REQUEST FOR PROPOSAL

(Bidding Terms & Draft Agreement)

Selection of Agency for

Supply, Installation, Commissioning, Implementation of IT Security Solutions for Air India Ltd.

Tender Ref No: AIR/IT-001/2017

Dated : 08.09.2017

Air India's Tender Reference No: AIR/IT-001/2017

Dated: 08.09.2017

Project Name: Selection of Agency for "Supply, Installation, Commissioning and Implementation of IT Security Solutions for Air India Ltd."

Name of Ministry/ Department: Air India Ltd., New Delhi

SECTION 1:

INSTRUCTIONS TO BIDDERS

Standard

1 Definitions

a) *"Client"* means Air-India Ltd with whom the selected Agency will sign the Agreement for providing IT Security Solutions as per the terms and conditions of contract for supply & services. The Agreement will be signed with the Client.

b) *"Agency"* means any entity or person selected to Supply, Install, commission, implement the IT Security Solutions for the client, by providing the services to the Client in accordance with the terms & conditions of the contract.

c) *"Contract"* means the Agreement at Section 6 signed by the Client and the selected Agency

d) *"Project specific information"* means such part of the RFP which contain conditions specific to the project and assignment.

e) *"Day"* means calendar day.

f) *"Government"* means the Government of India

g) *"Personnel"* means Technical Experts & staff provided by the Selected Agency.

h) *"Proposal"* means the Technical Proposal and the Financial Proposal.

i) *"RFP"* means the Request for Proposal prepared by the Client for the selection of Agency.

j) *"Assignment"* means the work that the Selected Agency shall perform pursuant to the Contract.

k) *"Affiliate"* means any corporation, firm, or other entity that directly or indirectly is controlled by or is under common control of another corporation , firm or entity.

l) *"Terms of Reference (TOR)"* means the conditions included in the RFP including those in Section 5 which explains the objectives, scope of work, activities, tasks to be performed, respective responsibilities of the Client, and the Selected Agency, and expected outcomes and deliverables of the Assignment.

2 Introduction

- Consultancy Development Centre (CDC), an autonomous institution of the Ministry of Science and Technology, Government of India is facilitating the Client - Air India Ltd, at New Delhi, for the selection of the Agency.
- The bidders are invited to submit a proposal in two parts - the Technical part and the financial part sealed separately, as specified in the Data Sheet. Late bids i.e. bids received after the specified date in the data sheet will not be considered. The Proposals submitted will be the basis for signing the Contract with the Selected Agency.
- The Bidders are required to familiarize themselves with the local conditions and take them into account while preparing their proposals. To obtain first-hand information on the

assignment and local conditions, Bidders are advised to attend a pre-bid conference as specified in the Data Sheet. Attending the pre-bid conference is optional. Bidders should contact CDC's representative named in the Data Sheet to obtain additional information on the pre-bid conference.

- Bidders may submit their comments and suggestions on the Terms of Reference including workable suggestions that could improve the quality/ effectiveness of the Assignment/job; and on requirements for Infrastructure including: Technical suggestions for security solutions, etc. during the pre-bid conference.
- Bidders shall bear all costs in connection with the preparation and submission of their proposals, attending pre-bid conference, etc.
- The Client may accept or reject any proposal in its discretion and may ask for any additional information or vary its requirements, add to or amend the terms, procedure and protocol set out in RFP for bonafide reasons. Further Client hereby reserves its right to annul the selection process at any time prior to the Contract award without incurring any liability towards the Tenderers.
- Availability of the RFP Documents -The RFP documents are available to all bidders who are interested in participating in the tender process. The documents can be downloaded from the website of CDC https://www.cdc.org.in/

3 Eligibility of Bidders

- A bidder should be a Company, ***registered under*** the **Indian *Companies Act, 1956/ Revised Companies Act, 2013*** with a minimum of 05 years into Operation having experience in providing complete IT security solutions architecture in any large company with Pan India infrastructure setup.

- Bidder should be an OEM or its authorized Vendor.(Vendor to submit official mail from OEM as Authentication/ Certification)

- Each OEM can bid directly or through maximum Three authorized Vendors .

- Bidder should be having domain expertise as IT security solution architecture provider. Vendor or OEM should have executed Minimum one (01) assignment of similar nature of providing IT security solutions in any Government / PSU organization.

- Bidder should have an cumulative Turnover of not less than Rs. 20 crores for Previous three financial Years (2014-15, 2015-16 & 2016-17)

- Eligibility Criteria elaborated in Data Sheet, Sr. No.8 (Pre-Qualification Criteria). Documentation proof of Company incorporation, Certification /Authentication from OEM should be submitted. Failing which, the proposal will be rejected. Vendor has to provide an Undertaking from the respective OEM.

3A Non-Eligibility

(i) Bids of those Bidders against whom any criminal case is pending before Court of Competent Jurisdiction or who have been convicted by Court of Competent Jurisdiction shall not be considered.

(ii) Bids of those Bidders, who will be found to be involved in theft or in non-payment of Government dues or taxes, will be out rightly rejected and will not be considered for the opening of the Financial Bid.

(iii) The Bids of those Bidders who have been black listed or debarred by Central Government or any Central Government Authority or any State Government or any State Government Authority, shall not be considered.

Explanation: For the purposes of this clause.

(i) If any Director of a Company is convicted by any Court of Competent Jurisdiction, it shall be deemed that such Company, has been convicted.

(ii) If any criminal case is pending against any Director of a Company, before any Court of Competent Jurisdiction, it shall be deemed that criminal case is pending against such Company.

The Bidder should submit a Self Declaration in compliance with its Eligibility. Bidders have an obligation to disclose any situation of Non-Eligibility that impacts their capacity to serve the best interest of The Client , or that may reasonably be perceived as having this effect. Failure to disclose said situations may lead to the disqualification of the bidder or the termination of its Contract.

4 Clarification and Amendment of RFP Documents

- Bidders may request a clarification on any clause of the RFP documents up to the number of days indicated in the Data Sheet before the proposal submission date. Any request for clarification must be sent in writing, or by standard electronic means to the address

indicated in the Data Sheet. CDC will respond in writing, or by standard electronic means and will send written copies of the response (including an explanation of the query) to all Bidders. Should the Client deem it necessary to amend the RFP as a result of a clarification, it shall do so following the procedure below:

- At any time before the submission of Proposals, Client may amend the RFP by issuing an addendum or Corrigendum in writing or by standard electronic means. The addendum/Corrigendum shall be uploaded on website, and will be binding on Bidders. Bidders shall acknowledge receipt of all amendments. To give bidders reasonable time in which to take an amendment into account in their Proposals, The Client may, if the amendment is substantial, extend the deadline for the submission of Proposals.

5 Conflict of Interest

Bidders, and any of their affiliates, shall be considered to have a conflict of interest and shall not be eligible for selection as Agency under any of the circumstances set forth below:

a) Conflicting Assignment/job: A bidder or any of its affiliates shall not be hired/selected for any Assignment/job that, by its nature, may be in conflict with this Assignment/job of the bidder to be executed for the same Client

b) Conflicting Relationships: A bidder that has a business or family relationship with a member of the Client Staff who is directly or indirectly involved in any part of (i) the preparation of the Terms of Reference of the Assignment/job, (ii) the selection process for such Assignment/job, or (iii) supervision of the Contract, may not be awarded a Contract, until and unless the conflict stemming from this relationship has been resolved in a manner acceptable to The Client.

Bidders have an obligation to disclose any situation of actual or potential conflict that impacts their capacity to serve the best interest of The Client , or that may reasonably be perceived as having this effect. Failure to disclose said situations may lead to the disqualification of the bidder or the termination of its Contract.

