Microsoft Project Professional or Latest 2016 64-bit**	It should be Professional 2016 64 bit or latest version.	2 Licenses
28.	**Cisco Adaptive Security Virtual Appliance Standard or latest**	• Throughput 1 Gbps or higher • 3DES/AES VPN throughput 125 Mbps Connections per second 20000 • VLANs 50 Concurrent sessions 100000 • Hypervisor Support • Virtual CPUs : 1 • Memory 2 GB or higher • Storage at Least 8 GB or higher .	4 Licenses

III. Residential Engineer

S.No.	Residential Engineer	Description of Services	Qty

29	**To be deputed for 3 Years.**	• The vendor shall depute One qualified Full Time resident engineer to the CERT-In on every working day (working hours:9.00 am to 5.30 pm) including Saturday and if required even on Holiday/ beyond working hours too. • Resident engineer provided by the vendor are to the satisfaction of the CERT-In. • The Resident Engineer as asked in the tender should be on direct role of the bidder and should be employed by the bidder in compliance with relevant Govt. acts of employment fulfilling statutory obligations including but not limited to provident fund, ESI, etc. An undertaking to this effect should be submitted by the Bidder. • The resident engineer should possess Bachelor's/ Master's degree in Engineering/Technology/ Computer Applications. • The vendor shall provide a suitable replacement of the Engineer deputed in case of his leave/absence. • The Resident engineer is expected that would be proficient in maintenance of IT infrastructure ,hardware, software and networking. • The resident engineer should be conversant with installation and configuration of cloud solution & backup software supplied. • Monitoring and troubleshooting LAN/Firewall//VPN/intranet etc. Configuration of printers and other Network peripherals on the network. • It will also be the responsibility of the Resident Engineers to lodge maintenance calls & follow-up. • Daily call and resolution reporting, infrastructure health status reporting, usage reporting, exception reporting. • All the expenses including salary/bills will be borne by the bidder. • Resident engineer will report to head of Cyber security assurance lab • Resident engineer will be required to work as per requirement of team for conducting tests. • Resident engineer will be responsible for all updates/patch installation in lab. • Any other activity/duties assigned to resident engineer, which is necessary for operation of lab.	1

Annexure-II

Technical Compliance Sheet

S.No.	Item Name	Quantity	Product Offered by Bidder	Technical Specifications	Compliance (Yes/No)
1	**Server (type-1: rack mountable - (2U)**	10		Rack Mounted with railing (2U)	
				Dual processor - Intel Xeon E5-2600 v4, 22 core per processor with 2.5MB per core cache or higher	
				Chipset Intel C610 series	
				Memory : 512 GB or higher DDR4 RAM with upgrade option upto 1.5 TB	
				DVD+/-RW Drive	
				Internal storage at least 18TB, 10K rpm SAS HDD hot plug	
				Integrated 4 port 10 Gigabit Ethernet (GbE)	
				At least 2 USB Port, 1 serial port	
				Redundant Power Supply	
2	**Server (type-2: rack mountable - (2U)**	3		Rack Mounted with railing (2U)	
				Dual processor - Intel Xeon E5-2600 v4, 10 core processor with 2.5 MB cache per core.	
				Chipset Intel C610 series	
				Memory :256 GB or higher DDR4 RAM	
				DVD+/-RW Drive	
				Internal storage atleast10TB, 10K rpm SAS HDD hot plug or higher	
				RAID Controller with 12 Gbps SAS, RAID levels 0, 1, 5, 6, 50	
				Integrated 4 port 10 Gigabit Ethernet (GbE)	
				At least 2 USB Port, 1 serial port	
				Redundant Power Supply	
				Windows Server 2016 Datacenter edition preloaded	

