ITI Limited

ITI Corporate Office
(Projects & Planning Division)
ITI Bhavan
Dooravani Nagar
BANGALORE – 560016

CIN No: L32202KA1950GOI000640

Tender

For Selection of Technology Partner to setupMulti-Service Platform / SOC

Ref: COR/PP/SOC/2021/02 **Dated:29th April,2021**

INTRODUCTION:

ITI Limited isa CPSUof Department of Telecom, Govt. of India, engaged in delivering large turnkey projects,in the field of IT/Telecom/networking and working as Master System Integrator for Planning, Manufacturing, Design, Supply, Installation, commissioning and maintenance of PAN India IT and Telecom related infrastructure and services. ITI is invitingproposal from eligible and competent business entities to setup a Multi-Service Platform at our premises to monitor, detect, contain, and remediate IT threats across critical applications, devices, and systems in our customer's physical & virtual IT environments.

ITI has been operating Tier-3 compliant Data Centre in its Bangalore plant where the services like Aadhaar authentication, E-banking and ERP services are provided. Various Data Centre services like Colocation (co-hosting), Managed services, e-mailing services are provided to various customers like PSU, Banking, Corporate and private as well as Start-ups. Company has also established 1000 racks capacity Data Centre and is providing various Cloud enabled service, managed and Colocation services.

In order to provide quality and competitive services to the customers, offers are invited from Intending Indian Multi-Service Providers (hereafter referred as IMSP)having expertise in relevant field of setting up a Multi-Service Platform.ITI would like to extend these Multi-Service Platform services toother organizations in India.

Accordingly, Proposals are invited through e-tenderfrom suchIMSPwho have the technical strength to deliver Multi-Service Platform / SOC for serving both on technology and business fronts.

The selection of theIMSP shall meet all the essential criteria and based on theirtechnical proposal and lowest Financial Quote as asked in Financial Bid.**Proposals are invited from IMSPs, under e-tender mode for Technical Proposal and Financial Proposal. The Due Date for submitting the bid is 20th May 2021 by 11:30 hours.**

The bids will be opened on is 20th May2021 at 16:00 hours.

Financial bids will be opened for only those IMSPs,qualifying the technical proposal evaluation. The date of financial bid opening will be intimated later.

1 CONTENTS

2 Tender Information 4
2.1 Technical Bid 5
2.2 Essential Eligibility Criteria For The Applicants 5
2.3 General Commercial Conditions 7
2.4 Bid Security Deposit (BSD) And Performance Bank Guarantee (PBG) 7
2.5 Technical Bid Evaluation 8
2.6 Financial Conditions 9
2.7 Financial Bid 10
2.8 Payment Terms 11
3 Instructions For Submitting Proposal Towards Tender 12
4 Check List Of Documents/Information To Be Submitted 14
5 Annexures 15
5.1 Annexure-I 15
5.2 Annexure-II 16
5.3 Annexure-III 17
5.4 Annexure- IV 18
5.5 Annexure- V 19
5.6 Annexure-VI 21
5.7 Annexure-VII 23
5.8 Annexure-VIII 24
5.9 Annexure-IX 29
5.10 Annexure-X 30
5.11 Annexure-XI 31
5.12 Annexure-XII 33
6 Detailed Scope Of Work Multi-Service Platform : 34
6.1 Identity & Access Management As A Service 35
6.2 Next Gen Firewall: 36
6.3 Network Access Control (NAC) 39
6.4 E-Mail Security: 40
6.5 Security Information And Event Management 41
6.6 End Point Detection And Response (EDR) 43
6.7 DLP (Data Loss Prevention) 45
6.8 Vulnerability Assessment And Penetration Testing 46
6.9 Analytics As A Service Includes Ueba 48
6.10 Multi-Service Platform Activities 49
7 Multi-Service Platform Minimum Requirements: 51
8 Warranty And Maintenance Support 52

9 SLAs And Penalties For Multi-Service Platform Individual Modules 54
10 Termination 66
11 Glossary 67

2 TENDER INFORMATION

	Type of tender	
i.	Number of bid submission stages for tender	Single stage bidding
ii.	Stages of Opening	Two (Note-2)
iii.	Bid Validity Period / Validity of bid Offer	150 days from the tender opening date.
iv.	**Note-1** The IMSP shall submit Technical& Financial bid simultaneously.	
v.	**Note-2** The bids will be evaluated technically first and thereafter financial bids of technically compliant ISMPs only shall be opened.	

2.1 TECHNICAL BID

	Scope of Work
i.	Planning, Engineering, Supply, Installation, Integration, Deployment, Testing, Commissioningand building of an Enterprise grade Multi-Service Platform at ITI datacenter in Bangalore, Warranty (1 year) and Operation and Maintenance supporton Turnkey Basis as per the requirements. (The detailed scope of work shall be read in conjunction with section 6 and Annexure-VII in the tender)
ii.	IMSPwould setup for various Multi-Service Platform services on comprehensive and standalone basis from ITI Multi-Service Platform (ex. IAM, Network security, Servers security, end point security, Data security (DLP), E-mail security, VAPT, UEBA (Analytics), SIEM, NG Firewall) to various customers. (The detailed scope of work has been mentioned in section 6 and Annexure-VII)
iii.	Support ITI for On Boarding of new customers for providing Multi-Service Platform servicesand for Cert-in Empanelment.

2.2 ESSENTIAL ELIGIBILITY CRITERIA FOR THE APPLICANTS

S.No	Pre-Qualification Criteria	Compliance Document
1	The IMSP must be a registered company in India (Public, Private, Partnership companies) under the Companies Act 2013 having at least five years of existence.	Certificate of Incorporation
2	The IMSP should have experience in providing Multi-Service Platform services in India for a minimum of three years as on 05.03.2021	PO copy or client's certificate substantiating the engagement which is 3 years or older.
3	The IMSP should have at least 20 crores turnover per year in the last 03 years (2017-18, 2018-19 and 2019-20,2020-21) from their India Operations	Audited balance sheets and certificate from CA to be submitted.

4	The IMSP should not have been blacklisted by any Government authority or Public sector Undertaking (PSU) or private organization as on date of submission of the tender, otherwise the bid will not be considered.	An undertaking (on their letter head) in this regard should be enclosed by the IMSP by authorized signatory.
5	The ISMP should have implemented SIEM and EDR solutions in at least 2 Enterprises.	A PO copy along with a self-declaration on the letter head of the organization submitting the reference jointly signed by the authorized signatory.
6	The IMSP should have a minimum of 50 individuals with minimum 4 years of experience in implementation and management of Security Operations Centre. All resources must be on the payroll of the IMSP.	Self-declaration to this effect on company's letterhead signed by authorized signatory of the IMSP.
7	The IMSP should be ISO 27001Certified	Certification copy required

The Financial bids of only such IMSPs shall be opened who are successful in technical bid evaluation

	2.3 GENERAL COMMERCIAL CONDITIONS
i.	The detailed BoM of Multi-Service Platform servicesis based on industry practice and is available as Schedule of Requirements (SOR) as per the Annexure-**VI and Section 6 –Detailed Scope of Work.**
ii.	The IMSP should complete the project within 24 weeks from the date of signing the Agreement and the detailed Timelines shall be as per Annexure-X
iii.	The IMSP shall Design, Plan, Engineer bytaking into consideration the existing IT infrastructure of the ITI Data Centre. Resources of ITI being used should be clearly specified in the bid. Also, bidder should certify that no supply of similar hardware that is available for use at ITI data centre, is being additionally supplied by bidder. Maintenance of such hardware shall also be the responsibility of Bidder.
iv.	To understand the existing infrastructure of ITI Data Centre, IMSP can visit Data Centre with prior appointment before preparing the final quote.
v.	The end-to-end integration of all devices /elements /applications etc., acceptance testing and commissioning of the project will be the sole responsibility of the selected IMSPs. In case of any unresolved conflict and technical overlap, the IMSP shall have overall responsibility to resolve the issues.
vi.	The ISMPs shall impart necessary training to ITI Engineers for undertaking installation, integration and acceptance testing for successful roll out of the Multi-Service Platform services.
vii.	IMSPs will be responsible for any shortfall in the BoM/BoQ/SOR as needed to fulfil the service requirements of customer.

	2.4 BID SECURITY DECLARATION AND PERFORMANCE BANK GUARANTEE (PBG)
i.	IMSPs are required to submit bid security declaration as per Annexure XI and XII
ii.	Performance Bank Guarantee (PBG) of 1.5% of the total bid value would be required to be submitted for the entire period of the project execution. This PBG amount would be released to the Multi-Service Provider after completion of the project. A separate PBG of the value 1.5% of the total bid value would be required to be submitted for the entire period of Warranty, Operation and Maintenance of the Multi-Service Platform project. This PBG would be released after completion of entire period.

2.5 TECHNICAL BID EVALUATION

S.No	Brief Description	Remarks by IMSP (Yes/No)
1	Presentation on complete solution proposed (with design documents and technical details)*	
2	Whether IMSP have implemented SIEM and EDR solutions at leastin 2 Enterprises.	
3	Nos of years of experience in Multi-Service Platform setup (> 3 Years)	
4	No. of successful Multi-Service Platform setups (= > 3 setups)	
5	Number of CISA, CISM, CISSP certified holders on the company roll and number of certified holder allotting to this project (>10 Members)	
6	Company average turnover of last three years 2017-18, 2018-19, 2019-20 (>20 Cr)	

***IMSPs shall arrange presentation on Solution Design and strength on following points:**

i) Detailed approach & methodology on Multi-Service Platformarchitecture and implementation plan.

ii) Detailed approach & methodology onMulti-Service Platformequipment power and cooling requirement details.

iii) Detailed approach & methodology on delivery management approach as Multi-Service Platformarrangements.

iv) Details of ISO Certification.

v) Details on strength of solution proposed Computing such as server, operating system and virtualization, Multi-Service Platformservices components IAM, NG FW, VAPT & APPSCAN, UEBA, NAC, SIEM, DLP, EDR, Email security (Please elaborate on sizing of solution in detail both for overall solution and at granular level of each application).

vi) The IMSP should give detailed sales plan for selling SOC as a Service to potential ITI customers to substantiate your revenue share in the financial bid.

vii) Costing of each of the services as per the market rate should be mentioned in the technical bid.

viii) Scope and Detailed Plan for support for Cert-in Empanelment.

ix) Detailed presentation on SoC Architecture- People- Process- Technology/Tools during technical evaluation.

2.6 FINANCIAL CONDITIONS

(1).	The technically qualified IMSP, whose overall quote is lowest, would be the selected choice.
(2).	The SOC service proposed to be launched through this project is a new effort and likely to build and add users progressively. Therefore, a progressive approach of building the capacity is being adopted and the IMSPs are requested to quote the prices of Add-Ons accordingly. In order to assess the best overall IMSP, a weightage quotient has been provided with each Add-On service as per the table given below and same shall be applied to the quoted price to evaluate the overall best IMSP. Whereas, the Lowest overall quote would help in evaluating the best-chosen bidder, the payment shall be made on the agreed/quoted price of the selected MSP for each item as needed.
(3).	ITI reserves the right to negotiate the quoted price for one and all items before acceptance.
(4).	Apart from seeking Technical and analytical expertise of MSP, its skills of presenting the SoC/Data services and On-Board of new customers shall be one of the major forte and it would be suitablyremunerated as per the quoted and agreed rate percentage.

(5).	**All comprehensive Services including Software/Firmware/Licences/Upgrades/Updates and Hardware if (any) at the SoC or at End Point(s), including but not limiting to following in order to launch the bouquet of services as per the SoW.**	**Weightage (Multiplying Quotient) as per the progressive Quantum of the User Base (End Points-EPs)**			
		Up to **500** End Points	**>500<1000** End Points	**>1,000<3,000** End Points	**>3,000** End Points
A.	**Variable as per the Quantum of EPs**	Multiplying Factor			
(i)	Identity & Access Management as a Service.	0.5	0.3	0.12	0.08
(ii)	Network Access Control as a Service.				
(iii)	E-mail Security as a Service.				
(iv)	End Point Detection as a Service (EDR).				
(v)	Data loss prevention (DLP) as a Service.				
B.	**One time for the Ultimate Quantum of EPs**	Multiplying Factor			
(i)	Firewall with DDoS as a Service.	1.0			
(ii)	Security Information and Event Management (SIEM) as a Service.				
(iii)	Vulnerability and Penetration Testing (VAPT) as a Service includes Appscan.				
(iv)	Analytics as a service includes UEBA.				
C.	**Variable as per the Quantum of EPs**	Multiplying Factor			
(i)	%age Revenue Share to the MSP from the ITI's billed revenue to the customers.	1.0			
D	**Variable as per the Quantum of EPs**	Multiplying Factor			
(i).	Operation and Maintenance services per Annum.	0.5	0.3	0.12	0.08

2.7 FINANCIAL BID

All comprehensive Services including Software/Firmware/Licences/Upgrades/Updates and Hardware if (any) at the SoC or at End Point(s), including but not limiting to following in order to launch the bouquet of services as per the SoW.		**Financial Quotes for the SoC Service, per End Point**			
		Up to**500** End Points	**>500<1000** End Points	**>1,000<3,000** End Points	**>3,000** End Points
A.	**Variable as per the Quantum of EPs**	**Rupees (In Words and Figures)**			
(i)	Identity & Access Management as a Service.	a1	a2	a3	a4
(ii)	Network Access Control as a Service.				
(iii)	E-mail Security as a Service.				
(iv)	End Point Detection as a Service (EDR).				
(v)	Data loss prevention (DLP) as a Service.				
B.	**One time for the Ultimate Quantum of EPs**	**Rupees (In Words and Figures)**			
(i)	Firewall with DDoS as a Service.	b			
(ii)	Security Information and Event Management (SIEM) as a Service.				
(iii)	Vulnerability and Penetration Testing (VAPT) as a Service includes Appscan.				
(iv)	Analytics as a service includes UEBA.				
C.	**Variable based on Number of EPs & Customers**	**Percentage (In word & Figures)**			
(i).	%age Revenue Share from the billed revenue to the customers.	c			
D.	**Variable as per the Quantum of EPs**	**Rupees (In Words and Figures)**			
(i).	Operation and Maintenance services per Annum.	d1	d2	d3	d4

Quotes, after applying Weightage Multipliers:

A= [a1*0.5+a2*0.3+a3*0.12+a4*0.08] **B= [b*1.0]** **C= [{(A+B) *0.04}] *[c/100].**

D= [d1*0.5+d2*0.3+d3*0.12+d4*0.08]

Overall, Assessed Quote for evaluating L1 Bidder: [A+B+C+D]

Notes:

(1) The weightage formulae are just for the assessment of L1 Bid and may have no relevance with the actual payouts and would not be challenged by any bidder on whatever ground.