6 Proposal Validity

The Data Sheet indicates how long Bidders' Proposals must remain valid after the submission date. During this period, bidders shall ensure the availability of Technical staff nominated in the Proposal and also the financial proposal shall remain unchanged. The Client will make its best effort to complete the selection process within this period. Should the need arise; The Client

may request the bidders to extend the validity period of their proposals. Bidders who do not agree, have the right to refuse to extend the validity of their Proposals; under such circumstance The Client shall not consider such proposal for further evaluation.

7 Preparation of Proposals

The Proposal as well as all related correspondence exchanged by the Bidders and The Client shall be written in Hindi or English language, unless specified otherwise. In preparing their Proposal, bidders are expected to examine in detail all the documents comprising the RFP. Material deficiencies in providing the information requested may result in rejection of a Proposal. While preparing the Technical Proposal, Bidders must give particular attention to the following:

- The bidder must have a clear understanding of the proposed solution architecture and the nature of Security installations & Services required.
- While making the proposal, the bidder must ensure that they provide all the information as sought by The Client , failing which the proposal shall be considered as non-responsive. Should submit a Bidder's compliance to Scope of Work for the said project.
- A Bidder may propose for Technical Solution 'A', Solution 'B' or both.

Bidders are required to submit a Technical Proposal (TP) in forms provided in Section-III. The Data sheet in Section-II indicates the formats of the Technical Proposal to be submitted. Submission of wrong type of Technical Proposal will result in the Proposal being deemed non-responsive.

The Technical Proposal shall provide the information indicated in the following paras from (a) to (m) using the attached Standard Bid Response Forms (Section 3)

a) **Form Tech 1-A:** Letter of Proposal submission

b) **Form Tech 1-B** : Authorization certificate for Representation

c) **Form Tech 1 C**: Bidder's Profile & Bidder's Compliance (Eligibility) & Technical Solutions (General Requirements), along with supporting documents

d) **Form Tech-2** : A brief description of the bidder's organization will be provided in Form Tech-2. In the same Form, the bidder will provide details of experience of assignments, which are similar to the proposed assignment/ job as per the terms of reference. For each activity, the bidder should clearly indicate the role and level of involvement in the same. Information should be provided only for those Assignment/jobs for which the Bidder was legally contracted as an independent entity or as one of the lead member

within a joint venture/consortium. Assignment/jobs completed by individual technical staff working privately or through other firms cannot be claimed as the experience of the Bidder, but can be claimed by the Technical staff themselves in their CVs. Bidders should be prepared to substantiate the claimed experience along with the proposal and must submit letter of award /copy of contract for all the assignments mentioned in the proposal.

e) **Form Tech-3:** A description of the Execution plan for performing the Assignment/job covering the following subjects: Understanding the Requirement of Project, Proposed Security Solution framework, work execution plan , and Technical Manpower schedule is to be finalized as provided under Form TECH-3 of Section 3.

f) **Form Tech 4:** The execution plan should be consistent with the Work/ Implementation Schedule (Form TECH-4 of Section 3) which will show in the form of a bar chart the timing proposed for each activity.

g) **Form Tech-5:** The list of the proposed Technical team by area of expertise, the position that would be assigned to each team member and their tasks is to be provided in Form TECH-5 of Section 3.

h) **Form Tech-**6: Declaration - Bidder's Compliance – Technical Solutions (Solution 'A'/solution 'B')

i) **Form Tech-7** : Self Declaration by Bidder – Scope of Work

j) **Form Tech-8:** Self Declaration by Bidder – Non Eligibility

k) **Form Tech-9:** OEM Certificate, OE Manufacturers Authorisation Letter (To be submitted on OEM letterhead , also OEM to send the Authorisation Letter directly to Air India at Email nirmal.sahai@airindia.in

l) Training: A detailed description of the proposed Work execution plan for training needs to be given, if the Data sheet specifies training as a specific component of the Assignment/job.

The Technical Proposal shall not include any financial information. A Technical Proposal containing financial information may be declared non-responsive.

Financial Proposal*:* The Financial Proposal shall be prepared using the attached Standard Forms (Section 4). The financial proposal shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.

The financial proposal shall be in the form of Lump sum fee for the each proposed solution ('Solution 'A' , Solution 'B'.)

8 Taxes

For the purpose of evaluation, the financial proposal should be in the form of lump-sum fee (exclusive of taxes) for the proposed solution. All taxes (GST) and other impositions as applicable in India, will be additions and shall not be included in the Financial Proposal

9 Currency

Bidders shall express the price of their Assignment/job in Indian Rupees (INR) only.

10 Earnest Money Deposit (EMD)/ Bid Security

1. Bidders shall submit, along with their Bids, an EMD/ Bid Security (amount specified in the Data Sheet table), in the form of a Demand Draft drawn, in favour of Air India Ltd., payable at New Delhi **OR** in the Form of Irrevocable and unconditional Bank Guarantee in favour of Air india Ltd (As per Format given), from State Bank of India or any Nationalised or scheduled Indian bank, approved by the Reserve Bank of India and valid for six months from the last date of the bid submission. Format for Bank Gurantee is attached.
2. The EMD i.e. bid security is interest free.
3. The bid security/EMD, for the amount mentioned above, of successful bidder would be returned upon submission of Performance Bank Guarantee. The bid security of all unsuccessful bidders will be returned by Air India Ltd at the earliest either after expiry of the final bid validity or within 30 day after award of the contract to the successful bidder
4. The bid submitted without bid security/EMD, mentioned above, will be liable for rejection without providing any further opportunity to the bidder concerned.
5. The bidder shall extend the validity of the offer on request by Air India Ltd.
6. The bid security/EMD may be forfeited:
    - If a bidder withdraws its bid during the period of bid validity
    - In case of a successful bidder, if the bidder fails to sign the agreement in accordance with terms and conditions

11 Late Bids

Bids received after the due date and time as specified in the Data Sheet (including the extended period if any) for any reason whatsoever, shall not be entertained.

12 Submission, Receipt, and Opening of Proposal

a) The original proposal, both Technical Proposal and Financial Proposal shall contain no inter lineation or overwriting, except as necessary to correct errors made by the Bidders themselves. The person who signed the proposal must initial such corrections. Submission letters for both Technical Proposal and Financial Proposals should respectively be in the format of TECH-1-A of Section 3, and FIN-1 of Section 4.

b) An authorized representative of the bidder shall initial all pages of the original Technical Proposal and Financial Proposal. The authorization shall be in the form of a written power of attorney accompanying the Proposal or in any other form demonstrating that the representative has been dully authorized to sign. The signed Technical Proposal and Financial Proposals shall be marked "ORIGINAL".

c) The original and 1 copy of the Technical Proposal along with 1 Soft copy, shall be placed in a sealed envelope clearly marked "TECHNICAL PROPOSAL- Air India – IT Security Solutions" Similarly, the original Financial Proposal along with 1 in soft copy, shall be placed in a sealed envelope clearly marked "FINANCIAL PROPOSAL- Air India – IT Security Solutions (Not to be opened with the Technical Proposal)". The envelopes containing the Technical Proposals, Financial Proposals, shall be placed in an outer envelope and sealed. This outer envelope shall bear the submission address, reference number and be clearly marked "BID for Air India– IT SECURITY SOLUTIONS---DO NOT OPEN, BEFORE [insert the time and date of the opening indicated in the Data sheet]". CDC shall not be responsible for misplacement, loss or premature opening if the outer envelope is not sealed and/or marked as stipulated.

d) If the Financial Proposal is not submitted in a separate sealed envelope duly marked as indicated above, this will constitute grounds for declaring the Proposal non-responsive.

e) The Proposals must be sent to the address/addresses indicated in the Data sheet and received by CDC no later than the time and the date indicated in the Data sheet, or any extension to this date. Any proposal received by CDC after the deadline for submission shall be returned unopened.

f) Bidders must submit TWO Hard copies of Technical Proposals (ONE Original + ONE copy) along with ONE Soft copy on a non-rewritable CD. The Words "Technical Proposal- Air India – IT Security Solutions" must be written in indelible link on the CD.

g) Among the two copies the ORIGINAL' document must be clearly identified and marked as "ORIGINAL" on the top right corner of the first page. The other must be marked as "COPY"

on the top right corner of the first page. In case of discrepancy between the hard and soft copies, the hard copy (original) will taken as final.

h) Bidders must submit only ONE Hard copy of Financial Proposal along with ONE Soft copy on a non-rewritable CD. In the CD, the bidder must submit the soft copy of the commercial bid in protected Excel sheets. Incase of discrepancy between the soft and hard copies, the hard copy (original) will be taken as final. The Words "Financial Proposal- Air India IT Security Solutions" must be written in indelible link on the CD.

i) The Hard copy must be signed by the authorized signatory on all the pages before being put along with CD in the envelope. Unsigned Hard copy of the Financial proposal will lead to rejection of the bid.