3	**Network Packet Capture and analytic appliance :**	1		The Packet capture appliance should have a throughput of 1 Gbps.	
				The Storage capacity for retention should be atleast 50 TB.	
				Appliance Network interfaces 2 X 1 Gb and 2 X 10 Gb Copper.	
				CPU/Memory: at least Intel xeon series 6 Cores CPU with 128 GB Memory.	
				The solution should support Easy-to-use dashboards for analysts for threat hunting and investigation.	
				The Packet capture appliance should support high-speed packet capture with deep packet inspection capabilities.	
				Capability of analysis of logs and packets.	
				Capability for data enrichment and application of threat intelligence to raw data	
				Should monitor a line rate of 20 Mbps perspective and should capture 15 Days of RAW Data and 30 Days META Data.	
				Capability of network performance monitoring for Packet Capture.	
				Security analytics for Logs & Packets.	
				Interoperability, XML WSDL API, SNMPv2 MIB, SNMP traps, Syslog, TACACS+, SMTP	
				Device Management, Console access, HTTP, HTTPS, Telnet + SSH CLI, SNMP	
				Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay, page reconstruction, image views, artifact & raw packet extractions.	
				The solution should support session reconstruction.	
				The solution architecture should be multi-tiered with the raw data capture and management capability in two different distinct appliances.	
				Should support automated analytics.	
				The solution should support session reconstruction for session size atleast 30 MB and object extractions from sessions like zip, office documents, media, attachments etc	

				Solution should support creating additional parsers for protocols and object analysis without any additional license	
				Solution should creates session meta data at the point of capture (i.e. while held in memory) for near realtime creation and increased performance.	
				Solution should have filtering capabilities to drop or truncate certain traffic to maximize performance and storage use.	
				Solution should support native SSL decryption for HTTPS protocol	
				QoS (Quality of Service) monitoring	
				In order to optimize the data store for captured traffic, the solution must: a) Filtering off network traffic to discard unwanted traffic based on filtering conditions using OSI Layers 2-7. b) Truncate traffic based on filtering conditions using OSI Layers 2-7. c) Solution should provide options to choose which alerts to remove and which to keep.	
				Capability of Specific Service monitoring.	
4	**Network Cable manager**	5		1 U Rack mountable	
				Horizontal	
				Deep cable compartments to allow maximum cable density	
				Rounded edges throughout to protect cable jackets from damage	
				Pass-through holes on double-sided models to protect cable while facilitating routing between front and back sides	
				The front side of the manager must provide support, management and high capacity for patch cords, while the back must support Cat 5e, 6, 6A and fiber optic cables.	
5	**Router**	1		CPU/Memory: at least Intel xeon series 6 Cores CPU with 128 GB Memory.	
				The solution should support Easy-to-use dashboards for analysts for threat hunting and investigation.	

				The Packet capture appliance should support high-speed packet capture with deep packet inspection capabilities.	
				Capability of analysis of logs and packets.	
				Capability for data enrichment and application of threat intelligence to raw data	
				Should monitor a line rate of 20 Mbps perspective and should capture 15 Days of RAW Data and 30 Days META Data.	
				Capability of network performance monitoring for Packet Capture.	
6	**Hardware based Firewall:**	1		Security analytics for Logs & Packets.	
				Interoperability, XML WSDL API, SNMPv2 MIB, SNMP traps, Syslog, TACACS+, SMTP	
				Device Management, Console access, HTTP, HTTPS, Telnet + SSH CLI, SNMP	
				Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay, page reconstruction, image views, artifact & raw packet extractions.	
				The solution should support session reconstruction.	
				The solution architecture should be multi-tiered with the raw data capture and management capability in two different distinct appliances.	
				Should support automated analytics.	
				The solution should support session reconstruction for session size atleast 30 MB and object extractions from sessions like zip, office documents, media, attachments etc	
				Solution should support creating additional parsers for protocols and object analysis without any additional license	
				Solution should creates session meta data at the point of capture (i.e. while held in memory) for near realtime creation and increased performance.	
				Solution should have filtering capabilities to drop or truncate certain traffic to maximize performance and storage use.	
				Solution should support native SSL decryption for HTTPS protocol	
				QoS (Quality of Service) monitoring	