(2) The multiplying factors are only for adjudging the L1 bid and the actual payments shall accrue based on the quoted/agreed prices.

(3) At the beginning, only the agreed prices for the 500 End Points shall be payable for the items linked with quantum. For the higher slabs, the payment shall be built up on the lower slabs i.e. after adding the previous slab's payout.

(4)The quoted and agreed percentage share of billed revenue for launching and maintain SoC services to the end customers shall be payable on actualisation from the customer.

(5) In cases of onboarding of the new customer(s), the percentage of revenue to be shared with MSP shall be on escalated rate of 2 times in a year.

(6) The annual O&M Charges shall be fixed for a period of initial three years, which shall stand escalated @10% per annum, thereafter.

(7) The Intended MSP shall quote each & every item in the financial bid and all fields are compulsory.

(8) The prices for each of the services should be quoted individually.

Any of the cells (a1 to a4, b, c, d1 to d4) if left blank, the financial bid would liable for rejection.

2.8 PAYMENT TERMS

S.No	Activity /Milestones /deliverables	Payment to be released	Document to be submitted by the successful IMSP
1	Set up readiness, submission of design /engineering documents and Material delivery (Hardware /appliances /software/Licenses /Tools)	30% of total project cost	Original challan/ Invoice delivery proof duly signed by ITI Ltd official
2	Successful implementation, integration, training and knowledge transfer	25% of total project cost	After Documents submission, acceptance by ITI official
3	UAT, commission ,Project documentation submission including training materials and Sign-off	35% of total project cost	Sign off letter issued by ITI official
4	After 1 Year of UAT Completion	10% of total project cost	Sign off letter issued by ITI official

3 INSTRUCTIONS FOR SUBMITTING PROPOSAL TOWARDS TENDER

The Technical Bid and financial bid shall be uploaded on TenderWizard only on or before **20-05-2021**:

https://www.tenderwizard.com/ITILIMITED

The offerwill be rejected, if the financial quote is not offered.

1. Schedule of Bidding:
    a. Last date of seeking clarifications: 10th May2021
    b. Pre-bid session with IMSPs : 07th May 2021
    c. Bid Submission: 20th May2021 by 11:30 Hrs
    d. Bid opening: : 20th May2021 at 16:00 Hrs
2. Financial Bid opening will be done after the evaluation of Technical bid (Only for technically qualified IMSPs).
3. Bid should be valid for a period of 150 days from the date of opening of tender response.
4. Conditional offers and multiple offers are liable for rejection.
5. The IMSPs should give Clause by clause compliance (as per Annexure-I of tender) with reference to supporting documents;otherwise, the offers are liable for rejection.
6. All the pages of the technical offer and the price bid shall be signed by an authorized person of the IMSP.
7. The IMSPto indemnify ITI from any claims/penalties/statuary charges, penalties with legal expenses etc.
8. Late offer: Any offer received after the prescribed timeline shall be rejected.
9. Language of offers: The offers prepared by the IMSPsand all the correspondences and documents relating to the offers exchanged by the companies shall be written in English language.
10. Financial quote shall be firm throughout the contract irrespective of reason, what so ever, including the exchange rate fluctuation.
11. IMSPs may like to discuss tender bidding conditions, bidding process & clarifications, if any may do so with GM-PP and obtain the required information/clarification by due date.
12. **Cost of tender:** The IMSP shall bear all costs associated with the preparation and submission of his offer against this tender, including cost of presentation for the purposes of clarification of the offer. ITI will, in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tender process.
13. **Amendment of tender:** At any time prior, to the last date for receipt of offers, ITI, may, for any reason, whether at its own initiative or in response to a clarification requested by prospective IMSPs, modify the tender document by an amendment. ITI may, at their discretion, extend the last date for the receipt of offers and/or make other changes in the requirements set out in the Invitation for tender.
14. **Disclaimer:** ITI and/or its officers, employees disclaim all liability from any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of ITI and/or any of its officers, employees.
15. On the Bid-opening day, only technical bids will be opened. The IMSPs who are desirous of attending bid opening shall inform ITI in writing and a maximum of two persons from an IMSP are allowed to attend the Bid opening.

    Venue of bid opening:

    First Floor Conference Room
    ITI Corporate Office, ITI Bhawan
    Dooravaninagar P.O.,
    Bengaluru – 560 016.

16. Letter of authority from the IMSP authorizing the persons to attend the Bid opening shall be submitted by such person(s).
17. ITI reserves the right to suspend or cancel the tender process at any stage, or to accept, or reject any, or all offers at any stage of the process and / or to modify the process, or any part thereof, at any time without assigning any reason, without any obligation or liability whatsoever and the same shall be published in the ITI website or intimated through email.
18. The IMSP shall bear all costs associated with the preparation and submission of its tender, including cost of presentation for the purpose of clarification of the offer, if so desired by ITI.
19. If the last day for bid submission/openingis declared as a holiday, the bid submission and opening will be at the same time and venue on the next working day.
20. **Accessibility of** Tender: Complete tender with terms and conditions and amendments/clarifications if any shall be provided at the following websites:
    a. **https://www.tenderwizard.com/ITILIMITED**
    b. **https://www.itiltd.in**
    c. **https://www.eprocure.gov.in**

21. All Enquiries and Clarification with regards to thisTENDER shall be addressed to:

The General Manager (PP)
ITI Corporate Office
Dooravaninagar P.O.,
Bengaluru – 560 016.
Mob: +91 080-25617490 /7987198519/ 7978712658
Mail:brahmap_crp@itiltd.co.in/ sbaskey_crp@itiltd.co.in /mayur_bgp@itiltd.co.in

	4 CHECK LIST OF DOCUMENTS/INFORMATION TO BE SUBMITTED	
	a.	IMSP Profile as per Annexure-II
	b.	Technical literature/Brochures of the offered Solution/equipment. Documents on Multi-Service Platform services
	c.	A declaration, that the technology offered shall be upgradable to new requirement
	d.	Valid Power of Attorney along with resolution of Board for authorizing the person signing the bid for this tender.
	e.	Undertaking of NDA & PBGby IMSPs shall be submitted as per Annexure-III.
	f.	Performance Bank guarantee as per Annexure-IX
	g.	Undertaking of Authenticity as per Annexure-IV
	h.	Non-Disclosure Agreement as per Annexure-V
	i.	Non Blacklisting declaration as per Annexure-VII
	j.	Pre contract integrity Pact as per Annexure-VIII
	k.	Details of possession of Quality certification – ISO 27001 and any other certifications inCyber Security area.
	l.	Bid Security Declaration as per Annexure- XI and XII
	o.	Compliance certificate as per Annexure-I.

5 ANNEXURES

5.1 ANNEXURE-I

Compliance Statement

Section Details	Clause Numbers	Compliance (YES/NO)	Documentary Reference, If any
Technical Bid	2.5		
Scope of Work	2.1 , Section 6 and Annexure VII		
Essential Eligibility Criteria for the Applicants	2.2		
General Commercial Conditions	2.3		
BSD& PBG	2.4 and Annexure – X,XI,XII		
Financial Conditions	2.5		
Financial Bid	2.7		
Instructions for submitting Proposal towards tender	3		

5.2 ANNEXURE-II

IMSP's Profile				
S.No	**Description**	**IMSP Response**		
1	Name and address of the company			
2	ITI Tender Reference			
3	Company Directors Profile			
4	Contact Details of the IMSP (Contact person name with designation, Telephone Number, FAX, E- mail and Web site)			
5	Area of business			
6	Annual Turnover for 3 financial years (Rs in Cr)	2017-18	2018-19	2019-20
7	Date of Incorporation			
8	GST Registration number			
9	PAN Number			
10	CIN Number, if applicable			
11	Number of technical manpower in company's rolls			
12	Number of qualified developers			
13	Valid Power of Attorney along with resolution of Board for authorizing the person signing the bid for this tender to be submitted.			

5.3 ANNEXURE-III

UNDERTAKING of NDA & PBG

(To be submitted onIMSP's Letter Head)

M/s…… do here by undertake and declare that:

1. The Non-Disclosure Agreement (NDA) signed shall also be applicable and abided by us unequivocally.
2. That we are not under any blacklist by Central Govt. /any State or UT Govt. / PSU/ organized sector in India or by GST authorities and fully comply the Terms and conditions of Tender by ITI Ltd.
3. We agree to submit PBG for an appropriate amount as per the quantum of work assigned under in the standard PBG format as required by ITI.
4. That we undertake to indemnify ITI from any claims / penalties / statuary charges, liquidated damages, with legal expenses etc., as charged by the customer.
5. That all the hardware/ software supplied under the contract arrangement shall not contain any embedded malicious codes that could inhibit the desired functions of the equipment or cause the network to malfunction in any manner.

Duly authorized to sign the bid for and on behalf of:

[Insert complete name of IMSP]

Datedon_____day of_____[insert date of signing]

Corporate Seal (whereappropriate)

5.4 ANNEXURE- IV

Undertaking of Authenticity

(To be signed by authorized signatory of the IMSP)

Ref: _____ Date: _____

To

General Manager [PP]
ITI Ltd, Doorvani Nagar,
Bengaluru,
Karnataka- 560016

Undertaking of Authenticity

With reference to the hardware items (as mentioned in the Commercial Bid) quoted to you vide our quotation No.:_____ dated _____ in response to your tender no. _____, we hereby undertake that all the components / parts / assembly / software used in the hardware items shall be original / new from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly / software are being used or shall be used.

We also undertake that in respect of licensed operating system if asked for by you in the purchase order, the same shall be supplied along with the authorised license certificate and also that it shall be sourced from the authorised source.

Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation for the IT hardware / software already billed, we agree to take back the same, if already supplied and return the money if any paid to us by you in this regard.

We (IMSP name) also take full responsibility of both parts & service SLA as per the content even if there is any defect by our authorised service centre / reseller / IMSP etc.

Signature of Authorised Signatory

Name: _____

Designation: _____

Date: _____

Place: _____

Phone & E-mail: _____

Name of the Organisation: _____

5.5 ANNEXURE- V

Non-Disclosure Agreement

(TO BE EXECUTED ON A NON-JUDICIAL STAMPED PAPER of requisite value based on place of execution)

WHEREAS, we, _____, having Registered Office at _____, hereinafter referred to as the COMPANY, are agreeable to execute "Implementation and Management of Multi-Service Platform" as per the scope defined in the Tender No. _____ for ITI, having its Head office at DoorvaniNagar, Bengaluru (hereinafter referred to as the ITI Ltd) and WHEREAS, the COMPANY/LLP/Partnership understands that the information regarding the ITI's /ITI's customers Infrastructure shared by the ITI ltd in their tender is confidential and/or proprietary to the ITI Ltd, and

WHEREAS, the COMPANY/LLP/Partnership understands that in the course of submission of the offer for the said tender and/or in the aftermath thereof, it may be necessary that the COMPANY/LLP/Partnership may perform certain jobs/duties on the ITI's /it is customers properties and/or have access to certain plans, documents, approvals, data or information of the ITI Ltd;

NOW THEREFORE, in consideration of the foregoing, the COMPANY/LLP/Partnership agrees to all of the following conditions, in order to induce the ITI Ltd to grant the COMPANY/LLP/Partnership specific access to the ITI's customers property/information:

The COMPANY/LLP/Partnership will not publish or disclose to others, nor, use in any services that the COMPANY/LLP/Partnership performs for others, any confidential or proprietary information belonging to the ITI Ltd / ITI customers unless the COMPANY/LLP/Partnership has first obtained the ITI's written authorisation to do so;

The COMPANY/LLP/Partnership agrees that information and other data shared by the ITI Ltd or, prepared or produced by the COMPANY/LLP/Partnership for the purpose of submitting the offer to the ITI Ltd in response to the said tender, will not be disclosed to during or subsequent to submission of the offer to the ITI Ltd, to anyone outside the company

The COMPANY/LLP/Partnership shall not, without the ITI Ltd's written consent, disclose the contents of this tender or any provision thereof, or any specification, plan, pattern, sample or information (to be) furnished by or on behalf of the ITI Ltd in connection therewith, to any person(s) other than those employed/engaged by the COMPANY/LLP/Partnership for the purpose of submitting the offer to the ITI Ltd and/or for the

performance of the Contract in the aftermath. Disclosure to any employed/engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Yours Sincerely,

Signature of Authorised Signatory

Name of Authorized Signatory:

Designation:

Office Seal:

Date

Place

5.6 ANNEXURE-VI

Service Description (SOR)

S.No	**Description**		**Qty**
1	Identity & Access Management	Initially for 500 users scalable up to 5000 users as per ITI's customer requirement	1
2	Data Loss Prevention (DLP)	Initially for 500 users scalable up to 5000 users as per ITI's customer requirement	1
3	E Mail security appliance	Initially for 500 licenses and can be scalable up to 5000 as per the ITI's customers requirement. Concurrent user handling capability of atleast 2000.	1
4	Network access control appliance	Initially for 500 licenses and can be scaled up for 5000 as per the ITI's customers requirement.	1
5	Operating system	Unix /Linux /windows where ever the suitable flavour applicable shall be installed, Licenses are perpetual, should be on the name of ITI Ltd or ITI Ltd customers name	As Per requirement
6	Databases	The actual database requirement will be as per the IMSPs proposed solution	As Per requirement
7	Antivirus	All the servers / appliances must be installed and protected by Antivirus.	As Per requirement
8	Licenses	All the software supplied to ITI ltd or its customers shall be fully licensed and ownership to be transferred to ITI Ltd or Its customers as per actual requirement of the business. All the licenses should be unlimited and are perpetual.	As Per requirement
9	SIEM Licenses	This should be industry prominent and shall meet all the needs of ITI Ltd or Its customers' requirements with unlimited licenses.	1
10	VAPT and Applications Scan	This should be industry prominent and shall meet all the needs of ITI Ltd or Its customers' requirements with unlimitedand perpetual licenses.	1
11	Firewall	1,00,000 concurrent sessions, and 10,000 sessions per second, memory of atleast minimum 16 Gb, Minimum IPS throughput of 1Gbps, should have at least minimum appliance 240 GB SSD of on-board storage.	2

12	End point detection appliance license	Initially for 500 licenses as base and can be scaled up to 5000 as per the ITI's customers requirement.	1
13	Threat hunting and Intelligence	As per ITI Ltd or Its customer requirement and customization need to be done by the IMSP. Licenses are unlimited and perpetual.	1
14	Reporting & dashboards development	As per ITI Ltd or Its customer requirement and customization need to be done by the IMSP. The licenses are unlimited and perpetual.	1
15	UEBA (Analytics)	IMSP shall customized their solution as per ITI's requirement. Unlimited license and perpetual	1
16	Hardware	Supply of hardware like server infrastructure, Network infrastructure, Backup appliance, Storage infrastructure and any other infrastructure, software, tools and appliances are in the scope of IMSP only. The servers and applications are in cluster mode, high available, automatic switchover if any failovers and single point of failover should be avoided.	
The IMSP shall design, engineer, size, install and configure hardware and services to meet the above bare minimum requirement keeping in mind that all hardware configuration would be scalable and capable of catering to thefuture requirements.			