Note:

- It is important that Technical and Commercial Proposals are properly indexed with all pages sequentially numbered either at the top or at the bottom right corner of each page
- Air India will not accept delivery of proposal in any manner other than that specified in this volume. Proposal delivered in any other manner shall be treated as defective, invalid and rejected.

13 Proposal Evaluation

From the time the Proposals are opened to the time the Letter of Intent(LOI) is issued to successful Bidder, the Bidders should not contact CDC on any matter related to its Technical Proposal and/or Financial Proposal. Any effort by Bidders to influence The client in the examination, evaluation, ranking of Proposals, and recommendation for award of Contract may result in the rejection of the Bidders' Proposal. A Selection Committee constituted will carry out the entire evaluation process.

a) ***Evaluation of Technical Proposals:*** The Selection Committee while evaluating the Technical Proposals shall have no access to the Financial Proposals until the technical evaluation is concluded and the competent authority accepts the recommendation.

- Proposals, which are not supported by adequate proof of the Signatory's Authority, will not be evaluated.

- The Selection Committee will evaluate the Technical Proposals only for those Bidders who satisfy the pre-qualification criteria as referred in the Data Sheet. The Technical Proposals will be evaluated based on the documentary evidence submitted by the Bidder. Each proposal will be evaluated based on the Qualification criteria, Total compliance to the

solution requirements. A Proposal shall be rejected at this stage if it does not respond to important aspects of the RFP, and particularly the Terms of Reference , it fails to Comply with the General requirements, and Technical solutions requirements. The Technical Proposals which are incomplete shall not be evaluated.

- The Proposal shall be rejected if Bidder does not fulfill the eligibility criteria or the validity period of the proposal is less than 120 days.
- *Clarification/additional information may be sought during scrutiny*

b) ***Opening & Evaluation of the Financial Proposals:***

After the technical evaluation is completed, the qualified Bidders shall be informed in writing about the time and location for opening the Financial Proposals. Bidder's attendance at the opening of Financial Proposals is optional but it shall be recorded and signed by all present.

- Financial Proposals shall be opened publicly in the presence of the Bidder's representatives who choose to attend. The Financial Proposal of the Technically Qualified Bidders i.e. who comply with the General and Technical solutions specifications, will then be inspected to confirm that they have remained sealed and unopened. The Financial Proposals of Technically qualified bidders shall then be opened, and their quotes in the form of Lump sum fee for proposed security solution will be read aloud and recorded.

The proposal with the LOWEST LUMP SUM FEE (in RS) (excluding taxes) for each solution, as given in FORM FIN 2 shall be ranked as L-1 for respective solution and will be considered for award of Contract.

14 Award of Contract

The Client shall issue a Letter of Intent(LOI) to the Selected agency. The Selected agency will sign the Agreement after fulfilling all the formalities/pre-conditions mentioned in the standard form of contract in Section-6, within 15 days of issuance of the LOI. The Selected agency is expected to commence the Assignment/job from such date as mentioned in the Agreement.

15 Confidentiality

Information relating to evaluation of Proposals and recommendations concerning awards shall not be disclosed to the Bidders who submitted the Proposals or to other persons not officially

concerned with the process, until the publication of the award of Contract. The effort by Bidder to seek confidential information related to the process will result in the rejection of its Proposal.

16 Bid Validity Period

Bid submitted by Bidder shall be valid for the period of 120 days from the last date of submission of Bid.

SECTION 2:

DATA SHEET

DATA SHEET

1.	Name of the client:	**Air India Ltd**
2.	Tender Reference No	**Tender Reference No :** AIR/IT-001/2017
3.	Release of Request for Proposal	Date: 08.09.2017
4.	Place of availability of Tender Documents (RFPs)	Website of Consultancy Development Centre (CDC) www.cdc.org.in/
5.	Place of submission of Response of Tender	Consultancy Development Centre (CDC) 2nd Floor, Core-4B, India Habitat Centre, Lodhi Road, New Delhi-110003 Tel: 011- 24603425, 24602601 Fax: 011-24602602
6.	Bid Security/ EMD requested:	The Bidder will be required to submit a Bid Security/ Earnest Money Deposit (EMD) in the form of an irrevocable and unconditional Bank Gurantee valid for period of 6 months from the date of Bid submission **OR** DD for in favour of **Air India Ltd, New Delhi** • **Rs. 4,00,000/- (Four Lakhs Rupees) for Solution "A"** • **Rs.8,00,000 (Eight Lakhs Rupees) for Solution "B"**
7.	Documents part of RFP:	Section 1 - Instructions to Bidders Section 2 – Data Sheet Section 3 - Technical Proposal - Standard Forms Section 4 - Financial Proposal - Standard Forms Section 5 - Terms of Reference Section 6- Standard Form of Contract
8.	Pre-Qualification Criteria	(a) The bidder (Company) must be an OEM or its Authorized Vendor and should be a Company *registered under* the Indian *Companies Act, 1956/ Revised Companies Act, 2013.* with a minimum of five (05) years into Operation, having

		relevant experience in providing IT security solutions. (Incorporation/ Registration Certificate required). (b) The bidder must be an OEM or a Vendor of any OEM. Vendor to submit official mail from OEM as Authentication/ Certification) (c) The **bidder (Company)/OEM** having expertise as solution provider for IT Security Solutions (supply, installation, commissioning, implementation)**. It** should **have a Past Experience** of Minimum **one (01) assignment** of similar nature of providing IT security solutions in Government or and Public Sector (Copy of work order/ Contract of the mentioned assignment/proof of facility required) (d) The bidder must have a minimum and cumulative Turnover of not less than Rs. 20 crores for Previous three financial Years (2014-15, 2015-16 & 2016-17) **Financial years** (2014-15, 2015-16 & 2016-17) (Audited Accounts/Certificate from Auditors required) Documentary proof with respect to the above criteria is essential without which the proposal will be rejected. Technical and Financial evaluation will be done only for the bidders satisfying the above criteria.
9.	Technical and Financial Proposals requested:	Yes
	Name, objectives, and description of the assignment:	As detailed in TOR (Section 5)
10.	Pre-bid Meeting will be held on:	Date: **19th September, 2017** Time: **1100 hrs** Venue: Consultancy Development Centre (CDC) Core-4B, 2nd Floor, India Habitat Centre, Lodhi Road, New Delhi-110003 Tel: 011- 24603425, 24602601 Fax: 011-24602602

11.	Contact details for pre-bid Meeting:	**Mr. S. K. Sharma** Head (Business Development) Consultancy Development Centre Core 4B 2nd Floor, India Habitat Centre, Lodhi Road New Delhi – 110 003 Tel: 91 11 24603425; 24602601 Fax: 91 11 24602602 Email: sksharma@cdc.org.in *Bidders to confirm their participation in the pre-bid conference to the above person.*
12.	Email address to send Pre-Bid Queries	sksharma@cdc.org.in
13.	Last date for submission of written queries by Bidders	Till Pre-Bid Meeting
14.	Date of Release of Pre-Bid Clarifications	Within 4 working days after Pre-Bid Meeting
15.	Address for requesting any clarifications is:	**Mr. S. K. Sharma** Head (Business Development) Consultancy Development Centre Core 4B 2nd Floor, India Habitat Centre, Lodhi Road New Delhi – 110 003 Tel: 91 11 24603425; 24602601 Fax: 91 11 24602602 Email: sksharma@cdc.org.in
16.	The Client envisages the need for continuity for downstream work:	Yes
17.	Clauses on fraud and corruption in the Agreement:	Clause 6.2.9 of Section 6
18.	Language(s) of the submitted proposals:	**English** The Contract to be signed with the Selected Agency shall be written in the English language, which shall be the language that shall govern the contractual relations between The Client and the Selected Agency.