				In order to optimize the data store for captured traffic, the solution must:	
				a) Filtering off network traffic to discard unwanted traffic based on filtering conditions using OSI Layers 2-7.	
7	**Rack Mountable Managed Switch(1U)**	2		b) Truncate traffic based on filtering conditions using OSI Layers 2-7.	
				c) Solution should provide options to choose which alerts to remove and which to keep.	
				Capability of Specific Service monitoring.	
				The Packet capture appliance should have a throughput of 1 Gbps.	
				The Storage capacity for retention should be atleast 50 TB.	
				Appliance Network interfaces 2 X 1 Gb and 2 X 10 Gb Copper.	
				CPU/Memory: at least Intel xeon series 6 Cores CPU with 128 GB Memory.	
				The solution should support Easy-to-use dashboards for analysts for threat hunting and investigation.	
				The Packet capture appliance should support high-speed packet capture with deep packet inspection capabilities.	
				Capability of analysis of logs and packets.	
				Capability for data enrichment and application of threat intelligence to raw data	
8	**Laptops-1:**	3		Intel Core i7-7600U (2.8 GHz, 4 MB cache, 2 cores) or higher	
				RAM: 16 GB	
				512 GB Solid-State Drive (SSD)	
				13.3" diagonal LED, Touchscreen with Corning Gorilla Glass	
				360 degree screen flexibility	
				720p HD webcam	
				Intel Dual Band Wireless-AC 8265 802.11 a/b/g/n/ac (2x2) Wi-Fi and Bluetooth	
				External optical drive of laptop brand	
				At least 2 USB, 1 HDMI, headset jack	
				Sign in with IR camera and fingerprint sensor	
				Weight : Maximum upto 1.5 Kg	

				Leather Sleeve and Backpack	
				Stylus	
				Charging adapter and battery.	
				Windows 10 Pro 64 bits	
				Microsoft office 2016 professional or latest	
9	**Laptops-2:**	8		Intel Core i7-6920 (Quad Core 2.90GHz, 3.80GHz Turbo, 8MB cache) or higher	
				RAM 64 GB DDR4 2133 Mhz or higher	
				Screen maximum size: 43.1cm (17) touch screen	
				Memory: 64GB DDR4 2133MHz	
				HD Graphics CARD	
				2 TB SATA OR SSD storage	
				4 USB, 1 HDMI, 1 Headphone and microphone jack, 1 SmartCard Reader	
				802.11a/b/g/n /ac wireless card	
				Camera 720p HD webcam	
				6 cell or higher Li-Ion battery	
				Windows 10 Professional 64 bit	
				Microsoft office 2016 professional or latest	
				Good Quality branded Laptop bag (backpack)	
10	**Desktop Workstations:**	5		Intel Xeon Processor E5-2600 64 bit at least 6 core per processor	
				Memory: Quad channel, atleast 128GB	
				Internal drives: SATA 4 TB or higher	
				Windows 10 Professional 64 bit	
				Microsoft office 2016 professional or higher	
				DVD RW Super Multi Drive	
				Monitor (19.5 diagonal, LED Backlight Technology, Contrast Ratio: 1000:1, Pixel Per Inch: 94, Height-adjustable stand ,Tilt, Swivel, Pivot)	
				USB Mechanical key board	
				Mouse USB Optical Mouse	
				Inbuilt speaker systems	
				HD Graphics card	

11	**MacBook Pro:**	3		15.4-inch (diagonal) LED-backlit display with IPS technology.	
				Operating system: macOS Sierra or latest with boot camp.	
				Touch Bar with integrated Touch ID sensor .	
				2.6 GHz quad-core Intel Core i7 processor (Turbo Boost up to 3.5GHz) with 6MB shared L3 cache or higher.	
				16GB onboard memory.	
				256GB SSD.	
				720p HD camera.	
				Ethernet Adapter .	
				Stereo speakers,Dual microphones,3.5-mm headphone jack.	
				Adaptors for VGA and HDMI.	
				License of Windows 10 Pro 64 bit.	
				Microsoft Office 2016 for MAC.	
				Good Quality branded Laptop bag (backpack).	
				3-year onsite comprehensive warranty.	
12	**All in One Color Network printer:**	1		Print, copy, scan	
				Print and Copy Speed: 50/50 PPM (Color/B&W)	
				Print Resolution atleast: 1200 x 1200 dpi	
				Scan Speed : 100 original / min. (Simplex) and 200 original/min. (Duplex)	
				Direct Print of Word, Excel, Power Point, PDF etc. file from USB media.	
				10+ inch Control Panel	
				Scan resolution 100dpi, 150dpi, 200dpi, 300dpi,400dpi,600dpi	
				Paper Size – Max. SRA3 and Min. A5	