5.7 ANNEXURE-VII

UNDERTAKING FOR NOT BLACKLISTING

(Non-Blacklisting declaration)

To:

General Manager (PP)

ITI Ltd, Registered & Corporate Office

ITI Bhavan, Dooravaninagar,

Bengaluru-560016 (Karnataka, India)

Subject: Non-Blacklisting declaration in connection with participation in tender No: ……..for …….

Dear Sir,

This is to notify you that our Firm/Company/Organization/LLP intends to submit a proposal in response to invitation for tender No: …….. for providing ……. In accordance with the above we declare that:

a. We are not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this assignment.

b. We are not blacklisted by any Central/ State Government/ agency of Central/ State Government of India or any other country in the world/ Public Sector Undertaking/ any Regulatory Authorities in India or any other country in the world for any kind of fraudulent activities.

Sincerely,

[IMSP's NAME]

Name

Title

Signature

5.8 ANNEXURE-VIII

PRE-CONTRACT INTEGRITY PACT

(To be executed on plain paper and submitted along with Technical Bid/ TENDER. To be signed by the IMSP and same signatory Competent/ Authorized to sign the relevant contract on behalf of the ITI Ltd).

TENDER No.....

This Integrity Pact is made on .....day of 2021

BETWEEN:

ITI Limited, ……..having its Registered & corporate office at ITI Bhavan, Dooravaninagar, Bangalore – 560016 India, and established under the Ministry of Communications & IT, Government of India (hereinafter called the Principal), which term shall unless excluded by or is repugnant to the context, be deemed to include its Chairman & Managing Director, Directors, Officers or any of them specified by the Chairman & Managing Director in this behalf and shall include its successors and assigns) ON THE ONE PART

AND:

M/s ….…… represented by .....Chief Executive Officer (hereinafter called the IMSP(s)), which term shall unless excluded by or is repugnant to the context be deemed to include its heirs, representatives, successors and assigns of the IMSP/contract ON THE SECOND PART.

Preamble

WHEREAS the Principal intends to award, under laid down organizational procedures, TENDER/contract for..... (name of the Stores / equipment's / items). The Principal, values full compliance with all relevant laws of the land, regulations, economic use of resources and of fairness/ transparency in its relations with its IMSP(s).

In order to achieve these goals, the Principal has appointed an Independent External Monitor (IEM), who will monitor the TENDER process and the execution of the contract for compliance with the principles as mentioned herein this agreement.

WHEREAS, to meet the purpose aforesaid, both the parties have agreed to enter into this Integrity Pact the terms and conditions of which shall also be read as integral part and parcel of the TENDER and contract between the parties.

NOW THEREFORE, IN CONSIDERATION OF MUTUAL COVENANTS STIPULATED IN THIS PACT THE PARTIES HEREBY AGREE AS FOLLOWS AND THIS PACT WITHNESSETH AS UNDER:

SECTION 1 – COMMITMENTS OF THE PRINCIPAL

The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:

a. No employee of the Principal, personally or through family members, will in connection with the TENDER for or the execution of the contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the personal is not legally entitled to.

b. The Principal will, during the TENDER process treat all IMSP(s) with equity and reason. The Principal will in particular, before and during the TENDER process, provide to all IMSP(s) the same information and will not provide to any IMSP(s) confidential/ additional information through which the IMSP(s) could obtain an advantage in relation to the TENDER process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons. If the principal obtains information on the conduct of any of its employee, which is a criminal offence under IPC/PC Actor if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary action as per its internal laid down Rules/ Regulations.

SECTION 2 – COMMITMENTS OF THE IMSP / CONTRACTOR

2.1 The IMSP(s)/Contractor(s) commits himself to take all measures necessary to prevent corruption. He commits himself observe the following principles during the participation in the TENDER process and during the execution of the contract.

a. The IMSP(s)/contractor(s) will not, directly or through any other person or firm offer, promise or give to any of the Principal's employees involved in the TENDER process or the execution of the contract or to any third person any material or other benefit which he/ she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever (during the TENDER process or during the execution of the contract.

b. The IMSP(s)/contractor(s) will not commit any offence under IPC/PC Act, further the IMSP(s)/contractor(s) will not use improperly, for purposes of competition of personal gain, or pass onto others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

c. The IMSP(s)/Contractor(s) of foreign original shall disclose the name and address of the agents /representatives in India, if any. Similarly, the IMSP(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

d. The IMSP(s) f Contractor(s) will, when presenting the bid, disclose any and all payments made, are committed to or intend to make to agents, brokers or any other intermediaries in connection with the award of the contract.

e. The IMSP(s)/Contractor(s) will not bring any outside influence and Govt. bodies directly or indirectly on the bidding process in furtherance to his bid.

f. The IMSP(s)/Contractor(s) will not instigate third persons to commit offences outlined above or to be an accessory to such offences.

SECTION 3 – DISQUALIFICATION FROM TENDER PROCESS & EXCLUSION FROM FUTURE CONTRACTS

If the IMSP(s)/Contractor(s), during TENDER process or before the award of the contract or during execution has committed a transgression in violation of Section 2, above or in any other form such as to put his reliability or credibility in question the Principal is entitled to disqualify IMSP(s)/Contractor(s) from the TENDER process.

If the IMSP(s)/Contractor(s), has committed a transgression through a violation of Section 2 of the above, such as to put his reliability or credibility into question, the Principal shall be entitled exclude including blacklisting for future TENDER/contract award process. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the Principal taking into consideration the full facts and circumstances of each case, particularly taking into account the number of transgression, the position of the transgressor within the company hierarchy of the IMSP(s)/Contractor(s) and the amount of the damage. The exclusion will be imposed for a period of minimum one year.

The IMSP(s)/Contractor(s) with its free consent and without any influence agrees and undertakes to respect and uphold the Principal's absolute right to resort to and impose such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground including the lack of any hearing before

the decision to resort to such exclusion is taken. The undertaking is given freely and after obtaining independent legal advice.

A transgression is considered to have occurred if the Principal after due consideration of the available evidence concludes that on the basis of facts available there are no material doubts.

The decision of the Principal to the effect that breach of the provisions of this Integrity Pact has been committed by the IMSP(s)/ Contractor(s) shall be final and binding on the IMSP(s)/Contractor(s), however the IMSP(s)/Contractor(s) can approach IEM(s) appointed for the purpose of this Pact.

On occurrence of any sanctions/ disqualifications etc. arising out from violation of integrity pact IMSP(s)/ Contractor(s) shall not entitled for any compensation on this account.

Subject to full satisfaction of the Principal, the exclusion of the IMSP(s)/Contractor(s) could be revoked by the Principal if the IMSP (s)/ Contractor(s) can prove that he has restored/ recouped the damage caused by him and has installed a suitable corruption preventative system in his organization.

SECTION 4 – PREVIOUS TRANSGRESSION

4.1 The IMSP(s)/Contractor(s) declares that no previous transgression occurred in the last 3 years immediately before signing of this Integrity Pact with any other company in any country conforming to the anti-corruption/transparency International (TI) approach or with any other Public Sector Enterprises/ Undertaking in India of any Government Department in India that could justify his exclusion from the TENDER process.

4.2 If the IMSP(s)/ Contractor(s) makes incorrect statement on this subject, he can be disqualified from the TENDER process or action for his exclusion can be taken as mentioned under Section-3 of the above for transgressions of Section-2 of the above and shall be liable for compensation for damages as per Section- 5 of this Pact.

SECTION 5 – COMPENSATION FOR DAMAGE

5.1 If the Principal has disqualified the IMSP(s)/Contractor(s) from the TENDER process prior to the award according to Section 3 the Principal is entitled to forfeit the Earnest Money Deposit/Bid Security/ or demand and recover the damages equitant to Earnest Money Deposit/Bid Security apart from any other legal that may have accrued to the Principal.

5.2 In addition to 5.1 above the Principal shall be entitled to take recourse to the relevant provision of the contract related to termination of Contract due to Contractor default. In such case, the Principal shall be entitled to forfeit the Performance Bank Guarantee of the Contractor or demand and recover liquidate and all damages as per the provisions of the contract agreement against termination.

SECTION 6 – EQUAL TREATEMENT OF ALL IMSPS/CONTRACTORS

6.1 The Principal will enter into Integrity Pact on all identical terms with all IMSPs and contractors for identical cases.

6.2 The IMSP(s)/Contractor(s) undertakes to get this Pact signed by its subcontractor(s)/sub- vendor(s)/ associate(s), if spy, and to submit the same to the Principal along with the TENDER document/contract before signing the contract. The IMSP(s)/Contractor(s) shall be responsible for any violation(s) of the provisions laid down in the Integrity Pact Agreement by any of its subcontractors/ sub-vendors / associates.

6.3 The Principal will disqualify from the TENDER process all IMSPs who do not sign this Integrity Pact or violate its provisions.

SECTION 7 – CRIMINAL CHARGES AGAINST VIOLATIG IMSP(S)/CONTRACTORS

7.1 If the Principal receives any information of conduct of an IMSP(s)/Contractor(s) or sub-contractor/ sub-vendor/associates of the IMSP(s)/Contractor(s) which constitutes corruption or if the principal has substantive

suspicion in this regard, the principal will inform the same to the Chief Vigilance Officer of the Principal for appropriate action.

SECTION 8 – INDEPENDENT EXTERNAL MONITOR(S)

8.1 The Principal appoints competent and credible Independent External Monitor(s) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extend the parties comply with the obligations under this pact.

8.2 The Monitor is not subject to any instructions by the representatives of the parties and performs his functions neutrally and independently. He will report to the Chairman and Managing Director of the Principal.

8.3 The IMSP(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all product documentation of the Principal including that provided by the IMSP(s)/Contractor(s). The IMSP(s)/Contractor(s) will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The Monitor is under contractual obligation to treat the information and documents IMSP(s)/Contractor(s) with confidentiality.

8.4 The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meeting could have an impact on the contractual relations between the Principal and the IMSP(s)/Contractor(s). As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in specific manner, refrain from action or tolerate action.

8.5 The Monitor will submit a written report to the Chairman & Managing Director of the Principal within …….. to …….. weeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.

8.6 If the Monitor has reported to the Chairman & Managing Director of the Principal a substantiated suspicion of an offence under relevant IPC/PC Act, and the Chairman & Managing Director of the principal has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

8.7 The word 'Monitor' would include both singular and plural.

8.8 Details of the Independent External Monitor appointed by Principal at present is furnished below:

Shri Javeed Ahmad, IPS(Retd.)
M-1101, Shalimar Gallant Apartment,
Vigyanpuri ,Mahanagar,Lucknow-226006

SECTION 9 - FACILITATION OF INVESTIGATION

9.1 In case of any allegation of violation of any provisions of this Pact or payment of commission, the Principal or its agencies shall be entitled to examine all the documents including the Books of Accounts of the IMSP(s)/Contractor(s) and the IMSP(s)/Contractor(s) shall provide necessary information and documents in English and shall extend all help to the Principal for the purpose of verification of the documents.

SECTION 10 - LAW AND JURISDICTION

10.1 The Pact is subject to the Law as applicable in Indian Territory. The place of performance and jurisdiction shall the seat of the Principal.

10.2 The actions stipulated in this Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extent law in force relating to any civil or criminal proceedings.

SECTION 11 – PACT DURATION

This Pact begins when both the parties have legally signed it. It expires after 12 months on completion of the warranty/ guarantee period of the project /work awarded, to the fullest satisfaction of the Principal.

If the IMSP(s)/Contractor(s) is unsuccessful, the Pact will automatically become invalid after three months on evidence of failure on the part of the IMSP(s)/Contractor(s).

If any claim is lodged/made during the validity of the Pact, the same shall be binding and continue to be valid despite the lapse of the Pact unless it is discharged/determined by the Chairman and Managing Director of the Principal.

SECTION 12 - OTHER PROVISIONS

12.1 This pact is subject to Indian Law, place of performance and jurisdiction is the Registered & Corporate office of the Principal at Bengaluru.

12.2 Changes and supplements as well as termination notices need to be made in writing by both the parties. Side agreements have not been made.

12.3 If the IMSP(s)/Contractor(s) or a partnership, the pact must be signed by all consortium members and partners.

12.4 Should one or several provisions of this pact turn out to be invalid, the remainder of this pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

12.5 Any disputes/ difference arising between the parties with regard to term of this Pact, any action taken by the Principal in accordance with interpretation thereof shall not be subject to any Arbitration.

12. 6 The action stipulates in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

In witness whereof the parties have signed and executed this Pact at the place date first done mentioned in the presence of the witnesses:

For PRINCIPAL	ForIMSP(S)/CONTRACTOR(S)
……	……
Name Designation.	Name Designation.
Witness:	
1. ……..	1. ……
2. ……..	2. …….