19.	Reports that are part of the assignment must be written in the language	English
20.	Training is a specific component of this assignment:	Yes
21.	Taxes: [Specify Bidder's liability:]:	As per clause no 5.4.8
22.	Bidder to state cost in the national currency:	Indian Rupees
23.	Bidder to submit Bidder's Compliance to the Scope of Work/services as per TOR	Yes
24.	Validity of Bid Propsosal	Proposals must remain valid for one hundred twenty (120 days after the last day of bid submission
25.	Address to submit Techno-Commercial Bid	Head (Business Development) Consultancy Development Centre Core 4B 2nd Floor, India Habitat Centre, Lodhi Road New Delhi – 110 003 Tel: 91 11 24603425; 24602601 Fax: 91 11 24602602
26.	Proposals submission date:	Not later than the following date and time: Date: **3rd October, 2017** Before **1400 hrs**
27.	Address for correspondence:	**Mr. S. K. Sharma** Head (Business Development) Consultancy Development Centre Core 4B 2nd Floor, India Habitat Centre, Lodhi Road New Delhi – 110 003 Tel: 91 11 24603425; 24602601 Fax: 91 11 24602602 Email: sksharma@cdc.org.in
28.	Commencement of assignment:	On the date and at the location specified in the LOI/Agreement
29.	Opening of Technical Bids	3rd October, 2017 at **1430 hrs**

Section 3:

TECHNICAL PROPOSAL - STANDARD FORMS

TECH FORMS	FORM NAME	X / √	Mention list of all supporting documents attached (if any)
TECH-1-A	Letter of Proposal Submission		
TECH-1-B	Authorization Certificate for Representation		
TECH-1-C	Bidder's Profile & Compliance Sheets		
TECH-2	Company's Organization and Experience		
	(A). Company's Organization		
	(B). Company's Experience		
TECH-3	Description of the Job requirements, The Proposed Solution and Work Execution Plan for Performing the Assignment/ Job		
TECH-4	Work /Implementation Schedule		
TECH-5	Team Composition and Task Assignments/ Jobs		
	(A). Summary of Project Team / Team Composition		
TECH-6	Bidder's Compliance- Technical Solutions		
TECH-7	Self Declaration by Bidder – Scope of Work		
TECH-8	Self Declaration by Bidder – Non Eligibility		
TECH-9	OEM Authorisation Letter		

Form Tech 1A: Letter of Proposal Submission

[To be submitted on the Letterhead of the Bidder]

[*Location, Date*]

To: [*Name and address of The Client*]

ED-IT (O)
Air India Ltd.
Airlines House, 113, Gurudwara Rakabganj Road
New Delhi-110001

Dear Sir

We, the undersigned, offer to provide the complete solutions for **Supply, Installation, Commissioning and Implementation of IT Security Solutions to Air India Ltd**, in accordance with your Request for Proposal dated [*Insert Date*].

We are hereby submitting our Proposal, which includes this Technical Proposal, and also the Financial Proposal sealed under a separate envelope.

We undertake the total responsibility for performance of the Contract, if awarded to us.

We hereby declare that all the information and statements made in this Proposal are true and accept that any misrepresentation contained in it may lead to our disqualification.

We understand that **Air India Ltd.** is not bound to accept any Proposal it receives.

We remain,

Yours faithfully,
*Authorized Signatory [*In full and Designation*]:

Name and Title of Signatory:
Name of Bidder:
Address:
Seal/stamp of Bidder:
* **NB:** ***Authorization in form of power of Attorney is required on a non-judicial Stamp Paper.***

Form Tech 1B: Bidder's Authorization Certificate

[To be submitted on the Letterhead of the Bidder]

[*Location, Date*]

To,

ED-IT (O)
Air India Ltd.
Airlines House, 113, Gurudwara Rakabganj Road
New Delhi-110001

<*Bidder's Name*> _____, <*Designation*> _____ is hereby authorized to sign relevant documents on behalf of the company in dealing with Proposal of reference <*Reference No. & Date*> _____. He is also authorized to attend meetings and submit technical & financial information as may be required by you in the course of processing above said proposal.

Thanking you,

Authorized Signatory

_____

<*Company Name*>

Seal/stamp of Bidder:

Form Tech 1C: Bidder Details and Compliance Sheet (Eligibility & Technical Solutions-General Requirement)

1	**Company Information**	**Details**
1.1	Company Name	
1.2	Details Address Phone number Email Fax Website	
1.3	Contact Person: ***Chief Executive/ Head of Operations*** Name Designation Mobile Number Email Fax	
1.4	Contact Person: ***Project Leader*** Name Designation Mobile Number Email Fax	
1.5	Status of the Company (Public Ltd/ Pvt Ltd.) :	
1.6	Details of Incorporation of the Company	Date: Ref:
1.7	Permanent Account Number (PAN)	
1.8	Valid GST registration No.	

COMPLIANCE SHEET – ELIGIBILITY- PRE-QUALIFICATION

[To be submitted on letter head of bidder]

2	Pre-Qualification Criteria and Supporting Documents	Compliance X / √
2.1	Is your organization registered and has been in operation for at least five years in area of providing IT security solutions?	
	Attach Incorporation/ Registration Certificate or any other supporting document.	
2.1 (a)	Is your organization functioning as OEM or its VENDOR Attach the supporting documents of OEM or Vendor certificate. Vendor to submit official mail from OEM as Authentication/Certification	
2.2	The bidder must have a minimum and cumulative Turnover of not less than Rs. 20 crores for Previous three financial Years (2014-15, 2015-16	
	Attach Audited Accounts/Certificate from Auditors or any other supporting document.	
2.3	Do you have the Technical Manpower for undertaking IT security solutions assignments	
	Attach Summary of Project Team/ Team Composition of Technical Manpower (Currently working with the bidder)	
2.4	Do you have an experience of minimum one (01) assignment for Providing IT Security solutions Architecture and services to Government or and Public Sector?	
	Attach Copy of work order, Contract for each of the mentioned assignments or any other supporting document.	
2.8	Have you submitted the Bidder's compliance for the subject Scope of Work	

Documentary proof is essential without which the proposal may be rejected. Technical and Financial evaluation will be done only for the bidders satisfying the above criteria.