				Memory : min. 5 GB RAM and min. 500 GB HDD	
				Standard Single Pass Duplex Scanning Unit	
				Interface : USB 2.0 or 3.0 10Base-T/100Base-Tx/1000Base-T	
				Inbuilt Duplex mode	
13	**Rack**	1		One 42U Racks for IT Devices with integrated active cooling in the cabinet	
				Racks should be modular, flexible and easy to expand with Fire Detection Systems	
				Capacity 3 KW	
				1 nos of 3.5 KW Precision Air Conditioner with fixed scroll compressor 19 inch rack mountable design fits only in 6U height.Cooling units should be integrated and mounted.	
				Cooling unit should be mount in the botom of the cabinet ; cold Aise should have Upward airflow and Hot Aise have Downward Airflow	
				Useable Space 32U or higher	
				Atleast 2 no. of 32Amp 1Phase PDU with atleast 12 no. IEC C13 & 4 no. IEC C19 Socket	
				Integrated Monitoring	
				Temperature, Humidity, Door Switch Sensor, Access Control, Water Leak Sensor and Camera Based Local Surveillance,Events Alerts, SNMP, Email notification	
14	**Rack Mountable KVM switch with built-in monitor capable of connecting 16 inputs:**	1		1U rack mount	
				17" or 19" LED-backlit LCD monitor	
				BIOS-level access	
				Hot pluggable - add or remove computers without having to power down the switch	
				One console controls at least 16 computers directly	
				Multiplatform support: Windows, Linux, Unix, HP-UX, SUN Solaris.	
				Computer selection via front panel buttons, hotkeys, or On Screen Display	
				BIOS-level access	
				Auto PS/2 and USB interface detection.	
				Firmware upgradeable	
				Fully compliant with USB specification.	

				Dual interface – support computers with PS/2 or USB keyboard and mouse.	
				All necessary interface cables	
				3 year On-site comprehensive Warranty	
15	**KVM Switch(Minimum 4 Ports)**	4		Direct Computer Connections: 4 or more	
				Port Selection Hotkey, Pushbutton, on screen display (OSD)	
				Console Ports	
				2 x USB Type ,1 x HDB-15 1 x Mini Stereo Jack ,1 x Mini Stereo Jack	
				KVM Ports	
				Console Keyboard Connector:1 x USB	
				Console Mouse Connector- 1 x USB	
				Console Video Connector- 1 x VGA-15 pin female(2048 x 1536; DDC2B)	
				Console Audio Connectors- 1 x Mini-DIN Speaker Port, 1 x Mini DIN Microphone port	
				4 KVM Cables with each Switch	
16	**Backup storage solution**	1 No.		Rack mountable: 1U/2U	
				Capacity: Minimum 30 TB usabale capacity (300 TB logical capacity) or higher	
				Atleast one quad port 10 GbE, one 16 GBPS dual port FC card and dual port 1 GbE card	
				Protocol support: NFS, CIFS, OST, VTL	
				Deduplication and compression ratio of 10:1	
				Throughput: 20TB/hr	
				Backup solution should be image level backup solution specifically designed for Virtual Environments.	
				Proposed backup appliance should have single deduplication pool across all protocols, data types and backup softwares to achieve maximum storage optimization.	
				Proposed backup appliance should have RAID 6 and hot spare.	

				Backup solution should be totally agentless but should support application aware backup processing including truncation of MS MS SQL, Exchange transaction logs.	
				Backup solution should be Hardware Agnostic Solution and it should support any type of storage for storing the Backups.	
				Backup solution should store a backup recovery point as a single file.	
				The proposed backup solution must support at least AES 256-bit encryption capabilities.	
				Backup solution should include inline de duplication and compression of backup files.	
				Backup files should be self-sufficient and recovery should not depend on files catalog or indexing.	
				Backup solution should support file level recovery from an image level backup of Windows\Linux\ Solaris guest file systems.	
				Backup solution should provide the RTO equal to High Availability and be able to boot the Virtual Machines directly from the Backup to reduce the downtime.	
				Backup solution should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO.	
				Solution shall have native feature for Automated Backup Verification.	
				Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.	
				Solution should provide instant server recovery in the Sandbox for server testing purposes.	
				Solution should provide Backup and Replication capabilities in one console.	
				The solution should support Windows as well as Linux different flavors	