5.9 ANNEXURE-IX

PERFORMANCE BANK GUARANTEE PROFORMA

1. As agreed under the relevant terms and conditions of Letter of Intent / Purchase Order Ref ……Dated …..… between M/s ITI Ltd., (with address) (hereinafter called the Purchaser) and M/s……(hereinafter called the Supplier) for supply of ……..(herein after called the said Purchase Order), the supplier hereby agrees to furnish a Security Deposit against supply performances by way of an irrevocable Bank Guarantee for Rs…….(Rupees…….only). We……..[Indicate the name of Bank] (Herein after referred to as` THE BANK') at the request of the supplier do hereby undertake to pay to the purchaser, an amount not exceeding Rs……..(Rupees……only) against any loss or damage caused to or suffered or would be caused to or suffered by the Purchaser, by reasons of breach by the said Supplier of any of the terms or conditions contained in the said Letter of Intent.

2. We. ……[Indicate the name of the Bank] do hereby undertake to pay the amount due and payable under this Guarantee without any demur, merely on a demand from the purchaser stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by the purchaser, by reason of breach by the said Supplier of any of the terms or conditions contained in the said Letter of Intent or by reason of the Supplier's failure to perform the said Letter of Intent. Any such demand made on the bank shall be conclusive as regards the amount due and payable by the Bank under this Guarantee shall be restricted to an amount not exceeding Rs…….(Rupees ……only).

3. The Bank further agrees that the Purchaser shall be the sole judge as to whether the said supplier has committed any breach or breaches of any of the terms and conditions of the contract and the extent of loss, damage, costs, charges and expenses caused to or suffered by or that may be caused to or suffered by the Purchaser on account thereof, and the decision of the Purchaser that the said Supplier has committed such breach or breaches and as to the amount or amounts of loss, damage costs, charges and expenses caused to or suffered by or that may be caused to or suffered by the Purchaser from time to time shall be conclusive, final and binding on the Bank.

4. We undertake to pay to the Purchaser, any money so demanded notwithstanding any dispute or disputes raised by the Supplier in any suit or proceedings pending before any Court or Tribunal relating thereto our liability under this present being absolute and unequivocal.

5. It shall not be necessary for the Purchaser to proceed against the Supplier before proceeding against the Bank and the Guarantee herein contained shall be enforceable against the Bank not withstanding any security, which the Purchaser may have obtained or obtains from the Supplier.

6. We…….[Indicate the name of Bank] further agree with the Purchaser, that the Purchaser shall have the fullest liberty without our consent and without effecting in any manner our obligation hereunder to vary any of the terms and conditions of the said Letter of Intent or to extend time of performance by the said Supplier from time to time or to postpone for any time of from to time any of the powers exercisable by the Purchaser against the said Supplier and to forbear or enforce any of the terms and conditions relating to the said Letter of Intent and we shall not relieved from our liability by reasons of any such variation, or extension being granted to said Supplier or for any forbearance, act or omission on the part of the Purchaser or any indulgence by the Purchaser, to the said Supplier or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

7. This Guarantee will not be discharged due to the change in the constitution of the Bank or the Supplier.

8. We ……..[Indicate the name of Bank] undertake not to revoke this Guarantee during its currency except with the previous written consent of the Purchaser, in writing.

9. Notwithstanding anything contained in the foregoing clauses, our liability under this guarantee is restricted to Rs. ……(Amount in words also) and our guarantee shall remain in force until …….(expiry of warranty period). Unless a demand is made against us to enforce a claim under this guarantee within three months from the date, all your rights under this guarantee shall be forfeited and we shall be relieved and discharged from all liability hereunder.

for……..[Indicate the name of Bank]

DATE:
PLACE:

5.10 ANNEXURE-X
Project Timelines:

S.No	Activity	Timeline
1	Agreement Signing	T0
2	Asset Discovery and Infra Reusability Plan	T1 = T0 + 2 weeks
3	Finalization & Approval of the submitted Plan	T2 = T1 + 2 weeks
4	Supply, Installation and Commissioning & Testing of all required software, hardware and tools/ IT equipment / appliances, training and knowledge transfer	T3 = T2 + 12 weeks
5	Validation & UAT	T4 = T3 + 4 weeks
6	Project Sign Off & Operationalization	T5 = T4 + 4 weeks
7	Warranty 1 Years	T5 + 1years

Penalties for Project delay

1. The project has to be completed within 24 weeks from the date of agreement, else penalties will be levied on delays beyond 24 weeks at the rate of Rs.5 Lakhs per week will be deducted.

5.11 ANNEXURE-XI

BID SECURITY FORM

Whereas _____

(hereinafter called the tenderer)

has submitted their offer dated _____

for the supply of _____

(hereinafter called the tender)

Against the Purchaser's Tender No._____

KNOW ALL MEN by these presents that WE_____ (Bank Name)

of_____ having our registered office at

_____are bound unto_____(hereinafter called the "Purchaser")

In the sum of _____

For which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this _____20_____.

THE CONDITIONS OF THIS OBLIGATION ARE:

(1)	If the tenderer withdraws or amends or modifies or impairs or derogates from the Tender in any respect within the period of validity of this tender.
(2)	If the tenderer having been notified of the acceptance of his tender by the Purchaser during the period of its validity
(a)	Fails to furnish the Performance Security for the due Performance of the contract.
(b)	Fails or refuses to accept/execute the contract.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 45 days after the period of tender validity and any demand in respect thereof should reach the Bank notlater than the above date.

_____

(Signature of the authorized officer of the Bank)

Name and designation of the officer

Seal, name & address of the Bank and address of the Branch

Note: Whenever the bidder chooses to submit the Bid Security in the form of Bank Guarantee, then he should advise the banker issuing the Bank Guarantee to immediately send by Registered Post (A.D.) an unstamped duplicate copy of the Guarantee directly to the Purchaser with a covering letter to compare with the original BG for the correctness, genuineness, etc.

5.12 ANNEXURE-XII

Bid Securing Declaration Form

Date:_____ Tender No._____

To(insertcompletenameandaddressofthepurchaser)

I/We. The undersigned, declarethat:

I/We understand that, according to your conditions, bids must be supported by a Bid Securing Declaration.

I/WeacceptthatI/Wemaybedisqualifiedfrombiddingforanycontractwithyouforaperiodofoneyearfrom thedateofnotificationifIam/Weareinabreachofanyobligationunderthebidconditions,becauseI/We

a) havewithdrawn/modified/amended,impairsorderogatesfromthetender,my/ourBidduringthe period of bid validity specified in the form of Bid;or

b) havingbeennotifiedoftheacceptanceofourBidbythepurchaserduringtheperiodofbidvalidity(i) fail or reuse to execute the contract, if required, or (ii) fail or refuse to furnish the Performance Security,inaccordancewiththeInstructionstoBidders.

I/WeunderstandthisBidSecuringDeclarationshallceasetobevalidifIam/wearenotthesuccessfulBidder, upon the earlier of (i) the receipt of your notification of the name of the successful Bidder; or (ii) thirty days aftertheexpirationofthevalidityofmy/ourBid.

Signed: (insertsignatureofpersonwhosenameandcapacityareshown)
in thecapacityof (insertlegalcapacityofpersonsigningtheBidSecuringDeclaration)

Name: (insertcompletenameofpersonsigningheBidSecuringDeclaration)

Dulyauthorizedtosignthebidforanonbehalfof(insertcompletenameofBidder)

Datedon_____dayof _____ (insert date ofsigning)

Corporate Seal (where appropriate)

(Note:IncaseofaJointVenture,theBidSecuringDeclarationmustbeinthenameofallpartnerstotheJoint Venture that submits thebid)

6 DETAILED SCOPE OF WORK MULTI-SERVICE PLATFORM :

The scope of this tender is to build the Enterprise grade Multi-Service Platform 1 year warranty and maintenance support for 1 year, can be extended, another four years on annual basis, based on performance. Once the Multi-Service Platform at ITI Data Centeris completed and fully functional, it is envisaged to provide the following capabilities to potential customers of ITI and other organizations in a services model deeming itself a Multi-Service Platform services provider.

As bundled services with a combination of all of the below or as well as standalone basis or two or more as per the ITI Ltd business requirement. TheIMSPshalldo Planning, Engineering, Supply, Installation, Integration, deployment, Testing, Commissioning, building of all the following services:

1. Identity & Access Management as a Service
2. Firewall with Anti-DDoSas a Service.
3. Network Access Control as a Service.
4. E-mail Security as a Service.
5. Security Information and Event Management (SIEM) as a Service.
6. End Point Detection as a Service(EDR).
7. Data loss prevention (DLP) as a Service.
8. Vulnerability and Penetration Testing (VAPT) as a Service includes Application scan.
9. Analytics as a service includes UEBA.

All the proposed solutions are multi-tenant, on premise / cloud or physical and MSSP based model.

As an IMSPProvider: Commission and run a Multi-Service Platform from ITI's DataCenter and delivery / offer services to potential customers as a bundled or on standalone basis.

The IMSP shall also develop a web self-care portal, android/iOS app,for the purpose of customer self- care portal and ITI admin portal, which can facilitate the following features:

1. Service subscription / Booking
2. Service provisioning and status updates
3. Complaint / fault booking and tracking
4. Billing and payments.
5. Dashboard and reports.

The designed web care portal shall have the facility to integrate with all the subsystems, legacy systems in IT landscape.

6.1 IDENTITY & ACCESS MANAGEMENT AS A SERVICE

The scope of work includes analysing customers IT Information access, gathering requirement of licenses, software and hardware, design and implementation of state of the art Identity and Access management(IAM) solution. The solution shall be capable of providing below features and functionality.

6.1.1. Password management and governance
6.1.2. Privilege Access management
6.1.3. Define roles and responsibility through Access management solution
6.1.4. Monitoring, identify and predict unwanted access
6.1.5. Create policies to control unwanted access
6.1.6. Isolate device from network with automated anomaly detection
6.1.7. User provisioning & de-provisioning
6.1.8. Compliance in user termination
6.1.9. Detection and prevention of insider cyber threat
6.1.10. Actionable threat intelligence
6.1.11. Multi tenanted Service deployment
6.1.12. Cloud native deployable
6.1.13. Single Sign-on
6.1.14. Multi-Factor Authentication
6.1.15. Analytics and Reporting.

The IMSP should be responsible to design, develop and execute the project.

6.2 NEXT GEN FIREWALL:

The scope of work includes, analysing the current infrastructure of the customer, scrutinizing the network elements in place and suggesting the deployment of high available firewalls for security improvements and network defence.

6.2.1 The Next gen firewalls should meet current industry standards, should beconfigured high available (HA) in dual redundancy in all aspects including power source. The firewall shall consists of the minimum features related to Anti-DDOS, NTA, IPS/IDS, Anti-APT. The IMSP isencouraged to supply all features in single box but, separate or mix of any two combinations can be acceptable.

6.2.2 The following are the minimum specifications but may demand higher configurations based on the market at the time of deployment:

6.2.2.1 Proposed solution should have Multi-Layer Threat Prevention suits with controls embedded like IPS, Antimalware, Anti-bot, web filtering, application-visibility/awareness, Anti-APT etc.

6.2.2.2 Should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Selecting rules, configuring policies, updating policies)provide automatic recommendation of removing assigned policies if vulnerability no longer exists.

6.2.2.3 Proposed solution should protect against distributed DoS attack and should have the ability to lock down a computer (prevent all communication) except with management server.

6.2.2.4 Proposed solution should protect against unknown threat using Threat Emulation and Threat Extraction.

6.2.2.5 Proposed solution should use network deception technology for threat detection and analysis.

6.2.2.6 Migration of Policies of the existing Firewall to the new firewall, if any applicable.

6.2.2.7 IPS/IDS:

6.2.2.7.1 The IPS filters must be categorised into the following categories for easy management: - Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities, Network Equipment, Traffic Normalization, Peer to Peer, Internet Messaging, Streaming Media

6.2.2.7.2 IPS solution must have vulnerability based filter which are known for most effectively for Zero Day Attack Protection.

6.2.2.7.3 The proposed IPS should support the ability to mitigate Denial of Service (DoS/DDoS) attacks.

6.2.2.7.4 The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report.

6.2.2.7.5 NG IPS engine must be a smart enough to inspect the traffic based on condition. If the traffic is suspicious then it goes for the deep packet inspection.

6.2.2.7.6 The proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic

6.2.2.8 Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp.

6.2.2.9 Able to auto discover assets communicating in the network.

6.2.2.10 Appliance /devices must support dynamic routing protocols OSPFv2 and v3, BGP, RIP, Multicasting PIM-SM, IGMP v2, and v3 etc.

6.2.2.11 IPS should provide application inspection for SIP, H.323, SNMP, FTP, SMTP, HTTP, DNS, ICMP, DHCP, SNMP to mention a few.

6.2.2.12 IPv6-enabled.

6.2.2.13 Network APT

6.2.2.13.1 The proposed solution should be able to detect and prevent persistent threats that comes through executable files, PDF files, Flash files, RTF files and/or other objects.

6.2.2.13.2 Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network.

6.2.2.13.3 The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.

6.2.2.13.4 The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.

6.2.2.13.5 Upon detection of the threat, the proposed solution should be able to perform behaviour analysis for advance threats.

6.2.2.13.6 The proposed solution should be able to inspect multi-protocol sessions to detect and flag suspicious activities including suspicious file downloads through the web, the suspicious mail attachment and internal infections.

6.2.2.14 Network Traffic Analyzer

6.2.2.14.1 Bandwidth Utilization , bandwidth hogs down to user /application/ device level and flow / packet based Monitoring and reporting.

6.2.2.14.2 Solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.

6.2.2.14.3 The solution should support the identification of applications tunnelling on other ports.

6.2.2.14.4 Should have deep-learning/machine-learning component to detect anomalous and suspicious communication in network traffic irrespective of its origin or destination and, protocol or application.

6.2.2.14.5 Machine Learning: Analyses unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious.

6.2.2.14.6 Should integrate with SOAR for sharing of network data in real time and, alerts as they happen.

6.2.2.14.7 Should include an analytics engine component that processes network traffic and /or generated session metadata to detect threats, risks and, anomalies.

6.2.2.14.8 Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance. Local Malware analysis appliance shall be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries or more in a virtual environment.

6.2.2.14.9 Should support more than 10,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy.

6.2.2.14.10 The solution shall have the capabilities of forensic proof of any unauthorized network access activity as follows: event timestamp, sequential network events, packet capture of suspicious interaction, malware behaviour, type of malware, severity, source and destination of attack. .

