Tender No. 2(63)/2017-CERT-In

Tender Document

For
Procurement of Hardware and Software License/Tools for Cyber Threat Information Exchange Facilities at CERT-In

Issued by:

Director General,
CERT-In

Government of India
Ministry of Communications and Information Technology
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/tools for setting up Cyber Threat Information Exchange facility 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 chain Department of Electronics and Information Technology (DeitY), CERT-In

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 Govt. 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 Supporting Documents Cover
   c. Commercial Bid

7. . The cover for the bids should bear the following inscription.
   “Quotation for Hardware & software for Cyber Threat Information Exchange Facility"
   Tender No. 2 (63)/2017-CERT-In
   Closing date & Time for submission of bids: 27.12.2017 upto 4:00 PM”

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 and online 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:

(Admin), 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 e-procurement portal.
    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 major 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 authority letter in prescribed format

18. DG CERT, 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, 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.100 Crores through sales of Hardware and Software for the last three financial years. The bidder organization should be a profitable organization for the last 3 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/OEM/Authorized partner for items no. 1 to 5, 11,12,13 and 14 to 16 . It is to be addressed to CERT-In, Ministry of

Electronics and Information Technology. For other items an undertaking could be submitted by the bidders that they will support the items for the warranty and the AMC period.

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 for the next two years after completion of the warranty period, as applicable. Bids received without the renewal quotes will be summarily rejected.

27. The bidder must quote for all the items for a total period of three years including the current year. The Cost and taxes should be indicated separately.

28. Total cost for the three years including taxes will be considered for calculating the L1 bidder. Orders will be placed for each year separately on successful completion of the previous year.

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 both the bids – technical and commercial.

30. The hardware and license for the Software Application / Tools 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. 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 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. Bidders may consider forming consortium if necessary. The qualification and eligibility criteria as provided in the document will have to be met by Principle Partner of consortium who will submit the bid. All the consortium members will share the responsibility jointly and severally. The bid document must clearly bring out the responsibility of each consortium partner.

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

44. 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.

45. **Pre-bid Meeting:** CERT-In shall hold a pre-bid meeting with the prospective bidders on **07.12.2017 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.

46. 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.

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

48. 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.

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

50. Incomplete quotations are liable to be rejected.

51. 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.

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

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

54. 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.

55. 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. The rates must be quoted strictly as per the 'Bill of Material' provided in Annexure-I of the Tender Document.

SUPPLY

56. 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.

57. 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.

.**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. 20 lakhs/- (Rupees Twenty 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 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) Upto 90% of the total payment shall be processed for payment by CERT-In on receipt of the pre-receipted bills in triplicate after delivery and satisfactory completion of installation, commissioning, testing and acceptance of the items and balance 10% payment would be released after expiry of the standard warranty period. 100% of the remaining payment may also be released on receipt of the pre-receipted bills in triplicate after delivery and satisfactory completion of installation, commissioning, testing and acceptance of the equipment, if the firm submits the Bank Guarantee for Performance Security of the amount equivalent to 10% of the quoted price, which should be valid for the 60 days beyond the duration of the warranty period.