				The Solution should support varieties of backup mechanisms like Full, Incremental, Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.	
				Replication should include failover and failback capabilities	
				Solution should be Agentless and should not require license, deploy, manage or monitor on hosts or VMs.	
				Solution should support 24x7 real-time monitoring and views of health, performance and workload of the virtual hosts.	
				The proposed Backup Solution must Allow to configure the maximum acceptable I/O latency level for production datastores to ensure backup and replication activities do not impact storage Availability to production workloads.	
17	**Software defined infrastructure solution: Cloud solution including computing, network & storage virtualization and Management Server.**	20 CPU licenses (10 servers, Dual CPU)		All components must integrate into single solution and setup as a single solution on the rack mountable servers specified at S.No. 1 above.	
				I.Cloud & Virtual Server management Capabilities	
				The cloud solution should support Heterogeneous virtual environment provisioning.	
				The solution should also automate and provision data-center services such as compute, storage, networking, backup, replication, load balancing, fault tolerance, security and firewall.	
				The solution should provide resource reclamation functionality which identifies and reclaims inactive and abandoned resources by automating the decommissioning and reuse of retired resources.	
				The solution shall provide automated provisioning of infrastructure, applications and custom services through a unified, web-based, multi-tenant self-service IT service catalog to reduce IT service delivery times.	

				The solution shall allow authorized administrators, developers or business users to request new IT services and manage specific cloud and IT resources, while ensuring compliance with policies.	
				The solution shall support creation of services such as 'Single VM' and a 'Multi-tier application infrastructure (including software based constructs such as load balancers)' as part of a standard template and also provide ready integration with the proposed platform to automate delivery of networking & security services such as switching, routing, load balancing and firewalling.	
				The solution shall support multiple levels of approval integrated with email notifications such that approvals/rejections can be done without having to login to the self-service portal.	
				The solution shall support extensibility capabilities to customize machine configurations and integrating machine provisioning /management with other enterprise-critical systems such as load balancers, configuration management databases IP address management systems, or Domain Name System (DNS) servers.	
				The solution shall extend operations capabilities to the requestor of the service (eg. ability to start/stop/suspend virtual machines, request additional resources and access the VM using RDP/SSH protocols) through the self-service portal based on entitlement.	
				The solution shall support granular role-based access control and entitlements of infrastructure services to consumers and allow administrators to manage and reserve (allocate a share of the memory, CPU and storage) resources for a group to use.	
				Solution should offer leases (time-limited provisioning of resources).	

				The solution should be able to define multiple tenants which would enable the administrators to create a secure multitenant infrastructure.	
				The solution should have the ability to create custom workflows to automate the delivery of anything as a service - XaaS (for example Email, Storage as a Service, Network as a Service , Backup as a Service etc.)	
				The Solution should provide Infrastructure as a Service support for multi hypervisor environment including vSphere, Hyper-V, RHEV and XEN etc. and support provisioning of infrastructure in public , private and hybrid cloud etc.	
				The solution should provide abstraction of application-specific deployment logic from the underlying cloud infrastructure which would allow true separation between applications and infrastructure and would enable reuse of the same blueprint on multiple virtual and cloud infrastructures.	
				The solution should provide Simple and Automated Application Provisioning capabilities along with the graphical drag-and-drop canvas for creating application blueprints that would make planning and deploying complex applications easily.	
				The solution provided automation of operations such as provisioning a virtual machine or adding storage capacity should cover peripheral systems such as a configuration-management database, IP address management, load balancing, monitoring and other management systems. As a result, the entire process can be automated without necessitating any manual cycles.	
				Should be able to integrate with Vmware ESXi platform.	
				The solution should provide complete visibility into all levels of infrastructure and applications through a single management console for multiple hypervisors, plus physical and cloud environments.	