Authorized Signatory

_____

<*Company Name*>

Seal/stamp of Bidder:
Date:

COMPLIANCE SHEET – GENERAL REQUIREMENTS (with Supporting Documents)

[To be submitted on letter head]

3	**Technical Solutions – Broad General Requirements for Security Architecture Project**	**Compliance X / √**
3.1	OEM should attain ISO 27001 Certification as well as should attain ISO for its Support Services	
3.2	OEM should have support Centre in India.	
3.3	The Proposed solution must cover following :– ➢ Next Generation Security Architecture-UTM (Firewall with IPS) ➢ Anti-APT Solution with Secure Web Gateway Solution	
3.4	Proposed Solution must have the overall capabilities of scanning various inbound and outbound traffic like Web, File, Network etc. for Monitoring, Detection, cleaning, Analysis and Blocking of APTs and other malicious content	
3.5	Proposed Solution must provide for a dedicated on-premise full-fledged sandboxing analysis solution.	
3.6	Proposed Anti-APT solution should work as a single system for Network, on-premise endpoints and off-premise endpoints with full correlation capabilities	
3.7	Proposed OEMs/ Vendor may use multiple devices/Appliances to fully comply for required functions for every proposed technology	
3.8	Proposed OEMs for Security solution must comply to at least one of the following two requirements a. Proposed OEM must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Next Generation Firewall with IPS(UTM) published by Gartner or in Latest NSS Lab Report. b. Proposed OEM for Anti-APT must have scored equal or more than 98.5% 'Security Effectiveness' in latest NSS Breach Detection Systems (BDS) report	
3.9	Bidder must ensure that the Proposed Solution is 100% compliant to all the requirements mentioned in General Requirements and Individual Solutions' Technical Requirements and also provide the proper documentation/proof to support the compliance. Any deviation, Partial Compliance or Non-Compliance will lead to rejection of the bid.	
3.10	Proposed OEM must have it's own dedicated security research team and also a cloud based infrastructure for providing real-time security intelligence. Proposed OEM should have their support in India and support cases should be handled directly from the OEM.	
3.11	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.	
3.12	Bidder should quote mentioning manufacturer's warranty, Subscriptions and part number and provide minimum 5 (Five) years full replacement warranty from the date of successful commissioning.	

Documentary proof is essential without which the proposal may be rejected. Technical and Financial evaluation will be done only for the bidders satisfying the above criteria.

Authorized Signatory

_____

<*Company Name*>

Seal/stamp of Bidder:
Date:

Form Tech 2: Company's Organization and Experience

(A) - Company's Organization

[Provide here a brief description of the background and organization of your Company/entity for this Assignment/job. The brief description should include ownership details, date and place of incorporation of the Company, objectives of the Company etc.

Years	*2014-15*	*2015-16*	*2016-17*
Turnover (INR)			

Attach Incorporation/ Registration Certificate, Audited Account Sheets/ P&L Sheets.

(B) - Company's Experience

Using the format below, provide information on each Assignment/job for which bidder, had legally Contracted as a *corporate entity* within an association, for carrying out Assignment/job similar to the ones requested under this Assignment/job (exact assignment / job details may be submitted) within India.

Company's Name: _____

Assignment Name:		Country: India
Location within Country:		Key professional staff Provided by Your Firm / entity(profiles):
Name of Client:		No. of Staff
Address:		Duration of assignment:
Start Date (Month/Year):	Completion Date (Month/Year):	Approx. Value of Services (in Current Rs):

Name of Associated Bidders, if any:		No. of Months of Key Technical/ professional staff, provided by Associated Bidders:
Name of Senior Staff (Project Director/Coordinator, Team Leader) involved and functions performed:		
Narrative Description of Project:		
Description of Actual Services Provided by Your Staff:		

Note: *Please provide documentary evidence i.e. copy of work order, Contract for each of above mentioned assignment. The experience shall not be considered for evaluation, if such requisite support documents are not provided.*

Authorized Signatory

_____

<*Company Name*>

Seal/stamp of Bidder:

Form Tech 3: Description of Proposed Solution, Technical Approach, and Work Execution Plan for Performing the Assignment/ Job

[Understanding of Requirement of Project, Proposed Solution and work Execution plan are key components of the Technical Proposal].

You are suggested to present your Technical Proposal divided into the following three chapters:

a). Technical Approach/ Understanding of the SOW,
b). Proposed Solution and its adherence to SOW
c). Work Execution Plan, and Time Schedule
d). Technical Team

a). **Technical Approach / Understanding of the SOW** : In this you should explain your understanding of the objectives of the Assignment/job, its purpose, scope and your technical plan for carrying out the activities and for providing the required architecture, implementation, testing, & training for the Assignment/job for obtaining the expected output, and the degree of detail of such output. You should highlight the problems being addressed and their importance, and explain the technical approach you would adopt to address them.

b). **Proposed Solution Architecture** : In this you should give comprehensive technical details of The Solution Proposed by you with adherence to SOW, explain the solutions you propose to adopt and highlight the need, compatibility and relevance in selecting the specific solution for the Client's requirement.

c). **Work Execution Plan**: The Bidder should propose and justify the main activities of the Assignment/job (Supply, installation, commissioning, implementation, testing & training of Security solutions architecture, their technical outputs, activities, sequencing, phasing and interrelations, milestones (including interim approvals by The Client, if any), and delivery dates of the deliverables. The proposed work plan should be consistent with the technical approach showing understanding of the TOR and ability to translate them into a feasible working plan. A list of the final deliverables should be included here. The work plan should be consistent with the Work Schedule of Form TECH-6.

d). **Technical Manpower** : The Bidder should propose composition of the Project team. Bidder should list the main disciplines of the Assignment/job, the key expert responsible, and proposed technical team.

Form Tech 4: Work Schedule

Implementation Schedule –Indicative

S. **No.**	**Activity**[1]	**Months**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**N**
1									
2									
3									
4									
5									
N									

[1]*Indicate all main activities of the assignment*

Form Tech 5: Team Composition

Summary of Project Team / Team Composition

Technical Team

S. No	Name	Position	Role Description	Nature of Tasks which will be Performed by him/ her	CV Attached (Yes/No)

Form Tech 6: BIDDER'S COMPLIANCE SHEET –TECHNICAL SOLUTIONS (with supporting Documents)

[To be submitted on the Letterhead of OEM]

Technical Specifications – Proposed Solution 'A' / Proposed Solution 'B'

SOLUTION 'A' : Next Generation Security Architecture-UTM (Firewall with IPS)

Solution's Technical Requirements

S. No	Functional Requirement	Bidder's Compliance	Remarks
1	**Basic Criteria**		
a)	OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services		
b)	OEM should have support Centre in India.		
c)	Appliance should have ICSA certification for Firewall.		
d)	The proposed solution should support High Availability Active-Active mode		
e)	Appliance Throughput		
f)	Firewall throughput of 100,000 Gbps		
g)	Minimum 17 Gbps of Antivirus Throughput		
h)	Minimum 30,000,000 Concurrent sessions		
i)	Minimum 22 Gbps of IPS throughput		
j)	Minimum 300,000 New Sessions/second		
k)	Minimum 11 Gbps of IPsec VPN throughput		
l)	Minimum of 5000 IPsec Site to Site tunnel support and 700 SSL VPN user support. License for the same should be included in the BOM.		
m)	Minimum of 8 x GBE Interfaces and 2 x GE SFP and 4 x 10 GE SFPwith expansion slot to accommodate more ports if required.		
n)	Should have minimum of 500 GB SSD drives in RAID		
2	**General Features**		
a)	Should be appliance based and rack mountable		
b)	Identity based Firewall		
c)	Intrusion Prevention System		
d)	Gateway Anti-virus		
e)	Gateway Anti-spam with DLP functionality		
f)	Web Content & Application Filtering		
g)	Web Application Firewall		
h)	Bandwidth Management		
i)	Inbuilt-on Appliance Reporting		
j)	High Availability (Active-Active & Active-Passive)		
k)	Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round		

	Robin Balance, Server Load Balancing.		
l)	Support for user authentication over SMS.		
m)	Country Based Blocking, FQDN support and should support MIX mode deployment		
n)	4 Eye Authentication feature for data integrity.		
o)	Should have an integrated wireless controller and should be able to manage multiple wireless access points centrally from web admin console.		
3	**Gateway Antivirus, Anti-Spyware and Anti-Spam**		
	Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management, DLP engine with automatic scanning of emails and attachments for sensitive data		
4	**Web and Application Filtering:**		
	URL, Keyword, File type block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL, block P2P application, anonymous proxies, Customized block on group basis. Minimum of 89 categories with more than 160 million URLS supported. 2000+ application support categorized into Characteristics, Technology, Category and Risk Level.		
	The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS.		
5	**Wireless Security and Control:**		
	Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported Aps		
6	**Security Features**		
	Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection		
7	**Web Application Firewall (WAF):**		
	Should have an option of WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.		