65. **PERFORMANCE SECURITY**

The successful bidder shall submit a Performance Security of 10% of the cost of the equipment within 15 days of the placement of purchase order. The Performance Security should be in the form of Bank Guarantee of any Indian Nationalized Bank. The Bank Guarantee should be valid for 60 days beyond the duration of the warranty period. 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 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. The bidder is required to quote for comprehensive renewal charges for each of the next two years separately after the completion of warranty period, in the given table for submitting the quotes.
2. Quoted price bid for the item plus respective quoted comprehensive renewal charges for that item for the next two years will be considered for calculating the L1 Bidder.
3. For the hardware maintenance/Firmware upgrade/software license renewal/ subscription of the software application / tools, the purchase order for the same will be awarded on annual basis, subject to previous satisfactory services.
4. Bill of Material' is available on website as the Annexure-I.
5. 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.
6. The e-token that is registered should be used by the bidder and should not be misused by others.
7. DSC once mapped to an account cannot be remapped to any other account.
8. 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.
9. 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.
10. The BOQ template 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.
11. 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.
12. Bidder, in advance, should prepare the bid documents to be submitted. If there is more than one document, they can be clubbed together.
13. 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.
14. The bidder reads the terms and conditions and accepts the same to proceed further to submit the bids
15. 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.
16. 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.
17. 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: rack mountable - (1U/2U)** • Rack Mounted with railing (1U/2U) • Dual processor - Intel Xeon E5-2600 v4, 22 core per processor with 2.5MB per core cache or higher • Memory : 512 GB or higher DDR4 RAM with upgrade option upto 1.5 TB • RAID levels 0, 1, 5, 6, 50 • DVD+/-RW Drive • Internal storage at least 10TB, 10K rpm SAS HDD hot plug • Integrated 4 port 10 Gigabit Ethernet (GbE) • At least 2 USB Port, 1 serial port • Redundant Power Supply	04
2.	**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
3.	**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
4.	**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
5.	**Laptops:** • 8th Generation Intel Core i7 processor (i7-8650U, i7-8550U) or latest • At least 32 GB DDR4-2133 non-ECC SDRAM (Transfer rates up to 2133 MT/s) • NVIDIA Quadro M620 (2 GB GDDR5 dedicated) • Internal memory: 512 GB SSD • Display: 14.0-inch or less diagonal multi-touch & anti-glare treatment; (10 bit supporting up to 1 billion colors).Supports multi-display, including up to three displays without the use of a docking solution, with hybrid graphics enabled. • Intel Dual Band Wireless-AC 8265 802.11a/b/g/n/ac (2x2) Wi-Fi and Bluetooth 4.2 Combo 5 • Full size premium backlight Bluetooth Keyboard with gestures support; integrated smart card reader • Thunderbolt 3 (Data Transfer up to 40 Gb/s, Power Delivery, DP1.2, Sleep and Charge); 1 USB 3.1 Gen 1 (Sleep and Charge); 1 headphone/microphone combo. • Expansion slots:1 microSD media card reader • 720p HD webcam with IR (front-facing) • Weight :less than 2.25 Kg • Windows 10 Professional or latest [64 bits] • Microsoft office 2016 or latest (Business) • Leather Sleeve and Backpack,Stylus, Charging adapter and battery.	2

	• Good Quality branded Laptop bag (backpack)	
6.	**MacBook Pro** • 3.1GHz dual-core Intel Core i5 [or latest series], Turbo Boost up to 3.5GHz, with 64MB of eDRAM • Retina display 13.3-inch (diagonal) LED-backlit display with IPS technology; 2560x1600 native resolution at 227 pixels per inch with support for millions of colours • 512GB PCIe-based onboard SSD / 16GB/8GB [latest] of 2133MHz LPDDR3 onboard memory • Full-sized backlit keyboard • Touch Bar with integrated Touch ID sensor • Ambient light sensor • Multi-Touch gestures ,Force Touch trackpad for precise cursor control and pressure-sensing capabilities • Charging and Expansion ports • Connectivity: • 802.11ac Wi-Fi wireless networking; IEEE 802.11a/b/g/n compatible • Bluetooth 4.2 or latest wireless technology • Camera and video support • Native DisplayPort output over USB-C • Video / display Connectivity adaptors: VGA, HDMI and Thunderbolt 2 output supported using adapters • Microsoft office Business for Mac Latest Version. • Separate media and license of Microsoft Windows 10 OS. • Good Quality branded Laptop bag (backpack).	2
7.	**Display Adaptors** • VGA-HDMI-DVI-converters	2
8.	**Rack** • Industry Standard 42U server rack. • 1 fixed shelf • 2 vertical power strips (at least 10 sockets each) • Perforated doors.	1
9.	**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 • Auto PS/2 and USB interface detection.	1