				The solution should be able to monitor the performance and health of underlying hypervisor and physical environment.	
				The solution should provide templates to ensure the hypervisor hardening, change, configuration and regulatory compliance, capability to automatically name and continuously update application components and version numbers, infrastructure & operations analytics and also policy-based configuration management which would assure compliance for virtual and physical environment.	
				The solution should have deep configuration data collection, change tracking, compliance assessment and remediation of noncompliant configurations across virtual & physical infrastructure and also provide unified reporting of configuration data and compliance assessment results for virtual & physical environment.	
				The solutions should provide Monitoring of OS level resources (CPU, disk, memory, network) for Windows and Linux OS and physical hardware resources of the hosts.	
				The solution should provide flexible group policies which would let admin to define specific health, risk and capacity thresholds, alert types and notifications, business hours and many other configuration settings at a group level to prioritize operational activities for business critical applications, production workloads or business units.	
				The solution should provide self-learning performance analytics and dynamic thresholds which can adapt to the environment to simplify operations management and eliminate false alerts and based on Historical data and trending, solution should be able to send proactive smart alerts to avoid potential downtime.	
				II. Computing/Server Virtualization	
				Bare Metal Solution: Install directly on the bare metal server hardware with no dependence on a general purpose OS.	

				Guest OS: Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.	
				VM Capability: Create Virtual machines with up to 120+ virtual processors, 2+ TB virtual RAM and 2+ GB Video memory in virtual machines for all the guest operating system supported by the hypervisor.	
				VM Live Migration: Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option, no disruption to users or loss of services.	
				Storage Live Migration: Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.	
				High Availability: In case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software and also should be able to proactively identify the capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.	
				On the fly resource addition: CPU, Memory & devices to virtual machines can be added when needed without disruption in working for both windows and Linux based VMs.	
				VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.	
				Enforcing security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits.	
				Support boot from iSCSI, FCoE, and Fibre Channel SAN.	

				Integrate with NAS, FC, FCoE and iSCSI SAN infrastructure leveraging high performance shared storage to centralize virtual machine file storage for greater manageability, flexibility and availability.	
				Virtual Switch: Span across a virtual datacenter and multiple hosts should be able to connect to it. In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.	
				Replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level.	
				Backup and recovery for virtual machines should allow admins to backup virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability.	
				III. Network Virtualization	
				Logical Switching – Reproduce the L2 and L3 switching functionality in a virtual environment, decoupled from underlying hardware.	
				Logical Routing – Routing between logical switches, providing dynamic routing within different virtual networks	
				Logical Firewall – Distributed firewall, kernel enabled line rate performance, virtualization and identity aware, with activity monitoring.	
				Logical Load Balancer – Solution should provide a server load balancer with features like SSL offload.	
				Logical VPN – The solution should provide L2VPN, SSLVPN, site-to-site IPSEC VPN services.	
				It should support deployment of multiple instances of virtual networks independent of each other.	
				The solution shall provide a networking & security virtualization layer that allows delivery of network services in software.	

				On-demand network creation, define routed, NAT or Private network profiles based on application topology, creation of security groups based on existing security policies.	
				The solution should enable integration of third-party network and security solutions & and offer logical switches on virtualized infrastructure.	
				The virtualization solution should offer to bridge VXLAN layer2 Networks and VLAN based networks	
				The Solution should offer Centrally managed distributed L2-L4 stateful firewall that is kernel-level integrated into the virtualized host architecture.	
				The distributed firewall should be embedded in-kernel in host architecture and should provide atleast 15 Gbps or better performance per host	
				The solution should offer to Integrate with solutions for antivirus, malware, and intrusion prevention.	
				The solution should offer to Create, change, and manage security policies across all Virtual Networks.	
				The solution should provide industry-standard IPSec and SSL VPN capabilities that enables securely extending the virtual datacenter.	
				The solution should provide support for the Netflow.	
				The Platform should model the entire Data Center and tie together visibility across the domains of compute, network and security for physical, virtual and cloud.	
				The software should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting.	
				The Platform should be able to generate report that includes amount of traffic that's East-West, Internet, VM to VM, VM to Physical, Hair-pinned and Unprotected.	
				The Users should be able to monitor all the virtual as well as physical hops on the path between two machines.	
				The Platform should be designed for agentless deployment.	
				IV. Storage Virtualization	