6.2.2.14.11 Should support virtual system/instance with each virtual system/instance having dedicated CPU, Memory and Disk, so that each system/instance should be able to run independently in terms of version, and reboot of one should not affect other system/instance.

6.2.2.14.12 Should support capability to integrate with other security solutions to receive contextual information like security group tags/names.

6.2.2.14.13 Should support automatic Real Time Signature generation based on Rate Variant, Rate Invariant algorithms & Challenge Response Mechanisms; within few seconds, without human intervention.

6.2.2.14.14 Should support Open based Application ID for access to community resources and the ability to easily customize security to address new and specific threats and applications quickly.

6.2.2.14.15 Should support behavioural analysis using behavioural algorithms and automation to defend against threats, including Mirai DNS Water Torture, Burst and Randomized attack

6.2.2.14.16 Network-flood protection should include:

6.2.2.14.16.1 TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood

6.2.2.14.16.2 UDP flood, ICMP flood

6.3 NETWORK ACCESS CONTROL (NAC)

6.3.1 The IMSP shall implement Network Access Control (NAC) to enforce policies on machines accessing the network to improve visibility of the network and mitigate risk.

6.3.2 Scope involves the provision, implementation and management of NAC Solution on entire IT Infrastructure. It also include all components and subcomponents like Hardware & Software Licenses, Accessories and other Components. The proposed solutions should support network visibility and access management through policy enforcement on devices and users of corporate networks.

6.3.3 The IMSP shall deliver the Role-based controls of users, devices, applications or security posture post authentication policy enforcement, with designs of pre or post admission enforcement. The IMSP shall use agent or agentless based approach in line or out of band as per industry best practices.

6.3.4 The proposed solution should be a physical appliance deployed in a cluster environment with N+ 1 redundancy with High Availability (HA).

6.3.5 The proposed solution must have RAID redundancy (for hard drives), network redundancy (for management network interfaces) and Power-Supply redundancy, must be easily scalable to support monitoring 100000 devices but should initially support health-check / integration of minimum 5000 End-Points.

6.3.6 The proposed solution / appliance shouldalso have thefollowing capabilities but not limited to:

6.3.6.1 Guest life-cycle management, Profiling and visibility, Guest-networking access, Security posture check,BYOD control, Device Admin/TACACS+, Certificate Authority and Incidence response.

6.3.6.2 Solution should have centralized architecture with web or Graphical User Interface (GUI) based dashboard for monitoring, reporting, notification, maintaining and policy push for the registered users centrally.

6.3.6.3 The solution should not be a "point of failure" in the flow of network traffic; failure of one or more of the solution components should not affect the functionality of the organizational network of ITI’s customers.

6.3.6.4 The solution should support alerting mechanism such as e-mail, SMS, able to identify and authenticate VPN users.

6.3.6.5 Solution must have single unified agent for VPN, Posture assessment & 802.1x authentication

6.3.6.6 Solution must allow supplicant provisioning without MDM

6.4 E-MAIL SECURITY:

6.4.1 A robust Email Security solution that can be have capabilities of signing for out bound mails with non-repudiation signature functionalities with enforced protection policies like SPF, DKIM DMARC.

6.4.2 Solution /Appliance shall support all the Spam, Antivirus, malware security rules, policies.

6.4.3 Shall support email security policies, able to Configure Encryption and DLP rules/policies.

6.4.4 Shall be able to have SMTP whitelist/blacklist rules and polices.

6.4.5 Shall easily integrate with existing systems like Syslog, SIEM, Multi-Service Platform tools and solutions.

6.4.6 Best practices for email security which include and IMSP shall ensure:

6.4.6.1 Utilize email encryption to protect both email content and attachments.

6.4.6.2 Ensure that web mail applications are able to secure logins and use encryption.

6.4.6.3 Implement scanners and other tools to scan messages and block emails containing malware or other malicious files before they reach your end users.

6.4.6.4 Implement a data protection solution to identify sensitive data and prevent it from being lost via email.

6.4.6.5 The solution should have virus-scanning engine available within the appliance that is recognized as a leader in Endpoint security Gartner report.

6.4.6.6 Solution must protect from Forged Email, Cousin Domain and advance phishing attack.

6.4.6.7 Solution should block ransomware and zero-day malware with attachment sandboxing.

6.4.6.8 Solution should stop phishing attacks using machine learning and advanced analysis techniques.

6.4.6.9 Solution should scan malicious URLs at the time-of-click for advanced threats.

6.4.6.10 Solution should generate granular reports for attachments and URLs scanned, junk mail and more.

6.4.6.11 Email Security Appliance must provide a safe view (PDF version) of a message attachment detected as malicious or suspicious.

6.5 SECURITY INFORMATION AND EVENT MANAGEMENT

6.5.1 The proposed Next Gen SIEM solution must enhance threat detection, compliance, and security incident management through the gathering and analysis of real-time and historical security event data and sources. It's main capabilities must provide a broad range of log event collection and management, increasing the ability to analyse log events and other data across dissimilar sources, and operational capabilities including incident management, dashboards, and reporting.

6.5.2 The solution should also offer data aggregation across the enterprise network and normalization of that data for further analysis. Additionally, it should enable security monitoring, user activity monitoring.

6.5.3 The solution / appliance shall have following capabilities:

6.5.3.1 Management & Reporting.

6.5.3.2 Normalization and Indexing.

6.5.3.3 Correlation Engine.

6.5.3.4 Data Management

6.5.4 Solution should encompass log, packet and end point data with added context and threat Intelligence.

6.5.5 The solution should provide an integrated dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.

6.5.6 There should be no limitation on number of devices to be supported. Any addition in number of devices should have no cost impact. The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required.

6.5.7 Solution should categorize log data into an easy-to-understand humanly readable format that does not require knowledge of OEM specific event IDs to conduct investigation, define new correlation rules, and/or create new reports/dashboards. However, the investigations are to be carried out by the successful IMSP.

6.5.8 Should be manageable and monitored from SIEM unified GUI console for Correlation, Alerting and Administration.

6.5.9 Shall apply machine learning, AI based models to detect and mitigate advance threats on real time basisand capable of threat intelligence feeds, dark web monitoring, workflow based automation with zero-day attacks protection of ITIs and its customers IT landscape.

6.5.10 Solution's search performance must be capable of searching through millions of structured (indexed) and unstructured (raw log) events.

6.5.11 SIEM solution should provide a centralized customizable dashboard as required in Multi-Service Platform functionality as per the ITI's requirement.

6.5.12 Solution should initiate actions to remotely disrupt, contain, and neutralize threats.

6.5.13 Solution should include Helpdesk and ticketing tool with the following capabilities:

6.5.13.1 Should be able to support and handle large volume of incident, service requests, and changes.

6.5.13.2 Should provide out-of-the-box categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, location or department.

6.5.13.3 Should support customization of severity level as per the requirements.

6.5.13.4 Should have a predefined/customizable field to indicate & trackprogress/status of the lifecycle of ticket(s).

6.5.13.5 The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure.

6.5.13.6 The ticketing tool should be integrated with ITI's existing Enterprise ticketing tool for ITI to raise the service request, change request and incident management.

6.5.13.7 The solution should have manual and automated escalation mechanism for incidents with SMS, E-mail alerts.

6.5.14 Security Orchestration Automation & Response (SOAR)

6.5.14.1 SOAR solution should be flexible enough to allow security operations to easily create bidirectional integrations with security products not supported by default.

6.5.14.2 SOAR solution should have ability to automate and orchestrate process workflows to achieve force multiplication, and reduce the burden of repetitive tasks on security analysts.

6.5.14.3 Should have capability to provide simulation environment to test playbooks without relying on access to real environment.

6.5.14.4 The following additional features should be available in the SOAR solution:

6.5.14.4.1 Detailed task tracking, including assignment, time spent and status.

6.5.14.4.2 Phase and objective tracking

6.5.14.4.3 Asset management, tracking all physical and virtual assets

6.5.14.4.4 Document and report management

6.5.14.4.5 Indicator and sample tracking, correlation and sharing

6.5.14.4.6 Evidence and chain of custody management involved in the incident

6.5.14.5 Auto-document the entire incident workflow manual as well automated steps for all incidents timestamp of all actions taken in an incident.

6.5.14.6 Provide automated report & dashboards for real time measurement of KPI's including MTTD, MTTR for each incident and overall Multi-Service Platform incidents.

6.5.14.7 Provide automated incident SLA breach report based on severity, type, creation time, closure time, and response time.

6.5.14.8 Should be able to parse all the fields from SIEM, UEBA alerts including but not limited to: creation time, update time, source/destination IP, source country, category, system, rule-name, severity, etc.

6.5.14.9 Should have threat intelligence feeds to properly correlate to the end of discovering attack patterns, potential vulnerabilities and other ongoing risks to the organization.

6.6 END POINT DETECTION AND RESPONSE (EDR)

6.6.1 The proposed Next Gen Endpoint Detection and Response (EDR) solution should detect threats across the environment. It should investigate the entire life cycle of the threat, providing insights into what happened, how it got in, where it has been, what it is doing now, and how to stop it. By containing the threat at the endpoint, the EDR solution should help eliminate the threat and prevent it from spreading. The EDR solution for ITI customers should have following capabilities:

6.6.1.1 The solution should offer EDR platform (Anti-malware, Web Reputation, Device Control, Machine learning , Behaviour Analysis, Endpoint Cloud Sandbox submission, Virtual Patching for endpointand Application Control, Endpoint FW) in single agent.

6.6.1.2 The solution should be able to Monitor and investigate endpoints regardless of their location—on premises, remote, or cloud base.

6.6.1.3 The IMSP will design, test, install, backup & restore, implement, maintain, upgrade, patch, operate, and administer an architecture, methods, and processes that protect Customer's data at rest and data in motion.

6.6.1.4 Detecting unauthorized behaviors of users, applications, or network services.

6.6.1.5 Blocking suspicious actions before execution

6.6.1.6 Processing data through ML and AI to identify malicious files or processes

6.6.1.7 Stopping unauthorized data movement

6.6.1.8 Analyzing suspicious app data in isolated "sandboxes"

6.6.1.9 Rolling back endpoints and data to a previous state in the event of a ransomware attack

6.6.1.10 Isolating suspect endpoints and processes

6.6.1.11 Delivering endpoint detection and response that can continuously monitor systems and networks to mitigate advanced threats.

6.6.1.12 Detection and response to targeted attacks

6.6.1.13 Native support for behavior analysis of users and technology assets

6.6.1.14 Threat intelligence including shared local threat intelligence coupled with externally-acquired threat intelligence sources

6.6.1.15 Reducing the need to chase false positives by correlating and confirming alerts automatically

6.6.1.16 Integrating relevant data for faster, more accurate incident triage

6.6.1.17 Centralized configuration and hardening capability with weighted guidance to help prioritize activities

6.6.1.18 To prepare, deploy, and operate deceptions, modern-day Distributed Deception Platforms (DDPs), use machine self-learning to understand new devices coming on and off the network, along with their profiles and attributes.

6.6.1.19 Comprehensive analytics

6.6.1.20 Prevention & Detection - mechanism to prevent the wide array of commodity and advanced attack routes.

6.6.1.20.1 Able to perform different scan Actions based on various malware types (Trojan, Worm, etc.)

6.6.1.20.2 The solution must identify malicious behaviour of executed files\running processes\registry modifications\ memory access and terminate them at runtime, or raise an alert (exploits, fileless, Macros, PowerShell, WMI etc.).

6.6.1.20.3 The solution must identify and block privilege escalation attacks, reconnaissance attacks (scanning), credential theft attempts form either memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder), lateral movement (SMB relay, pass the hash).

6.6.1.20.4 The solution must generate an intelligence driven detection in the UI.

6.6.1.21 Investigation & Response – overall toolset for efficient reaction to detect & protect live attack.

6.6.1.21.1 Solution must be able to remove (reset) malware changes in the windows registry, remove dropped file(s) and terminates running malicious processes.

6.6.1.21.2 The solution must support isolation and mitigation of malicious presence and activity locally and globally across the entire environment.

6.6.1.22 Monitoring & Control – routine activities to gain visibility and proactively discover and reduce attack surfaces.

6.6.1.22.1 The solution must generate inventory report of managed and un-managed assets on a network.

6.6.1.22.2 Must have behaviour monitoring capability to constantly monitor endpoints for unusual modifications to the operating system, work-related documents or on installed application.

6.6.1.22.3 The solution must include threat hunting.

6.6.1.22.4 The solution must support the discovery of unattended attack surfaces.

6.6.1.23 Infrastructure (EDR with Next Gen AV) - architecture, deployment, data collection and communication.

6.6.1.23.1 The solution must support rapid and seamless installation across all endpoints/servers in the environment.

6.6.1.23.2 The solution must have unified agent for all Windows and MacOSand must be managed from single unified console.

6.6.1.23.3 The sandbox solution must have a user interaction tool that provides a safe environment to dissect malware without the risk of infecting your network. Built into the appliance, analysts are able to interact with the sample while it is being analyzed including opening applications, clicking through dialogue boxes, and even reboot the virtual machine if needed.

6.6.1.23.4 The solution must provide an encrypted communication between the management server and the agents on the endpoints/servers.

6.6.1.24 Operation – ongoing management of EDR with Next Gen AV solution.The IMSP shall provide support for both deployed services /solutions at ITI data centre and customers.

6.6.1.24.1 The solution must also support and integration with common SIEM products, email infrastructure to notify security personnel in case of alerts.

6.6.1.24.2 The solution must assign a risk score to all objects within the protected environment.

6.6.1.24.3 The solution must provide a central collection and processing of alerts in real-time.

6.7 DLP (DATA LOSS PREVENTION)

6.7.1 Enterprise Data loss prevention for personal information protection & security compliance, intellectual property (IP) protection, and data visibility

6.7.2 The IMSP shall configure and tune Data Loss Prevention (DLP) policies as required by Customer.

6.7.3 The integrated DLP should provide protection to customer's data, which includes the following functions:

6.7.3.1 Protects private data - on or off network.

6.7.3.2 Advanced device control capability protects against data leaks via USB drives and other media

6.7.3.3 Aids compliance with greater visibility and enforcement. E.g. GDPR, PCI/DSS, PII, GLBA, HIPAA, PDPA, ISMS, etc.

6.7.3.4 The integrated DLP will be able to support the same policy across various security solutions like Web/Mail gateway, Exchange, Endpoints, etc.