	• Firmware upgradeable • Fully compliant with USB specification. • Dual interface – support computers with PS/2 or USB keyboard and mouse. • All necessary interface cables	
10.	**Portable Storage Devices** • 4TB portable USB harddisks • USB 3.0 • USB powered/ No external Power supply • Carrycase	4
11.	**Network Intrusion Prevention System** • Hardware dedicated appliance. • Atleast should have a Intrusion Prevention System (IPS) throughput of 800 Mbps and threat prevention throughout of 250Mbps in production environment. • Lab ideal testing condition minimum throughput should be atleast 3Gbps. • Features of Threat Emulation and Threat Extraction for complete protection against the sophisticated threats and zero-day vulnerabilities. • Capability to remove exploitable content, including active content and embedded objects, • Capability of reconstruction of files to eliminate potential threats. • atleast 10 x 1GbE ports, 4x x 1Gb SFP interface card, transceivers and 16 GB of memory for high connection capacity. • The user should be able to manage and monitor the appliance locally • Technical support from OEM.	1
12.	**SAN Storage** • 32TB SAS Storage 2 x 40GbE or 4 x 10GbE • Form Factor: 2U/4U chassis with two HA controllers and 24 SSD slots • SMB (CIFS), NFS, HTTP/S, FTP/S, iSCSI Block over Ethernet, • Features: Deduplication, snapshots, replication, file classification, file screening and quotas.	1
13.	**SAN switch** • 1 x 24 port 8G FC SAN switch with 8 licensed ports on each switch and web tools, zoning, enhanced group Management, full fabric and enterprise bundle. • 16 nos. of 10m LC- LC 8G FC cables	2

II. Software/Tools

S.No.	**Name Of the Software**	**Featured Required in the Software**	**Qty**

14	**TAXII Server**	• (OS/Virtualization Software/Hypervisor and any other software/hardware required to run this solution at servers at s.no. 1 needs to be supplied by bidders with no additional cost to CERT-In). • The central manager collects, process, disseminates data feeds, cyber threat intelligence information between parties, in a hub-spoke model. • Should have the capabilities to integrate threat feeds from selected Collection of Open Source Intelligence feeds, transformed to STIX, locally generated feeds, and can consume from other pers. • Authentication: supports session-less token-based authentication as primary method of authentication with fallback to Basic authentication. • TLP management of the data being shared. TLP red tagged data should be short lived and delete after a prescribed interval. • Support for STIX 2.0 alongwith STIX 1.0 • Support for Two Factor Authentication • Allow Source and Collection Management • Create STIX object based on a manual Form, from a pattern e-Mail, and CSV file and Yara object. • STIX object visualization • Integrations of threat intelligence with security applications and devices such as SIEMS. • Define custom actions based on dynamic rules. • Automatic Ingestion of shared threat Intel data into local knowledge database with context and discretion requiring minimal human resources. • Advanced Sharing options: Subscription Management, Dynamic Rule Based Sharing, Client Information. • Export Data in CSV, PDF, JSON and other formats. • TLS v2 based communication with Clients and end to end secure authentication, authorization and communication with clients. • Custom User Roles and Permissions for different levels of user. • Machine Learning based analysis to reduce noise, remove duplicate threat intelligence and use machine learning to correlate information for threat actor and respective campaigns. • Advanced Alerting and Notification such as Receive automatic alerts based on aggregated	1

		customized confidence score; Email and SMS Notifications. • Block-chain enabled identity management /authentication mechanism. • Define rules for different feeds or different types of STIX Objects. • Customization of server as per requirements. • Integration with different organizations need to be facilitated by bidder/OEM. • Analysis Engine to allow Management of ordered Data Collection. A TAXII Data Feed's organization allows specific portions of TAXII Data Feeds to be requested. • Integration of various publically available API's, free and commercials. • Portal / Dashboard for the user to manage the threat feeds.	
15	**Taxii Client**	• Customized Taxii Client. • Full control of client and messages with agency managing TAXII. • Customized as per requirement. • Inbox Service - to push information to a TAXII Server. • Poll Service - to request information from a TAXII Server. • Collection Management Service - to request information about available Data Collections or request a subscription. • Discovery Service - to discover available TAXII Services. • Support for STIX 2.0 alongwith STIX 1.0	1
16	**Server Hardware Virtualization software and Virtualization Managemen Server**	• Solution has to be installed in Server listed at s.no. 1. • Virtualization platform that provides server Virtualization which would be compatible with hardware and can manage all operations of a mini data center to run proposed STIX/TAXII solutions. • Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS. • Virtualization software shall allow heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux. • Virtualization software should be able to boot from iSCSI, FCoE, and Fibre Channel SAN • Virtualization software shall integrate with NAS, FC, and iSCSI SAN • Virtualization software shall have the capability for creating virtual machine templates to provision new servers • Virtualization software shall allow taking point-in-time snapshots of the virtual machines to	4 servers (8 CPU) hardware virtualization and 1 Virtualization Management Server.