8	**Advance Threat Protection:**		
	Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)		
9	**VPN:**		
	IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.		
10	**Load Balance:**		
	For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.		
11	**Bandwidth Management:**		
	Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.		
12	**Monitoring and Reporting System:**		
a)	· Includes Integrated Web Based reporting,, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1200+ drilled down reports on the appliance.		
b)	· Should provide User Threat Quotient (UTQ) report for actionable security intelligence, helping Administrators identify risky users with ease within the organization's network.		
c)	License for UTM (Unified Threat Management)		
d)	· One Year round the clock support for Gate Way Antivirus, spyware, Anti-Spam, WAF, content and application filtering. IPS, reporting and support, Upgrades.		
e)	· License period will be counted after activation.		

Supporting Documentary proof is essential without which the proposal may be rejected. Technical and Financial evaluation will be done for the bidders satisfying the above criteria.

Authorised Signatures

Agency/Supplier's Name:

Name & Designation

With seal/stamp

Date:
Place:

SOLUTION 'B' - ON-PREMISE ANTI-APT SOLUTION WITH SECURE WEB GATEWAY

[To be submitted on the Letterhead of OEM]

1	**Anti-APT Solution**		
Sr.No	**Functional Requirement**	**Bidder's Compliance**	**Remarks**
1	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.		
2	The proposed solution should support the native CEF,LEEF format for SIEM log integration		
3	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects.		
4	Solution must be custom built Anti-APT solution and must not have network perimeter security component part devices like firewall and IDS/IPS		
5	Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network		
7	Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance threats.		
8	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.		
9	Solution should provide risk based alerts or logs to help prioritize remediation effort.		
10	Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.		
11	*The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox.*		
12	The proposed solution should use customizable OS sandboxes for detecting zeroday malwares, This should not be a CPU or chip based function.		
13	Solution should have ability to interrupt malicious communication.		
14	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth.		
15	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.		
16	Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.		
17	Solution deployment should cause limited interruption to the current network environment.		

18	The proposed solution should able to work with the existing technologies for advance threat protection through web protocol.		
19	The proposed solution should be able to detect lateral movement (East-West) of the attacker without the need of installing agents on endpoint/server machines.		
20	The proposed solution should support at least 100+ protocols for inspection.		
21	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.		
22	The Proposed solution should be able to support up to 5 network segments on a single appliance.		
23	The proposed solution should be able to identify and help understand the severity and stage of each attack.		
24	The proposed solution should have built in capabilities to add exceptions for detections.		
25	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.		
26	The proposed solution should support Multiple protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device		
27	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.		
28	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.		
29	The Proposed solution must provide a web service interface/API for customer to customize integration.		
30	The Proposed solution must have capabilities to correlate the detections on the device itself.		
31	The Proposed solution should support remote packet capturing for Kerberos traffic from the remote location for analysis.		
32	The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session.		
33	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.		
34	The proposed solution should integrate with web security solution to block threats coming via HTTP, HTTPs and FTP		
35	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, ransomeware protection, C&C detection, ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero		

	day malwares by sharing Indicators of Compromise.		
36	The proposed solution should be able to run atleast 60 parallel sandboxes for analysis of payload and on-premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis		
37	Endpoints should be able to submit suspicious files directly to the on-premise customized sandbox solution without the need to be intercepted by network based security solutions.		
38	Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008 & 2012)		
39	The solution should allow administrator to categorize files as safe based on Hash values (MD5) and proposed solution should be able to provide customizable sandbox to match customer's endpoint environments.		
40	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection.		
41	Solution must have the capability to analyze large files and must be able to support more than 40MB file size.		
42	The Proposed solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing. This requirement should be based on virtual execution and should not be a Hardware or chip based function.		
43	The proposed solution should have capability to scale out the detection when the bandwidth increases in future.		
44	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp		
45	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files and proposed solution should support atleast 5 Ethernet Interfaces.		
46	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing and solution should have capabilities to scan inside password protected Archive and should have capabilities to detect Malwares and Spywares on windows and non windows platforms.		
47	The proposed solution should have option to configure unrestricted internet for sandboxes and proposed solution must have capabilities to detect Mac, Linux and mobile malwares.		
48	The Proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..)		
49	The Proposed solution should be able to Identify suspicious embedded object in document file like OLE & Macro extraction, Shell code & exploit matching		

50	The Proposed solution should have option to share Indicators of compromise for mitigation and clean up with AV endpoint and Web gateway to block threat at web gateway level. Anti-APT solution should share intelligence with endpoint and security web gateway solution, similarly endpoint and security web gateway should submit files to anti-APT solution for analysis and all three solution should manage through single management console.		
52	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.		
53	The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.		
54	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.		
55	The proposed solution shall support Remote administration using SSH/HTTPS and proposed solution shall support CLI, GUI/Web based Administration Console		

Secure Web Gateway and Content Filtering solution

2	**Secure Web Gateway and Content Filtering solution**		
Sr.No	**Functional Requirement**	**Bidder's Compliance**	**Remarks**
1	Should be an integrated solution to provide HTTP/FTP/HTTPS/IM Antivirus, Content Filtering, Categorized URL Filtering and Web Proxy Caching		
2	Should Software appliance on bare metal hardware. As a virtual machine with Vmware ESX/ESXi and Microsoft HyperV & Should be Embedded OS - hardened and performance tumed, provided by OEM, low maintenance with CLI interface and Should be Software Virtual Appliance		
3	Should support Forward Proxy, Reverse Proxy, Transparent, Bridge Mode, WCCP, ICAP		
4	Should Support external Load balancer as High Availability option and HA in Transparent Bridge Mode		
5	WRS Page Analysis (Content Scan), WRS/URL Feedback Option, HTTPS Scanning, Should support Automatic URL Updates, Proactive Web Threats (real-time)		
6	Should support atlest 30 Languages and should support User-Defined Categories with Dynamic Classification, Real-time Page Analysis (content scan)		
7	Should support Customized HTML Block/Warning Page and Should Support Global and Per Policy Whitelisting with URL Blacklisting		
8	Should have Proprietary AV Scanning technology from same OEM and Application Control to identify popular web applications & allow administrators to create policies to monitor or control them.		

9	General Pattern String Match, Web Site Match, URL Key Word Match, Per Policy White List, Approved Lists - URL, Approved Lists - Filename, File Object-type Filtering - File type blocking with MIME Content Type, True File Type Matching and Blocking		
10	Quota Filtering, Thumbnail / Image Blocking, Compressed File Filtering - Should Block, Pass, Quarantine		
11	Should have following FTP Scanning functionality, Reverse FTP Proxy, Passive FTP Support, Active FTP Support, Should Support IP Address based FTP Access Control, FTP Port Filtering		
12	Should have following HTTPS Scanning functionality and Decrypt HTTPS traffic from selected Web categories		
13	Should have following AV and Spyware scanning capability, Cloud and Signature based Antivirus, Cloud and Signature based Spyware, Phishing - PhishTrap and Cloud-based Web Reputation, Pharming - Web Reputation and URL Filtering, Bots, Cloud and Signature based Keylogging		
14	Heuristic Scanning, Signature Matching, Customizable File Filters for Scanning, Large file handling, Compressed File Support - with block, bypass and quarantine modes		
15	Quarantine File Support, Real-time Page Analysis (content scan), Automatic Signature Updates, Incremental Updates, Rollback Updates, Solution should be able to detect and block Brute Force Attacks against Passwords, Manual and Automated Updates, Botnet Detection Technology		
16	Solution should have Web cache acceleration with File Cache, Dynamic Object Cache and Static Object Cache and Selective Category Logging, full URL Logging		
17	The Solution should have captive portal page to authenticate the users instead of the traditional browser popup that asks for the username and password, The captive portal page should be fully customizable by the customer to reflect their needs.		
18	If there is no LDAP account or the Web Gateway Security couldn't auto detect the user's UserID from LDAP, the web Gateway Solution should present the Captive Portal authentication page for login credential		
19	Solution should support Network Packet Capturing so Administrators can analyze traffic with a feature that allows packet captures for selected interfaces or a single interface.		
20	Should be Virtual/Software appliance solution and support following Server System, VMware ESX v4.0/4.1 and Hyper-V Support		
21	Should integrate with Anti-APT solution to receive IOC's and both solution should have central management console for central visibility.		