6.7.4 The solution should have an integrated dashboard that provides a balanced view and a high-level summary of incidents. It should provide an overview of information leaks in the system, what actions are being taken on them, which channels are problematic, and what kinds of violations are being made. The report should provide summaries per channel, severity, and action and provides an overall picture of information leaks on in the network.

6.7.5 The proposed solution is able to provide DLP functionality without additional agent footprint or 3rd party integration

6.7.6 Must have customizable DLP templates, option to import and export data identifiers, and add DLP expression

6.7.7 Must be able to integrate with endpoint encryption solution to automatically encrypt protected data at rest and in motion

6.7.8 The solution should beable to integrate with SIEM.

6.7.9 The platform must integrate with quoted orchestration tools to provide end to end automation & rich application context to the workload

6.7.10 Must support user justification option when violating the DLP policies.

6.8 VULNERABILITY ASSESSMENT AND PENETRATION TESTING

6.8.1 To follow Standard frameworks and methodologies exist for conducting penetration tests, these include Open Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), the NIST Special Publication 800-115, the Information System Security Assessment Framework (ISSAF) and the OWASP Testing Guide.Proposed solution should be in alignment with these frameworks and must have the following:

6.8.1.1 The Multi-Service Platform shall have multi-service approaches broadly classified as Breach Attack Simulation Services [Black box], Internal Security Assessment [Grey box], and Red Team vs Blue Team [Adversary Attack Simulation] to understand and improve the overall security posture of ITI customers. The IMSP shall provide Red & blue teaming services as and when required to the ITI's customers.

6.8.2 Live discovery of any digital asset across any computing environment

6.8.3 Continuous visibility into where an asset is secure, or exposed, and to what extent

6.8.4 Prioritisation of remediation based on business risk

6.8.5 Benchmarking of cyber exposure compared to industry peers and best in class organisations

6.8.6 Measurement of cyber exposure as a key risk metric for strategic decision support

6.8.7 Types of testing required shall be but not limited to:

6.8.7.1 Website/Application

6.8.7.2 External/Internal infrastructure.

6.8.7.3 Firewall Ruleset Review (All type of OEMs /vendor devices).

6.8.7.4 Build review (Desktops / laptops /servers including all type of OS).

6.8.7.5 VPN (Including remote access technologies, authenticated or black box test).

6.8.7.6 VOIP

6.8.8 **VAPT Activities**:

The IMSP shall be able to carry out as per the ITI requirement to be comprehensive but not limited to following activities:

6.8.8.1 Network Scanning, Port scanning, system identification and trusted system scanning.

6.8.8.2 Vulnerability scanning, Malware scanning, Spoofing, Application Security Testing.

6.8.8.3 Access Control Mapping, Denial of Service Attack (DOS), Password cracking, Cookie Security.

6.8.8.4 Functional Validations, DMZ Network architecture review, Firewall rule review, OS Security configuration, Database Security Configuration, any other attacks.

6.8.8.5 Website / Web – Application Assessment :Website / Web- Application assessment should be done as per the latest OWASP guidelines including the following:

6.8.8.5.1 Vulnerabilities to SQL Injections, CRLF injections, Directory Traversal, Authentication hacking/attacks.

6.8.8.5.2 Password strength on authentication pages, Scan Java Script for security vulnerabilities, File inclusion attacks, Exploitable hacking vulnerable.

6.8.8.5.3 Web server information security, HTTP Injection, Phishing a website, Buffer Overflows, Invalid Inputs, and Insecure Storage.

6.8.8.5.4 Any Other attacks, which are vulnerability to the website and web-applications.

6.8.8.5.5 Web Assessment should be done by using Industry Standards and also as per the Open Web Application Security Project (OWASP) methodology to Identify the security vulnerabilities including top web application vulnerabilities viz. Cross Site Scripting (XSS), Injection Flaws, Malicious File Execution, Insecure Direct Object Reference, Cross Site Request Forgery(CSRF), Information Leakage and Improper Error Handling, Broken Authentication and Session Management, Insecure Cryptographic Storage, Insecure Communications, Failure to Restrict URL Access

6.8.8.5.6 Identify remedial solutions and recommendations for making the web applications secure.

6.8.8.6 Approach to be followed in Penetration Testing is given here in below:

6.8.8.6.1 Aggressiveness (Passive Scanning).

6.8.8.6.2 Information base (Grey Box Test).

6.8.8.6.3 Scope (Focused).

6.8.8.6.4 Approach (Overt).

6.8.8.6.5 Technique (Network-based).

6.8.8.6.6 Starting point (from the outside and the inside)

6.8.9 **Method of VAPT:**

6.8.9.1 Conduct of VAPT as per the Scope, Evaluation & Submission of Preliminary Reports of Findings and Discussion on the Findings.

6.8.9.2 Submission of Reports with detailed security gaps, addressing the gaps and resolution of the same.

6.8.9.3 Final submission of the reports by the vendor and acceptance of the Report by ITI Ltd or its customers.

6.8.9.4 Any other Specific Reporting Requirements as and when required by the ITI or its customers with a regular status reporting at executive level and strategic level, comprehensively technical reports to ITI team with review in details of gaps identified and recommendations.

6.8.9.5 The selected IMSP should also make arrangements to have sufficient team to carry out other IT audits in ITI's customers premises as and when required

6.8.9.6 VAPT benchmarking can be as per the CIS practices, which are globally acceptable.

6.9 ANALYTICS AS A SERVICE INCLUDES UEBA

6.9.1 The proposed UEBA solution should focus on analysing activity – specifically user behaviour, device usage, and security events - within the network environment to help companies detect potential insider threats and compromised accounts. It should define a type of cyber security process that takes note of the normal conduct of users. In turn, they should detect any anomalous behaviour or instances when there are deviations from these "normal" patterns. The solution provided by the IMSP should cover the following features:

6.9.1.1 The ability to use behavioural base lining to accurately detect compromised user accounts.

6.9.1.2 Automation to create improved security efficiency.

6.9.1.3 The use of advanced behavioural analytics to help reduce the attack surface by frequently updating IT security staff and network admins about any potential weak points within the network.

6.9.1.4 Data-feed correlation (correlating multiple feeds and understanding relative risk across all entities).

6.9.1.5 The analytics platform must capture and analyze flow and process telemetry from all workloads across ITI DC, in real time and store in a time-series for data retention for minimum upto 5 months.

6.9.1.6 The platform must provide capability to edit and modify the discovered policies to define and include more absolute protection policies. It must export the policy to Network fabric, security devices etc.

6.9.1.7 The solution should detect unknown, zero day, and advanced persistent threats using pre-built threat content focused on insider threats, fraud, and other key use cases.

6.9.1.8 The solution should generate comprehensive identity and risk profiles for every user and entity.

6.9.1.9 The platform must integrate with quoted orchestration tools to provide end to end automation & rich application context to the workload

6.9.1.10 The platform must automatically group endpoints with similar behaviour and security posture into policy groups and should be able to correlate network traffic to actual application process that generated it.

6.9.1.11 The platform must provide the ability to simulate the policies using near real time data, without having to enforce the policy.

6.9.1.12 The analytics platform must automatically generate per application whitelist policy and enforce the auto generated whitelist policy allowing only the required traffic, blocking everything else.

6.9.1.13 The platform must provide full audit logging of all system access and changes applied.

6.9.1.14 Application policy must be dynamically updated and enforced as application changes.e.g. scale-out, migration, DR etc.

The above all proposed services should be complaint with IT Governance, Risk and Compliance (GRC) and provide a single, federated framework to integrate various IT processes and security solutions and support those processes for the purpose of defining, maintaining and monitoring GRC. All security related applications, dashboards and other tools and techniques should be in line with MITRE ATT&CK framework, ISO/IEC 27001 and 27002, ISO 15408 complaint, IPV6 ready. CVE compliant and provides vulnerability risk scoring based on accepted industry standards (CVE,CVSS). And generate vulnerability risk score based on CVE/CVSS standards and report in the form of dashboards.

6.10 MULTI-SERVICE PLATFORM ACTIVITIES

A successful IMSP shall expected to perform the following activities at ITI Multi-Service Platform.

6.10.1 Security monitoring of attacks into/on/against IT assets. The IMSP shall provide support for both deployed services /solutions at ITI data centre and customers end point.

6.10.2 Manage security, configuration, availability, performance management, advisory for the security devices and its software.

6.10.3 Ensure Malware Scanning / Protection/ Presentation /Reporting as required by any organization total Anti-APT solution.

6.10.4 Provide proactive threat intelligence and threat hunting.

6.10.5 Vulnerability Assessment & Penetration Testing for critical devices/ servers /applications/solutions on quarterly basis / as and when required and provide solution for closure.

6.10.6 Risk assessment and mitigation, protection, execution support for the Security solutions, devices, software and tools of Multi-Service Platform.

6.10.7 Ensure adherence to organization's Information Security Policy and Cyber Security Policy.

6.10.8 Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments ITAA 2008 and guidelines in place.

6.10.9 Provide forensics support as per the requirement of ITI in case of any incident or as and when required.

6.10.10 Adhere to the Dashboards for reporting and SLA management.

6.10.11 **Event Classification &Triage**:

6.10.11.1 Regular monitoring and continuous learning of the network traffic and integration with honeypots of threats and vulnerabilities to classify an event on the network as threat.

6.10.11.2 There should be a real time response classification with the help of advanced security solutions and hardware capabilities in built with the network gateway.

6.10.12 **Prioritization & Analysis**:

6.10.12.1 Threats have to be prioritized based on the severity of the impact it is going to have on our business and infrastructure. A typical high, medium , low can be warranted.

6.10.12.2 All high priority threats must be addressed first and a detailed analysis and RCA must follow thereof, medium and low cannot be left unattended but must be addressed as soon as possible. No threat can be left unaddressed.

6.10.12.3 The analysis and RCA therefore must be used to createmore accurate classification and an triage system through continuous feedback and machine learning.

6.10.13**Remediation &Recovery**:

6.10.13.1 Real time remediation of the threat to the network and systems must have a plan in the form of a playbook and must adhere and complete the remediation activities.

6.10.13.2 A detailed list of steps undertaken and possible measures to avoid such in future must be a part of the playbook for reference and security guide.

6.10.13.3 Recovery measure should immediately follow protocols and approvals when there are special provisions to be made on the current processes or configurations.

6.10.14**Assessment &Audit**:

6.10.14.1 Regular and frequent assessment and audit on a pre-defined interval and sometimes ad-hoc in cases of special events must be common place and part of the Multi-Service Platform implicit activities.

6.10.14.2 A report of the audit must be analysed and discussed with a larger group to seek feedback and establish newer processed or configuration for a harder network and systems.

6.10.15**Security Dashboards &Reports**:

6.10.15.1 A visual snapshot of the security posture of the organization via dashboards and reports warrants a better understanding of the posture and enables to make better and informed decisions. The dashboards and report generation needs to be developed as per the ITI's requirements and customer requirements.

6.10.15.2 Customization of reports based on traffic, web protocols, location, services etc. must be available and can handle future customizations.

6.10.16**TOOLS AND SERVICES:**

The IMSPshall provide following tools, appliances and services related to various deliverables mentioned in the detailed scope of work but not limited to the following:

6.10.16.1 Asset Discovery, Vulnerability Assessment, Intrusion Detection, Behavioural Monitoring and Security Analytics. SIEM, Anti-APT (advanced persistence threat), VAPT advisory and remediation services. Analytics and dashboard development.

7 MULTI-SERVICE PLATFORM MINIMUM REQUIREMENTS:

7.1 SCALABILITY

All components of the Multi-Service Platform must support scalability to provide continuous growth to meet the requirements and demand coming in from various customers. A scalable Multi-Service Platform shall easily be expanded or upgraded on demand.

7.2 AVAILABILITY

All components of the Multi-Service Platform must provide adequate redundancy to ensure high availability of the Governance applications and other Multi-Service Platform services. Designing for availability assumes that systems will fail, are configured to recover from component or service failures with no application outage. The IMSP shall make the provision for high availability for all the services of Multi-Service Platform.

7.3 INTEGRATION AND INTEROPERABILITY

The entire proposed system/ subsystem should be integrated with all of the IT systems available in customer premises including legacy, interoperable to support information flow and integration. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

7.4 VALIDATION AND UAT AT ITI:

7.4.1 For all type of services deployed as per the tender, the IMSP, should validate all the services. The UAT sign off will be based on the meeting all the requirements and test case execution success on each feature of the service. Pre-UAT should be carried out by bidder, before offering UAT to ITI. Draft Format/structure of UAT should be submitted to ITI alongwith pre-UAT. UAT will be carried out by bidder based on UAT format approved by ITI.The IMSPis expected to utilize the existing network and infrastructure to validate the services for sign off. The UATshould be carried free of cost.

7.5 DOCUMENTATION:

For each service and features deployed at ITI or its customers, proper documentation of the service, and the corresponding training should be provided to the ITI or its customers. The project is deemed complete only after proper documentation is provided.

The IMSPs shall also provide the following documents as part of the deliverables of the project.