		be able to revert back to an older state • Virtualization software should have the ability to thin provision disks to avoid allocating all storage space upfront. • Virtualization software should have the ability to live migrate VM files from one storage array to another without any VM downtime. • Virtualization software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure. • The solution should manage anti-virus and anti-malware policies for virtualized environments with the same management interfaces used to secure physical infrastructure • Virtualization software should provide 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 • Virtualization software should allow configuring each virtual machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address, must support NIC teaming for load sharing and redundancy. • Virtualization software shall allow creating virtual switches that connect virtual Machines • Virtualization software shall support configurations of VLANs which are compatible with standard VLAN implementations from other vendors • Virtualization software should provide solution to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers. • The solution should support enforcing security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits. • Virtualization software shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines • Virtualization software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues. • Virtualization software shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected	

		physical hosts. • Virtualization software should provide VM-level encryption protects unauthorized data access both at-rest and in-motion • Management server to provide centralized web based console to manage all virtualized servers from single location. Management interface should have capability to manage the virtual machines and allocation of resources.	
17	**Paterva Maltego eXtra Large [XL]**	Subscription /Annual	1
18	**Virus Total Intelligence**	Subscription /Annual	1
19	**SHODAN API small business**	Subscription/ small business plan annual	1
20	**MAXQDA Analytics Pro Single User**	Perpetual License - Professional Single user license	1
21	**ATLAS.ti Single User**	Commercial or Government Single User License for Windows and MAC	1
22	**IBM SPSS Statistics Professional**	1 year subscription Profession Edition	1
23	**Microsoft Visio Professional 2016 or Latest 64 bit**	Microsoft Visio Professional 2016 or Latest 64 bit	2
24	**Microsoft Project Professional or Latest 2016 64-bit**	Microsoft Project Professional or Latest 2016 64-bit	2

III. Residential Engineer

S.No.	**Residential Engineer**	**Description of Services**	**Qty**
25	**To be deputed from STIX/TAXII Software OEM**	• The OEM of TAXII 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.	**1**

		• The resident engineer should possess Bachelor’s/ Master’s degree in Engineering/Technology/ Computer Applications. • The OEM 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 upgradation, cutomization, installation and configuration TAXII server and Client. • Monitoring and troubleshooting proposed setup. • 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 be responsible for all updates/patch installation in lab. • Any other activity/duties assigned to resident engineer, which is necessary for operation of lab.	

Annexure-II

Technical Compliance Sheet

S.no.	Item Name	Quantity	Product Offered by Bidder	Technical Specifications	Compliance (Yes/No)
1	Server (type: rack mountable - (1U/2U)	4		Rack Mounted with railing (1U/2U)	
				Dual processor - Intel Xeon E5-2600 v4, 22 core per processor with 2.5MB per core cache or higher	
				Memory : 512 GB or higher DDR4 RAM with upgrade option upto 1.5 TB	
				RAID levels 0, 1, 5, 6, 50	
				DVD+/-RW Drive	
				Internal storage at least 10TB, 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	Router	1		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	
3	Hardware based Firewall	1		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	
4	Rack Mountable Managed Switch(1U)	2		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)	
5	Laptops	2		8th Generation Intel Core i7 processor (i7-8650U, i7-8550U) or latest	
				At least 32 GB DDR4-2133 non-ECC SDRAM (Transfer rates up to 2133 MT/s)	
				NVIDIA Quadro M620 (2 GB GDDR5 dedicated)	
				Internal memory: 512 GB SSD	
				Display: 14.0-inch or less diagonal multi-touch & anti-glare treatment; (10 bit supporting up to 1 billion colors).Supports multi-display, including up to three displays without the use of a docking solution, with hybrid graphics enabled.	
				Intel Dual Band Wireless-AC 8265 802.11a/b/g/n/ac (2x2) Wi-Fi and Bluetooth 4.2 Combo 5	