Authorised Signatures

Agency/Supplier's Name:

Name & Designation

With seal/stamp

Date: Place:

Form Tech 7:

SELF DECLARATION – SCOPE OF WORK

[To be submitted on the letter head of the bidder]

Ref: _____ **Date: _____**

To:

ED-IT (O)
Air India Ltd.
Airlines House, 113, Gurudwara Rakabganj Road
New Delhi-110001

In response to the RFP ref no _____ dated _____ ,

On Behalf of _____, I/we/undersigned declare providing complete services to **The Client**, in accordance with the Scope of Work and terms & conditions mentioned in this RFP and proposed solution's adherence/ compliance to the Scope of Work. Deviation, if any will be with the mutual Agreement with Client.

I/we/undersigned will do our best to adhere to the proposed Implementation schedule/ Work plan schedule (for supply & services) and also for timely execution of all Deliverables/milestones. The compliance sheet for technical specifications is also attached.

Authorized Signature

Name and Designation

Name of Agency :

With seal/stamp

Date:

Place:

Form Tech 8: **SELF DECLARATION BY BIDDER – NON ELIGIBILITY**

SELF DECLARATION

[To be submitted on the letter head of the bidder]

Ref: _____ **Date: _____**

To:

ED-IT (O)
Air India Ltd.
Airlines House, 113, Gurudwara Rakabganj Road
New Delhi-110001

In response to the RFP ref no _____ dated _____ , On Behalf of _____, I/we/ undersigned declare on the following:

(i) Our Company/ Nor Any Director ever been convicted by any Court of Competent Jurisdiction.

(ii) No criminal case is pending before Court of Competent Jurisdiction against company/ or any Director

(iii) Not involved in theft or in non-payment of Government dues or taxes.

(iv) Not been black listed or debarred by Central Government or any Central Government Authority or any State Government or any State Government Authority.

(v) Our Agency has an unblemished past record and was not declared ineligible for corrupt or fraudulent practice either indefinitely or for a particular period of time.

I/We declare that all the statements made in this Declaration are true, complete and correct to the best of my/our knowledge and belief.

Authorized Signature

Name and Designation

Name of Agency :

With seal/stamp

Date:

Place:

Form Tech 9: **OEM AUTHORISATION LETTER**

O.E.MANUFACTURERS AUTHORISATION FORM

[To be submitted on the original Letterhead of the OEM]

[*Also OEM to send the Authorisation certificate directly to the Client at Email id nirmal.sahai@airindia.in]*

[Date]

To,

ED-IT (O)

Air India Ltd.
Airlines House, 113, Gurudwara Rakabganj Road
New Delhi-110001

Dear Sir,

Ref: Authorization for Air India-IT Security Solutions

Tender Ref. No. _____

Dear Sir,

We _____, (name and address of the manufacturer) who are established and reputed manufacturers of _____ (details of hardware/ software supported as part of the tender) do hereby authorize M/s _____ (name and address of the bidder) to bid, negotiate and conclude the contract with you against the above mentioned tender for the above equipment/ software manufactured/ developed by us.

We confirm that the products quoted are not "end of life or end of sale products" as on bid submission date. If in case the support for the product quoted has been stopped/ withdrawn till the time of delivery of equipment, the same will be changed with the equivalent or superior product at no extra cost.

We also undertake that the support including spares, patches, and upgrades for the quoted products will be available during the project duration.

Yours faithfully,

(Signature)

(Name)

(In the capacity of)

(Name and Address of Company)

Seal/Stamp

SECTION 4:

FINANCIAL PROPOSAL - STANDARD FORMS

Form Fin 1: Financial Proposal Submission Form

[*Location, Date*]

To

ED-IT (O)
Air India Ltd.
Airlines House, 113, Gurudwara Rakabganj Road
New Delhi-110001

Dear Sir,

We, the undersigned, offer to provide the Assignment/job for [Insert title of Assignment/job] in accordance with your Request for Proposal dated [Insert Date] and our Technical Proposal. Our attached Financial Proposals (in one sealed envelope) is for SOLUTION 'A' / SOLUTION 'B' for the sum of Total Rs_____ [Insert amount(s) in words and figures]. This amount is exclusive of all taxes. We hereby confirm that the financial proposals are unconditional and we acknowledge that any condition attached to financial proposal shall result in rejection of our financial proposals.

Our Financial Proposals shall be binding upon us up to expiration of the validity period of the Proposal.

We understand that you are not bound to accept any Proposal you receive.

Yours sincerely,
Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Company:
Address:

Seal/stamp of Bidder:

Form Fin 2: Lumpsum as per TOR of Section 5

BID PROPOSAL SHEETS

Name of the work: **Supply, Installation, Commissioning, Implementation of IT Security Solutions for Air India Ltd.**

Quotes submitted towards providing complete services to **The Client**, in accordance with the Scope of Work and terms & conditions mentioned in RFP.

The financial bid is based as Lump sum fee for each Solution as per following:

SOLUTION 'A' : Next Generation Security Architecture-UTM (Firewall with IPS)	
Proposed Solution for : Next Generation Security Architecture-UTM (Firewall with IPS) 2 nos at Delhi and 2 Nos at Mumbai	
	Amount (in INR) (Excluding taxes)
1. Supply, Installation & commissioning (Supply) Amount (1)	
2. Implementation, Testing and Training (Services) Amount (2)	
Total (Amount 1 + Amount 2)	

'And'

SOLUTION 'B' : Anti-APT solution with Secure Gateway	
Proposed Solution Architecture for : Anti-APT solution with Secure Gateway - 2 nos at Delhi and 2 Nos at Mumbai	
1. Supply, Installation & commissioning (Supply) Amount (1)	
2. Implementation, Testing and Training (Services) Amount (2)	
Total (Amount 1 + Amount 2)	

Note:

- For the purpose of Evaluation of Financial Proposal the Total Amount for each solution will be considered separately.
- The quotes mentioned in the Contract shall be deemed to include all amounts payable for the use of patents, copyrights, registered charges, trademarks and payments for any other intellectual property rights.
- Tax: Taxes are extra as applicable. All taxes (GST) and other impositions as applicable in India, be indicated in the proposal.

Signature of the Authorized Signatory

Place:

Name:

Date:

Designation:

Name & Address of the Bidder:

Seal/stamp of Bidder:

SECTION 5:

TERMS OF REFERENCE

5.1 About The Client

5.2 Technical Specification & Services Required

5.3 Architecture Available

5.4 Scope of Work

5.1 About The Client

The Client is Air India Ltd, having its head office at New Delhi and local offices all over the Country.

5.2 Technical Specification & Services Required

The Client Plans to install the latest and state of Art Next Generation Security Architecture to enhance the IT security infrastructure at its Premises at Head office at New Delhi and another office at Mumbai. All services (Supply, Installation, commission, implementation, testing & training) should be provided by Selected Agency.

The proposed solution to be deployed are required must cover following:

(i) Security Architecture Solution (Supply, installation, commissioning)

(a) **Solution A**: Next Generation Security Architecture-UTM (Firewall with IPS)– 2nos at Delhi in Failover mode and 2 nos at Mumbai in failover mode

(b) **Solution B:** Anti-APT Solution and Secure Web Gateway Solution. -2nos at Delhi in failover mode and 2 nos at Mumbai in failover mode

(ii) Implementation, Testing & Training for the proposed solution

5.3 Architecture Available

- Appoximate 6500+ end devices with Anti virus installed
- Two Centralized Internet Gateway with Firewall and IPS. One at, New Delhi with 2 links of 64 Mbps each. Another one at, Mumbai with 1 link of 100 Mbps and another link of 64 Mbps.
- Internet Gateways at Delhi, Mumbai and Kolkata (3 in Delhi, 2 in Kolkata and 1 in Mumbai) with UTM. Maximum band with at these locations is 8 Mbps at present
- *** The Client has approximately 6500 users in its network and approx. 100 Mbps Internet bandwidth at both Delhi and Mumbai locations..