7.5.1 Original manuals of all proposed hardware/software/applications.

7.5.2 Standard Operating Procedures (SOP).

7.5.3 Installation & Configuration Documents.

7.5.4 Network & Security Design Documents (Will be approved by the ITI or its customers).

7.5.5 Troubleshooting Manual.

7.5.6 Executive summary report for the project to the management.

7.5.7 Functional and operational requirements.

7.5.8 Project design/plan and Product description.

7.5.9 Guidance for best practices in implementation, operation and maintenance.

7.5.10 User acceptance test documents and Training materials.

7.5.11 Health check-up reports on every quarterly basis.

8 WARRANTY AND MAINTENANCE SUPPORT

a) The IMSP shall guarantee 24x7 availability with monthly uptime of 99.9% for the all the services under this project during the period of the Contract.

b) The "Uptime" is, for calculation purposes, equals to the Total contracted hours in a quarter less the Downtime. The "Downtime" is the time between the Time of Failure and Time of Restoration within the contracted hours. "Failure" is the condition that renders the ITI or ITI's customer unable to perform any of the defined functions. "Restoration" is the condition when the selected IMSP demonstrates that the solution is in working order and the ITI Ltd acknowledges the same.

c) If the IMSP is not able to attend the troubleshooting calls on solution due to closure of the office/non-availability of access to the solution, the response time/uptime will be taken from the opening of the office for the purpose of uptime calculation. The IMSP shall provide the Monthly uptime reports during the warranty and Operation and Maintenance period..

d) The percentage uptime is calculated on monthly basis as follows:

$$\frac{\text{(Total contracted hours in a month – Downtime hours within contracted hours) *100}}{\text{Total contracted hours in a month}}$$

g) For repeat failure, same or higher penaltywill be charged depending upon the delay in rectification of the problem.

h) Penaltywill be calculated on monthly basis and deducted against the Quarterly payments.

i) In case of Multi-Service Platform operations failure, the penaltywill be charged for both Multi-Service Platform Operations failure and individual security services /device failure.

m) The ITI reserves right to recover / adjust the Penalty from any dues pending to the IMSP.

n) However, the maximum Penalty levied shall not be more than the 20% of total value of the order per month.

o) If monthly uptime of Multi-Service Platform operations is less than 95%, the ITI shall levy penalty as above and shall have full right to issue notice & seek explanation under this tender document. The above penaltyshall be deducted from any payments due to the IMSP.

p) All the above Penalties are independent of each other and are applicable separately and concurrently.

q) Warranty shall be for a period of one year from completion of Supply, Installation, Testing and Commissioning of required hardware and software, appliances, tools modules including mapping of all business processes related to ITI Ltd customers.

r) The IMSP further represents and warrants that all licenses delivered / rendered under and in accordance with contract shall have no defect, arising from design or from any act, error/defect or omission of the Multi-Service Platform.

s) Upon receipt of notice of such defect / error or deficiency, the Bid shall, with all reasonable speed, repair or replace the defective equipment/software or parts thereof, without cost to Purchaser.

t) The IMSP shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all equipment, accessories etc. covered by the tender

u) Analysis & Requirements Study: IMSP shall study the entire solution, network infrastructure, existing Hardware and software, migration requirement if any required.

v) The network can be audited by forensic auditors/ethical hackers including third party agencies such as IITs, IIITs, IISc. Based on the inputs received from those auditors/third party agencies, the IMSP has to strengthen the network or all of the services in line with the industry standard.

9 SLAs AND PENALTIES FOR MULTI-SERVICE PLATFORM INDIVIDUAL MODULES

9.1 For purposes of this Service Level Agreement, the definitions and terms as specified in the agreement along with the following terms shall have the meanings set forth below:

- **"Availability"** shall mean the time for which the services and facilities offered by the implementation agency are available for conducting operations from the equipment /services offered.
- **"Incident"** refers to:
    - Any event / abnormalities in the functioning of the Multi-Service Platform services that may lead to disruption of Multi-Service Platform services.
    - Any security compromise or vulnerability observed in the client infrastructure.
- **"Uptime"** is the time the services and facilities are available,
- **"Security Monitoring"** means monitoring, identifying, analysing and responding all IT security related alerts and incidents occur due to exploitation of any vulnerabilities, through various threats or attack vectors.

"Priority" is the relative importance of an Incident based on Impact and Urgency of the required service. Incident designated with (i) **Priority Level - 1 (High)** characterized by High Impact and High Urgency, Major Business interruption, No workarounds is available, Emergency change may be required, (ii) **Priority Level – 2 (Medium)** characterized by High Impact and Medium Urgency; or Medium Impact and High Urgency; Business interruption, typically Workaround is available; and an Emergency Change is not required but a Normal Change may be required; (iii) **Priority Level – 3 (Low)** characterized by Low Impact and Medium Urgency; Medium Impact and Low Urgency, no business interruption, typically Workaround is available, any required Normal Changes can be planned for a date and time agreed with the customer.

For SLA calculation the following for formula is to be adapted where ever applicable appropriately

For Uptime

(Total number of contracted hours in a month – downtime hours with in the contract hours)*100

Total number of contracted hours in a month

For ticket resolution

(Total number of tickets unresolved in a month)*100

Total number of tickets books in a month

Sr.	Service Area	Service Level	Service time / quality	Service Level compliance measured per month & Penalties	
1	1. Security devices, logs Monitoring & Incident Reporting, Response 2. New use cases, request of logs, new devices integrations	1. Security Event Alerting, Log Analysis, Incident response Services. 2. 24x7 monitoring of all security devices in scope. 3. Categorization of Incidents into High, Medium and Low priority shall be carried out in consultation with the selected IMSP during the contract period.	**Response Time** 1. Critical Security Alerts (Priority 1) to be reported within 60 minutes. 2. High Criticality Security Alerts (Priority 2) to be reported within 2-4 hours. 3. Med/Low Criticality Security Alerts (Priority 3) to be reported within 8-12 hours	**MinimumSL target**: P1 – 97% P2 – 95% P3 – 92% **Expected SLA** P1 – 99% P2 – 97% P3 – 95%	Below 92% SL - Penalty: 0.1% of monthly payment per ticket Below Minimum SL target Penalty: P1 –0.5% P2 - 0.3% of monthly payment per ticket
2	Security incident resolution	1. Event Analysing, Triaging and Incident Resolution Services. 2. Sending out investigation details and status update of Incident to all ITI customers as per SL below: P1 – every 30 minute P2 – every 2 hour P3 – every 8 hours 3. Detail escalation matrix shall be finalized in consultation with the selected IMSP during the contract period.	**Resolution Time:** 1. High priority incident within 2 hours 2. Medium priority incident within 8 hours 3. Low priority incident within 24 hours	Minimum **SL target**: P1 – 98% P2 – 95% P3 – 93% **Expected SL target** P1 – 99% P2 – 97% P3 – 95%	Below 93% SL - Penalty: 0.1% of monthly paymentper ticket Below Minimum SL target Penalty: P1 - 0.5% P2 - 0.3% of monthly payment per ticket
3	Root Cause Analysis Reports and Closure	1. Sending out detailed Root Cause Analysis report post alert notification. 2. Action plan / mitigation steps for long term solution should be reported to ITI/ITI Customer point of contact as per the SL	**RCA & Closure** 1. High priority incident within 1-2 business day 2. Medium priority incident within 2-4 business day. 3. Low priority incident within 4-8 business day	Minimum **SL target**: P1 – 90% P2 – 87% P3 – 85% **Expected SL target** P1 – 95% P2 – 90% P3 – 87%	Below 85% SL - Penalty: 0.1% of monthly payment Below Minimum SL target Penalty: P1 - 0.5% P2 - 0.3% of monthly payment
4	Reports and Dashboard	1. Business metrics reporting. 2. Weekly, Monthly, Quarterly reports for each ITI's customer.	**Reporting** **Weekly:** day of week as agreed **Monthly**: Before 5th working day of each month **Quarterly**: 1st week of next quarter	Minimum **SL target**: 90% **Expected SL target** 95%	Below 90% SL - Penalty: 0.1% of monthly payment

5	Service uptime of all devices, system & tools pertaining to Multi-Service Platform solution	1. 24x7 uptime of all security devices in scope 2. Maintaining adequate spares, backup software, license, tools on-site	All critical system uptime desired is 100%	Minimum **SL target**: 99% **Expected SL target** 100%	Below 99% Penalty: 0.3% of monthly paymentper hour
6	Vulnerability Assessment & Penetration Testing	1. Security Vulnerability Scanning, Assessments of the enterprise IT infrastructure, OS, Network IP and applications and remediation upon ITI/ITI's customer approval / concurrence.	Monthly scanning report – 5th of calendar month **Resolution of vulnerability SL**: 1. Critical vulnerability alerts within 24 hours of identification. 2. High vulnerability alerts within 2 business day of identification 3. Non-critical and other vulnerability alerts within 4 business days of identification.	Minimum **SL target**: 90% **Expected SL target** 95%	Below 90% Penalty: 0.2% of monthly payment per ticket
7	Security Patch Upgrade	1. Assessment of existing security patch in all Multi-Service Platform and End points. 2. MSP Systems and end points shall be upgraded with the latest security patches upon ITI/ITI's customer approval	1. Ad-hoc patch upgrade as required as per Incident SL 2. Monthly patch upgrade successfully with 95% systems.	Minimum **SL target**: 90% **Expected SL target** 97%	Below 90% Penalty: 0.2% of monthly payment
8	Security Intelligence Services	1. Assessment and identification of global cyber threat & vulnerabilities and remediation	1. Advisories within 6 hours of new global threats & vulnerabilities disclosures 2. Resolution of vulnerability as per Sr. No. 6 above	Minimum **SL target**: 95% **Expected SL target** 97%	Below 95% Penalty: 0.5% of monthly payment
9	Continuous Service Level Improvement	1. Define a clear service improvement strategy from the past failure, learning, interaction with ITI/ITI's Customer	1. Minimum 2 ideas, CSI process per month 2. Reduction of TCO by 10% per quarter for ITI/ITI's customer	Minimum **SL target**: 93% **Expected SL target** 95%	Below 93% Penalty: 0.3% of monthly payment

Incident and Alarm Description

"Incident" are referred as:

- Any event/abnormalities in the functioning of the Multi-Service Platform equipment/services that may lead to disruption of Multi-Service Platform services.
- Any security compromise or vulnerability observed in the client infrastructure.

Incidents are classified into different severity level based on the impact of the incident:

S. no.	Severity Level	Incident Classification
1	Critical	I. Incidents, whose resolution shall require like device failure, device module failure, port failure, etc. The SLA would be measured for the time taken to bypass the device, establish logical redundancy and restore rest of the services of Multi-Service Platform. II. Any security incident occurred / vulnerability found, bearing impact to disable the operations of a whole Multi-Service Platform / part of the Multi-Service Platform elements. III. Any incident reported by Multi-Service Platform where a breach had already occurred.
2	High	I. Incidents, whose resolution require change in the architecture / design / configuration of the Multi-Service Platform components. II. Integration issue with any Multi-Service Platform infrastructure. III. Any security incident / vulnerability found bearing impact to disrupt the operation of any asset and limited to that asset only (example: network device, server, website, etc.). The SLA would be measured as per the time taken to isolate the device from the network without disrupting the rest of the operations of SOC. IV. Any other incident having an impact on the services provided by Multi-Service Platform
3	Medium	I. Incidents, whose resolution require software upgradation / patch management for the Multi-Service Platform infrastructure but have no serious impact on the ITI's Multi-Service Platform infrastructure. II. Any security incident / vulnerability found bearing no current impact on the ITI's infrastructure but may arise as a serious threat in future.
4	Low	I. Alerts / events reported by the Multi-Service Platform team which may be doubtful in nature as false positive and requires further investigation. II. Incident bearing no threat but only to be circulated as awareness and information . III. Any security threat / update provided by recognized bodies (e.g. CERT-In, NIST, etc.) for inclusion in Multi-Service Platform as best practises.

Note :

I. The above defined severity levels are base levels and can be framed/added more on mutual agreed terms and conditions after the selection of the IMSP.

II. The critical and high incident should be analysed and root cause analysis for the same should be provided by the successful IMSP for every such incident.

Note :-

1. Maximum combined penalty is to be capped at 20% of total monthly operation and maintenance charge for all the functional SLAs mentioned.

9.2 Operation and maintenance (O&M) :

9.2.1 IMSP shall provide O&M services for 3 years period. The cost of operation and maintenance will be fixed for 3 years. After completion of 3 years, an increment of 10% per yearwill be provided up to 5 years based on the performance of the IMSP. There will be an annual performance review for IMSP

9.2.2 The selected IMSP shall be required to sign an Operation and MaintenanceContract for Hardware & Software, appliances and tools as per the provisions made in this tender document at the time of acceptance of PO.

9.2.3 The IMSP should have an arrangement with the OEM such that ITI or its customers are able to log a call with the OEM directly.

9.2.4 No separate charges shall be paid to the IMSP for visit of engineers for attending the faults and repairs and for supply and transportation of spare parts.

9.2.5 The IMSP shall provide required services below during the O&M period:

9.2.5.1 Provide ITI/ITI's Customer with trouble shooting activities. The analysed issue will serve as an alternate escalation point to any phone 'hotline' IMSP may provide, and will directly contribute to the delivery of Customer's emergency Incident response. The deployed team must have at least three members with any one of the security certifications like CISA, CISM, and CISSP and have more than 4 years work experience in SOC operations.

9.2.5.2 Provide as requested by ITI/ITI's Customer any logs or alert/event information to assist in responding to Security Incidents according to Customer's security requirements and processes;

9.2.5.3 Coordinate and assist ITI/ITI's Customer with collecting and shipping systems or devices to be retained as evidence as deemed necessary by Customer.

9.2.5.4 Coordinate trouble shooting activities in conjunction with Customer's IT security team to the data integrity of any asset, which may be needed for evidence.

9.2.5.5 Coordinate collecting and providing ITI/ITI's Customer with any data or hardware deemed necessary by ITI/ITI's Customer to assist with the Incident response including logs, disk drives, files, servers, work stations, and other items which may be of evidentiary value.

9.2.5.6 Provide evidence acquisition including, but not limited to on-site data collection and digital forensic and fraud investigation as and when required.

9.2.5.7 Ensure all collected evidence adheres to documented chain of custody procedures.

9.2.5.8 Maintain evidence integrity and maintain strict chain of custody procedures for any items (physical or logical) pertinent to the Incident response investigation;

9.2.5.9 Provide assistance to ITI/ITI's Customer on validating and determining impact and scope of a potential security breach.

9.2.4.10.On the request of Customer, identify the initial point of entry into the system, the source of the intrusion, the tools and methods employed by the intruders, and any data compromised, as well as a list of all other systems, applications, or Third-Parties potentially compromised.

9.2.4.11.Assist Customer's IT security team in determining root cause analysis of a Security Incident or breach.

9.2.4.12.Provide the capability, lab environment, tools, and skills to reverse engineer various forms of malware to provide a detailed analysis of attack vectors.

9.2.4.13.Participate in event calls in conjunction with Customer's IT security team for the purposes of escalating and resolving a Security Incident.

9.2.4.14.Work with Customer's IT Security team in the restoration of IT services to Customer's Environments and problem resolution in accordance with Customer's security requirements.

9.2.4.15.Record timelines, actions, and events in accordance with Customer's security requirements and Security Incident management in the event of a Security Incident.

9.2.4.16.Provide reports in the Security Dashboard of all Security Incident response details and activities.