				Solution should offer Software defined Storage.	
				Solution should be capable to pools together server-attached flash devices and hard disks to provide shared datastore.	
				Combine storage capacity available with rack mountable servers mentioned at S.No.1 and allow the combined storage to use as Storage Area Network.	
				Storage should be available to VMs running in virtual environment.	
				Storage should be managed by cloud and management server	
				Support deduplication and compression.	
				Scalability of solution.	
				Policy based automation of the jobs.	
				Tight Integration with complete solution.	
18	**Adobe Media Server Professional 5 64-bit**	1 License		On-demand packaging for HTTP	
				Robust media origin services	
				Adobe Access DRM Support	
				Application-level multicast	
				Studio-grade DRM packaging	
				Advanced disk management for HTTP.	
19	**Print2Flash Commercial 3.4 [Server Mode] 64-bit**	1 License		Server mode 64 bit	
20	**Microsoft Office 2016 Professional Plus 64 bit**	5 Licenses		Professional Plus 64 bit or latest	
21	**Windows Server 2016 with downgradable option 64 bit**	1 License		Datacenter edition	
22	**Microsoft Windows Server 2016 64 bit(Standard Edition)**	4 Licenses		standard edition	
23	**Microsoft Windows Server 2016 64 bit(Datacenter Edition)**	5 Licenses		Datacenter Edition	
24	**Acrobat Pro DC**	2 Licenses		Compatible with Windows 7, 8 and 10 or Mac OS X v10.9 and v10.10.	
				Edit or export PDFs to Office.	
				Add audio and video files to PDFs.	
25	**Microsoft Visio Professional 2016 or Latest 64 bit**	2 Licenses		It should be Professional 2016 64 bit or latest version	

26	**Microsoft Windows 10 Professional 64 bit**	2 License		Professional 64 bit or latest	
27	**Microsoft Project Professional or Latest 2016 64-bit**	2 Licenses		It should be Professional 2016 64 bit or latest version.	
28	**Cisco Adaptive Security Virtual Appliance Standard or latest**	4 Licenses		Throughput 1 Gbps or higher	
				3DES/AES VPN throughput 125 Mbps Connections per second 20000	
				VLANs 50 Concurrent sessions 100000	
				Hypervisor Support	
				Virtual CPUs : 1	
				Memory 2 GB or higher	
				Storage at Least 8 GB or higher .	
29	**Residential Engineer**	1		The vendor shall depute One qualified Full Time resident engineer to the CERT-In on every working day (working hours:9.00 am to 5.30 pm) including Saturday and if required even on Holiday/ beyond working hours too.	
				Resident engineer provided by the vendor are to the satisfaction of the CERT-In.	
				The Resident Engineer as asked in the tender should be on direct role of the bidder and should be employed by the bidder in compliance with relevant Govt. acts of employment fulfilling statutory obligations including but not limited to provident fund, ESI, etc. An undertaking to this effect should be submitted by the Bidder.	
				The resident engineer should possess Bachelor's/ Master's degree in Engineering/Technology/ Computer Applications.	
				The vendor shall provide a suitable replacement of the Engineer deputed in case of his leave/absence.	
				The Resident engineer is expected that would be proficient in maintenance of IT infrastructure ,hardware, software and networking.	

				The resident engineer should be conversant with installation and configuration of cloud solution & backup software supplied.	
				Monitoring and troubleshooting LAN/Firewall//VPN/intranet etc. Configuration of printers and other Network peripherals on the network.	
				It will also be the responsibility of the Resident Engineers to lodge maintenance calls & follow-up.	
				Daily call and resolution reporting, infrastructure health status reporting, usage reporting, exception reporting.	
				All the expenses including salary/bills will be borne by the bidder.	
				Resident engineer will report to head of Cyber security assurance lab	
				Resident engineer will be required to work as per requirement of team for conducting tests.	
				Resident engineer will be responsible for all updates/patch installation in lab.	
				Any other activity/duties assigned to resident engineer, which is necessary for operation of lab.	