				Full size premium backlight Bluetooth Keyboard with gestures support; integrated smart card reader	
				Thunderbolt 3 (Data Transfer up to 40 Gb/s, Power Delivery, DP1.2, Sleep and Charge); 1 USB 3.1 Gen 1 (Sleep and Charge); 1 headphone/microphone combo.	
				Expansion slots:1 microSD media card reader	
				720p HD webcam with IR (front-facing)	
				Weight :less than 2.25 Kg	
				Windows 10 Professional or latest [64 bits]	
				Microsoft office 2016 or latest (Business)	
				Leather Sleeve and Backpack,Stylus, Charging adapter and battery.	
				Good Quality branded Laptop bag (backpack)	
6	MacBook Pro	2		3.1GHz dual-core Intel Core i5 [or latest series], Turbo Boost up to 3.5GHz, with 64MB of eDRAM	
				Retina display 13.3-inch (diagonal) LED-backlit display with IPS technology; 2560x1600 native resolution at 227 pixels per inch with support for millions of colours	
				512GB PCIe-based onboard SSD / 16GB/8GB [latest] of 2133MHz LPDDR3 onboard memory	
				Full-sized backlit keyboard	
				Touch Bar with integrated Touch ID sensor, Ambient light sensor	
				Multi-Touch gestures ,Force Touch trackpad for precise cursor control and pressure-sensing capabilities	
				Charging and Expansion ports	
				802.11ac Wi-Fi wireless networking; IEEE 802.11a/b/g/n compatible	
				Bluetooth 4.2 or latest wireless technology	
				Camera and video support	
				Native DisplayPort output over USB-C	
				Video / display Connectivity adaptors: VGA, HDMI and Thunderbolt 2 output supported using adapters	

				Microsoft office Business for Mac Latest Version.	
				Separate media and license of Microsoft Windows 10 OS.	
				Good Quality branded Laptop bag (backpack).	
7	Display Adaptors	2		VGA-HDMI-DVI-converter	
8	Rack	1		Industry Standard 42U server rack.	
				1 fixed shelf	
				2 vertical power strips (at least 10 sockets each)	
				Perforated doors.	
9	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	
				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	
10	Portable Storage Devices	4		4TB portable USB harddisks	
				USB 3.0	
				USB powered/ No external Power supply	
				Carrycase	
11	Network Intrusion Prevention System	1		Hardware dedicated appliance.	
				Atleast should have a Intrusion Prevention System (IPS) throughput of 800 Mbps and threat prevention throughout of 250Mbps in production environment.	

				Lab ideal testing condition minimum throughput should be atleast 3Gbps.	
				Features of Threat Emulation and Threat Extraction for complete protection against the sophisticated threats and zero-day vulnerabilities.	
				Capability to remove exploitable content, including active content and embedded objects,	
				Capability of reconstruction of files to eliminate potential threats.	
				atleast 10 x 1GbE ports, 4x x 1Gb SFP interface card, transceivers and 16 GB of memory for high connection capacity.	
				The user should be able to manage and monitor the appliance locally	
12	SAN Storage	1		32TB SAS Storage 2 x 40GbE or 4 x 10GbE	
				Form Factor: 2U/4U chassis with two HA controllers and 24 SSD slots	
				SMB (CIFS), NFS, HTTP/S, FTP/S, iSCSI Block over Ethernet	
				Features: Deduplication, snapshots, replication, file classification, file screening and quotas.	
13	SAN Switch	2		1 x 24 port 8G FC SAN switch with 8 licensed ports on each switch and web tools, zoning, enhanced group Management, full fabric and enterprise bundle.	
				16 nos. of 10m LC- LC 8G FC cables	
14	TAXII Server	1		OS/Virtualization Software/Hypervisor and any other software/hardware required to run this solution at servers at s.no. 1 needs to be supplied by bidders with no additional cost to CERT-In).	
				The central manager collects, process, disseminates data feeds, cyber threat intelligence information between parties, in a hub-spoke model.	

				Should have the capabilities to integrate threat feeds from selected Collection of Open Source Intelligence feeds, transformed to STIX, locally generated feeds, and can consume from other pers.	
				Authentication: supports session-less token-based authentication as primary method of authentication with fallback to Basic authentication.	
				TLP management of the data being shared. TLP red tagged data should be short lived and delete after a prescribed interval.	
				Support for STIX 2.0 alongwith STIX 1.0	
				Support for Two Factor Authentication	
				Allow Source and Collection Management	
				Create STIX object based on a manual Form, from a pattern e-Mail, and CSV file and Yara object.	
				STIX object visualization	
				Integrations of threat intelligence with security applications and devices such as SIEMS.	
				Define custom actions based on dynamic rules.	
				Automatic Ingestion of shared threat Intel data into local knowledge database with context and discretion requiring minimal human resources.	
				Advanced Sharing options: Subscription Management, Dynamic Rule Based Sharing, Client Information.	
				Export Data in CSV, PDF, JSON and other formats.	
				TLS v2 based communication with Clients and end to end secure authentication, authorization and communication with clients.	
				Custom User Roles and Permissions for different levels of user.	
				Machine Learning based analysis to reduce noise, remove duplicate threat intelligence and use machine learning to correlate information for threat actor and respective campaigns.	