9.2.4.17.Follow the escalation notification processes in accordance with Customer's Security requirements when IMSP identifies or is made aware of a security violation.

9.2.4.18.Provide on-demand automated electronic software deployment for Security Incident detection, remediation, and prevention efforts.

9.2.4.19.Perform detection and remediation activities which include:

9.2.4.19.1. Custom device scans to search for any policy violations including system.

9.2.4.19.2. Registry identifiers, hash matches (e.g., SHA1, SHA2, MD5), file size, file version etc. related to potential active Security Incidents.

9.2.5.9.1 During an active Security Incident, deploy security patches as defined by ITI/ITI's Customer Incident management processes.

9.2.5.9.2 During an active Security Incident, accompanying activities include:

9.2.5.9.2.1 Requirements gathering.

9.2.5.9.2.2 Collecting\refining\reporting of requested data collection.

9.2.5.9.2.3 Remediation action deployment.

9.2.5.9.2.4 24/7 engineering and deployment support during open Incident.

9.2.5.9.2.5 Participate in Customer's annual Incident response management exercises and provide recommendations for improvements based on the lessons learned.

9.2.6 Further , IMSP has to ensure the following points:

9.2.6.1 End of Support Life (EOSL) date for all the hardware and software item does not end before the end of the contract period. IMSP has to provide O&M during the contract period on extended EOSL basis for hardware and software applications in case needed at no extra cost to the purchaser.

9.2.6.2 In case the support of EOSL items is not extended by the OEMs, the IMSP shall arrange replacement of EOSL equipment in order to provide continued O&M services for entire period (i.e. Five years from start date of O&M) at no extra cost to the purchaser. The replaced products shall meet the requirements of the tender.

9.2.6.3 All the devices, appliances, software, hardware, resources that will be deployed should be complied with the guidelines of Govt. of India, CERT-in. The IMSP shall support to ITI during the process of CERT-in empanelment and IMSP should strictly follow the CERT-in guidelines during the entire engagement with ITI Ltd.

9.2.6.4 IMSP has to ensure upgrades/patches to latest version of deployed firmware, operating systems, security solution and application software during the period of O&M. Necessary changes in customization/configuration have to be done at no extra cost to the purchaser.

9.2.7 Patch Management

9.2.7.1 The patch management solution should be compatible with different Hardware provider OEM (HP, IBM, Dell, Wipro, Cisco).

9.2.7.2 The patch management solution should have regular patch update facility for all terminal devices (desktops & severs) including Software and Hardware, asset inventory management broadly covers Number of OS instances, Types of Server - Physical and Virtual Environment, various Server Operating system, Various types of Operating system - Windows, Unix and Linux with CPU/cores counts running in Desktops & Servers.

9.2.7.3 Able to identify and report the machines that have installed the patch that is to be rolled back.

9.2.7.4 The system must be intelligent to check the relevance of the computer before deploying a patch after download on the endpoint.

9.2.8 The support for upgrade, optimization, re-organization and tuning of hardware and software , tools appliances after commissioning, whenever needed during Warranty, O&M period shall be provided by the IMSP at no extra cost to the ITI Ltd.

9.3 **Training & Development**

9.3.1 ITI team members must be trained as and when required and able manage the Multi-Service Platform activities.

9.3.2 Responsibility Matrix and Frequency of training.

Responsibility matrix:	
Training	**Responsibility**
Project Execution Team Training on OEM Products	IMSP
ITI Support team Training	IMSP
Business User Training	IMSP
Frequency of Training	
Training	**Frequency**
Project Execution Team Training on OEM Products	1. Before start of the project training on systems /appliances /Tools & Techniques ofApplication implementation process.
	2. Refresher training every 2 weeks
	3.Incremental training on overall implementation
Support operation & Maintenance Training	1. Post project implementation process ends, trainings on all products /appliances /Tool & techniques applications development to be imparted to ITI team, ITI team will handle the L1 support activities.
	2. Refresher training once in every 2 weeks.

9.3.3 The IMSP shall provide all training material, documents and training aids. It shall also allow ITI's team to create copies of the training material for internal consumption (within ITI Ltd). The training material shall include all installation, configuration, customisation, operation & Maintenance, administration of all modules independently for all appliances /devices /tools & techniques. Training on various software modules shall have to be imparted by the Subject matter expert (SME) of the respective IMSP/ original equipment manufacturer (OEMs).

1. The training requirements are summarized below: No. of trainees – 50
2. Planning Phase: No. of Persons to be trained: 50
3. Execution Phase: Training for ITI team during Execution phase: Core team Training (Through Train-the-trainer program):

Module-wise training to be provided in the train-the-trainer program will be in the following manner:

Sr. No.	Module	No. of days Minimum	No. of Persons to be trained
1	IAM	10	4
2	SIEM	10	7
3	VAPT & Application scan	10	5
4	NG Firewall / Network Traffic analyser	7	5
5	UEBA	5	7
6	NAC	5	5
7	Email security	5	5
8	EDR	7	7
9	DLP	5	5

9.3.4 O&M Phase:

Specialized Refresher Training: Regular refresher trainings shall be imparted by IMSP to ITI team on various security modules / services as and when required.
No. of Persons to be trained: 50 persons across the organization involved in operation and support activities.
Period of training for each trainee: Minimum 1 month during project implementation, maintenance and support period\

9.3.5 Responsibility Matrix

S. no.	Designation	Roles and Responsibilities
1	Level 1 (ITI)	Level-1 activities will be the responsibility of ITI and consists of following. • Level 1 analyst will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available Multi-Service Platform log sources that include: o Firewalls and network devices. o Infrastructure server and end-user systems. o Threat intelligence platforms. o Web proxies. o Application logs and web-application firewalls. o Identity and access management systems. o Cloud and hybrid-IT provisioning, access, and infrastructure systems. o Antivirus systems. o Intrusion detection and prevention systems. • Monitor incoming event queues for potential security incidents.

		• Perform initial investigation and triage of potential incidents, and escalate or close events as applicable. • Monitor Multi-Service Platform ticket (or email) queue for potential event reporting from outside entities and individual users. • Maintain Multi-Service Platform shift logs with relevant activity from the shift. • Document investigation results, ensuring relevant details are reported to level 2 analyst for final event analysis. • Update or refer Multi-Service Platform collaboration tool as necessary for changes to Multi-Service Platform process and procedure as well as ingest Multi-Service Platform daily intelligence reports and previous shift logs. • Conduct security research and intelligence gathering on emerging threats and exploits. • Perform additional auxiliary responsibilities as outlined in the console monitoring procedure.
2	Level 2 (IMSP)	Level-2 activities will be the responsibility of Multi Service Provider and consists of following. • Approve and, if necessary, further investigate level 1- escalated events. • Mentor level 1 analysts to improve detection capability within the Multi-Service Platform. • Manage Multi-Service Platform event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary. • Serve as detection authority for initial incident declaration. • Function as shift subject-matter experts on incident detection and analysis techniques, providing guidance to junior analysts and making recommendations to organizational managers. • Drive and monitor shift-related metrics processes ensuring applicable reporting is gathered and disseminated per Multi-Service Platform requirements. • Conduct security research and intelligence gathering on emerging threats and exploits. • Serve as a backup analyst for any potential coverage gaps to ensure business continuity. • MSP Performance Monitoring. • Responsible for infrastructure deployment and upkeep and content development. • Develop, implement, and execute the standard procedures for the administration, backup, disaster recovery, and operation of the Multi-Service Platform systems infrastructure, including: o Operating system security hardening o Backup management o Capacity planning o Change management o Version or patch management

		○ Lifecycle upgrade management ○ Configuration management • Develop and maintain the technical architecture of the Multi-Service Platform system, enabling all the components to perform as expected and meeting established service-level objectives for system uptime. • Perform routine equipment checks and preventative maintenance. • Maintain up-to-date documentation of designs or configurations. • Respond to after hours (on-call support) infrastructure issues as required. • Be responsible for new product release management, policy and integration testing, security testing and vendor management. • Maintain hardware or software revisions, SIEM content, security patches, hardening, and documentation. • Develop and deploy content for the Multi-Service Platform infrastructure, including use cases for dashboards, active channels, reports, rules, filters, trends, and active lists. • Monitor and help optimize data flow using aggregation, filters, and use cases to improve the Multi-Service Platform monitoring and response capabilities. • Coordinate and conduct event collection, log management, event management, compliance automation, and identity monitoring activities. • Respond to day-to-day security change requests related to Multi-Service Platform operations.
3	Level 3 (IMSP)	Level-3 activities will be the responsibility of Multi Service Provider and consists of following. • Escalation handing and prompt issue resolution on the issues escalated by Customer , Multi-Service Platform in-charge or ITI Management • Reviews asset discovery and vulnerability assessment data. • Review standard security arrangements, provide external/semi-external reviews. • Explores ways to identify stealthy threats that may have found their way inside network, without detection, using previous experience in threat intelligence. • Conducts vulnerability and penetration tests on production systems to validate resiliency and identify areas of weakness to fix. • Investigate new vulnerabilities and share the latest industry level responses. • Recommends how to optimize security monitoring tools based on threat hunting discoveries. • Incident Forensic handling and analysis. • Network and security consulting and training. • Risk assessment and mitigation. • Manage remotely stored critical information (passwords, network configurations, etc.) during any high level incident. • Responsible for achieving the goals of the Multi-Service Platform program through the implementation of processes, procedures, and performance indicators related to security incidents and prevention management.

		• Responsible for maintaining smooth operations, ensuring service-level agreements (SLAs) are met. • Manage the overall day-to-day operations. They are responsible for ensuring events and/or incidents are detected and responded to in adherence to established process as well as procedures. • Oversee the analysts' daily tasking. • Manage the team's work scheduling. • Ensure effective incident management. • Identify chronic operational and security issues, and ensure they are managed appropriately. • Manage and escalate roadblocks that may jeopardize security monitoring operations, infrastructure and SLAs. • Serve as a senior mentor to Multi-Service Platform staff. • Track tactical issues in execution of Multi-Service Platform responsibilities. • Document and track analyst training requirements. • Ensure analysts follow existing procedures and all procedures are documented in accordance with local guidelines. • Manage the process improvement program for Multi-Service Platform processes. • Creation of reports, dashboards for Multi-Service Platform operation on weekly basis.

10 TERMINATION

ITI Ltd has various clauses for termination as under:

S.N.	Details for Termination
1	**Termination for non-performance (not meeting SLA)** ITI Ltdmay,withoutprejudicetoanyotherremedyforbreachofcontract,bygiving written notice of **30 days** to the IMSP, terminate the contract in whole or part a) If the IMSP fails to deliver any or all of the services within the period(s) specified in the contract or within any extension thereof granted by the ITI Ltd pursuanttoconditionsofcontractOR b) The Selected IMSP breaches its obligations under the scope document or the subsequent agreement and if the breach is not cured within 30 days from the date of noticeOR c) Serious discrepancy or demonstrable deterioration in the quality of service expected during the implementation,rolloutandsubsequentmaintenanceprocess OR d) There has been a breach of confidentiality or there is a cyber-security breach of nature detrimental to the interest of ITI Ltd. Decision of ITI Ltd in this connection shall be final and binding on the successful IMSP. e) The Selected IMSP (i) has a winding up order made against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution foritsvoluntarywindingupordissolutionorifitisdissolved.
2	**Termination for insolvency** ITI Ltd may at any time terminate the Contract by giving written notice of **30 days** to the IMSP, if the IMSP becomes bankrupt or otherwise insolvent. In thisevent termination will be without compensation to the IMSP, provided that such termination will not prejudice or affect any right of action or remedy, which has occurredorwillaccruethereaftertotheITI Ltd.
3	**Termination for the convenience of ITI Ltd** The ITI Ltdmay,atanypointduringthecurrencyofthiscontractmayterminate the contract by giving **30 days** advance notice to the IMSPs without assigning whatsoever reason. In this event, termination will be without compensation to the IMSP, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the ITI Ltd.

11 GLOSSARY

S.No	Glossary	
1	APT	Advanced Persistent Threat
2	BGP	Border Gateway Protocol
3	BoM	Bill of Materials
4	BYOD	Bring your Own Device
5	CISA	Certified Information Systems Auditor
6	CISM	Certified information Security Manager
7	CISSP	Certified Information Security Specialist Professional
8	CSRF	Cross Site Request Forgery
9	DC	Data Centre
10	DDoS	Distributed Denial of Service
11	DHCP	Dynamic host Control Protocol
12	DLP	Data loss /leak prevention
13	DNS	Domain Name Server
14	EDR	End point detection and response
15	EPP	End point protection
16	BSD	Bid Security Declaration
17	EOL	End of Life
18	EOS	End of Service
19	EP	End points
20	FTP	File Transfer Protocol
21	GRC	Governance, Risk and Compliance
22	IAM	Identity and Access Management
23	ICMP	Internet Control Message Protocol
24	IDS	Intrusion Detection System
25	IGMP	The Internet Group Management Protocol
26	IMSP	Intended Multi Service Provider /SOC service provider
27	IPS	Intrusion Prevention System
28	ISSAF	Information System Security Assessment Framework
29	MDM	Mobile Device Management
30	MSP	Multi Service Platform
31	NAC	Network Access Control
32	NDA	Non-Disclosure Agreement
33	NG FW	Next Generation Firewall
34	O&M	Operations and Maintenance
35	OEM	Original Equipment Manufacturer
36	OSPF	Open Shortest Path First
37	OSSTMM	Open Source Security Testing Methodology Manual
38	OWASP	Open Web Application Security Project
39	PBG	Performance Bank Guarantee
40	PIM-SM	Protocol-Independent Multicast
41	PTES	Penetration Testing Execution Standard
42	RIP	Routing Information Protocol
43	SIEM	Security Information and Event Management
44	SIP	Session Initiation Protocol
45	SME	Subject matter expert

46	SMTP	Simple Mail Transfer Protocol
47	SNMP	Simple Network Management Protocol
48	SOAR	Security Orchestration, Automation, and Response
49	SOC	Security Operation Centre
50	SoW	Scope of Work
51	TCP	Transmission Control Protocol
52	UAT	User Acceptance Testing
53	UEBA	User entity behaviour analytics
54	VAPT	Vulnerability assessment and penetration testing
55	VOIP	Voice Over IP
56	VPN	Virtual Private Network