				Advanced Alerting and Notification such as Receive automatic alerts based on aggregated customized confidence score; Email and SMS Notifications.	
				Block-chain enabled identity management /authentication mechanism.	
				Define rules for different feeds or different types of STIX Objects.	
				Customization of server as per requirements.	
				Integration with different organizations need to be facilitated by bidder/OEM.	
				Analysis Engine to allow Management of ordered Data Collection. A TAXII Data Feed's organization allows specific portions of TAXII Data Feeds to be requested.	
				Integration of various publically available API's, free and commercials.	
				Portal / Dashboard for the user to manage the threat feeds.	
15	Taxii Client	1		Customized Taxii Client.	
				Full control of client and messages with agency managing TAXII.	
				Customized as per requirement.	
				Inbox Service - to push information to a TAXII Server.	
				Poll Service - to request information from a TAXII Server.	
				Collection Management Service - to request information about available Data Collections or request a subscription.	
				Discovery Service - to discover available TAXII Services.	
				Support for STIX 2.0 alongwith STIX 1.0	
16	Server Hardware Virtualization software and Virtualization Management	4 servers (8 CPU) hardware virtualization and 1		Solution has to be installed in Server listed at s.no. 1.	
				Virtualization platform that provides server Virtualization which would be compatible with hardware and can manage all operations of a mini data center to run proposed STIX/TAXII solutions.	

	Server	Virtualization Management Server.		Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS.	
				Virtualization software shall allow heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux.	
				Virtualization software should be able to boot from iSCSI, FCoE, and Fibre Channel SAN	
				Virtualization software shall integrate with NAS, FC, and iSCSI SAN	
				Virtualization software shall have the capability for creating virtual machine templates to provision new servers	
				Virtualization software shall allow taking point-in-time snapshots of the virtual machines to be able to revert back to an older state	
				Virtualization software should have the ability to thin provision disks to avoid allocating all storage space upfront.	
				Virtualization software should have the ability to live migrate VM files from one storage array to another without any VM downtime.	
				Virtualization software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure.	
				The solution should manage anti-virus and anti-malware policies for virtualized environments with the same management interfaces used to secure physical infrastructure	
				Virtualization software should provide 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	

				Virtualization software should allow configuring each virtual machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address, must support NIC teaming for load sharing and redundancy.	
				Virtualization software shall allow creating virtual switches that connect virtual Machines	
				Virtualization software shall support configurations of VLANs which are compatible with standard VLAN implementations from other vendors	
				Virtualization software should provide solution to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers.	
				The solution should support enforcing security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits.	
				Virtualization software shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines	
				Virtualization software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues.	
				Virtualization software shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.	
				Virtualization software should provide VM-level encryption protects unauthorized data access both at-rest and in-motion	

				Management server to provide centralized web based console to manage all virtualized servers from single location. Management interface should have capability to manage the virtual machines and allocation of resources.	
17	Paterva Maltego eXtra Large [XL]	1		Subscription /Annual	
18	Virus Total Intelligence	1		Subscription /Annual	
19	SHODAN API small business	1		Subscription /Annual	
20	MAXQDA Analytics Pro Single User	1		Subscription/ small business plan annual	
21	ATLAS.ti Single User	1			
22	IBM SPSS Statistics Professional	1		Perpetual License - Professional Single user license	
23	Microsoft Visio Professional 2016 or Latest 64 bit	2		Commercial or Government Single User License for Windows and MAC	
24	Microsoft Project Professional or Latest 2016 64-bit	2		Microsoft Project Professional or Latest 2016 64-bit	
25	Residential Engineer (To be deputed from STIX/TAXII Software OEM)	1		The OEM of TAXII 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 should possess Bachelor's/ Master's degree in Engineering/Technology/ Computer Applications.	
				The OEM 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 upgradation, customization, installation and configuration TAXII server and Client.	
				Monitoring and troubleshooting proposed setup.	
				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 be responsible for all updates/patch installation in lab.	
				Any other activity/duties assigned to resident engineer, which is necessary for operation of lab.	