5.4 SCOPE OF WORK (Supply & Services)

The scope of work for Supply, Installation, Commissioning, Implementation, Testing, & training for the Security Solutions are as follows:

5.4.1 GENERAL REQUIREMENTS

Broad General Requirements of The Client from Security Architecture Project

The Client is looking forward to deploy State of the Art Next Generation Security Architecture

1. OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services

2. OEM should have support Centre in India.
3. The Proposed solution are required to be deployed must cover following :–
   - Next Generation Security Architecture-UTM (Firewall with IPS)
   - Anti-APT Solution with Secure Web Gateway Solution
4. Proposed Solution must have the overall capabilities of scanning various inbound and outbound traffic like Web, File, Network etc. for Monitoring, Detection, cleaning, Analysis and Blocking of APTs and other malicious content
5. Proposed Solution must provide for a dedicated on-premise full-fledged sandboxing analysis solution.
6. Proposed Anti-APT solution should work as a single system for Network, on-premise endpoints and off-premise endpoints with full correlation capabilities
7. Proposed OEMs/ Vendor may use multiple devices/Appliances to fully comply for required functions for every proposed technology
8. Proposed OEMs for Security solution must comply to at least one of the following two requirements
   a. Proposed OEM must be rated as ‘leaders’ or 'Challengers' in the latest Magic Quadrant for Enterprise Next Generation Firewall with IPS(UTM) published by Gartner or in Latest NSS Lab Report.
   b. Proposed OEM for Anti-APT must have scored equal or more than 98.5% 'Security Effectiveness' in latest NSS Breach Detection Systems (BDS) report
9. Bidder must ensure that the Proposed Solution is 100% compliant to all the requirements mentioned in General Requirements and Individual Solutions' Technical Requirements and also provide the proper documentation/proof to support the compliance. Any deviation, Partial Compliance or Non-Compliance will lead to rejection of the bid.
10. Proposed OEM must have it's own dedicated security research team and also a cloud based infrastucture for providing real-time security intelligence. Proposed OEM should have their support in India and support cases should be handled directly from the OEM.
11. Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
12. Bidder should quote mentioning manufacturer's warranty, Subscriptions and part number and provide minimum 5 (Five) years full replacement warranty from the date of successful commissioning.

5.4.2 Individual Solution’s Technical Requirements

1. **SOLUTION ‘A’ : Next Generation Security Architecture-UTM (Firewall with IPS)**

S. No	**Functional Requirement**
1	**Basic Criteria**
a)	OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services
b)	OEM should have support Centre in India.
c)	Appliance should have ICSA certification for Firewall.
d)	The proposed solution should support High Availability Active-Active mode
e)	Appliance Throughput

f)	Firewall throughput of 100,000 Gbps
g)	Minimum 17 Gbps of Antivirus Throughput
h)	Minimum 30,000,000 Concurrent sessions
i)	Minimum 22 Gbps of IPS throughput
j)	Minimum 300,000 New Sessions/second
k)	Minimum 11 Gbps of IPsec VPN throughput
l)	Minimum of 5000 IPsec Site to Site tunnel support and 700 SSL VPN user support. License for the same should be included in the BOM.
m)	Minimum of 8 x GBE Interfaces and 2 x GE SFP and 4 x 10 GE SFPwith expansion slot to accommodate more ports if required.
n)	Should have minimum of 500 GB SSD drives in RAID
2	**General Features**
a)	Should be appliance based and rack mountable
b)	Identity based Firewall
c)	Intrusion Prevention System
d)	Gateway Anti-virus
e)	Gateway Anti-spam with DLP functionality
f)	Web Content & Application Filtering
g)	Web Application Firewall
h)	Bandwidth Management
i)	Inbuilt-on Appliance Reporting
j)	High Availability (Active-Active & Active-Passive)
k)	Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round Robin Balance, Server Load Balancing.
l)	Support for user authentication over SMS.
m)	Country Based Blocking, FQDN support and should support MIX mode deployment
n)	4 Eye Authentication feature for data integrity.
o)	Should have an integrated wireless controller and should be able to manage multiple wireless access points centrally from web admin console.
3	**Gateway Antivirus, Anti-Spyware and Anti-Spam**
	Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management, DLP engine with automatic scanning of emails and attachments for sensitive data
4	**Web and Application Filtering:**
	URL, Keyword, File type block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL, block P2P application, anonymous proxies, Customized block on group basis. Minimum of 89 categories with more than 160 million URLS supported. 2000+ application support categorized into Characteristics, Technology, Category and Risk Level.
	The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS.
5	**Wireless Security and Control:**
	Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and

	manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported Aps
6	**Security Features**
	Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection
7	**Web Application Firewall (WAF):**
	Should have an option of WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.
8	**Advance Threat Protection:**
	Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
9	**VPN:**
	IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.
10	**Load Balance:**
	For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.
11	**Bandwidth Management:**
	Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.
12	**Monitoring and Reporting System:**
a)	· Includes Integrated Web Based reporting,, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1200+ drilled down reports on the appliance.
b)	· Should provide User Threat Quotient (UTQ) report for actionable security intelligence, helping Administrators identify risky users with ease within the organization's network.
c)	License for UTM (Unified Threat Management)
d)	· One Year round the clock support for Gate Way Antivirus, spyware, Anti-Spam, WAF, content and application filtering. IPS, reporting and support, Upgrades.
e)	· License period will be counted after activation.

2. SOLUTION 'B' : ON-PREMISE ANTI-APT SOLUTION WITH SECURE WEB GATEWAY

2(A)	**Anti-APT Solution**
Sr.No	**Functional Requirement**
1	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.
2	The proposed solution should support the native CEF,LEEF format for SIEM log integration
3	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects.
4	Solution must be custom built Anti-APT solution and must not have network perimeter security component part devices like firewall and IDS/IPS
5	Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network
7	Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance threats.
8	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.
9	Solution should provide risk based alerts or logs to help prioritize remediation effort.
10	Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.
11	*The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox.*
12	The proposed solution should use customizable OS sandboxes for detecting zero day malwares, This should not be a CPU or chip based function.
13	Solution should have ability to interrupt malicious communication.
14	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth.
15	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.
16	Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.
17	Solution deployment should cause limited interruption to the current network environment.
18	The proposed solution should able to work with the existing technologies for advance threat protection through web protocol.
19	The proposed solution should be able to detect lateral movement (East-West) of the attacker without the need of installing agents on endpoint/server machines.
20	The proposed solution should support at least 100+ protocols for inspection.
21	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.

22	The Proposed solution should be able to support up to 5 network segments on a single appliance.
23	The proposed solution should be able to identify and help understand the severity and stage of each attack.
24	The proposed solution should have built in capabilities to add exceptions for detections.
25	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.
26	The proposed solution should support Multiple protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device
27	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
28	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.
29	The Proposed solution must provide a web service interface/API for customer to customize integration.
30	The Proposed solution must have capabilities to correlate the detections on the device itself.
31	The Proposed solution should support remote packet capturing for Kerberos traffic from the remote location for analysis.
32	The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session.
33	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.
34	The proposed solution should integrate with web security solution to block threats coming via HTTP, HTTPs and FTP
35	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, Ransomeware protection, C&C detection, and ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.
36	The proposed solution should be able to run at least 60 parallel sandboxes for analysis of payload and on-premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis
37	Endpoints should be able to submit suspicious files directly to the on-premise customized sandbox solution without the need to be intercepted by network based security solutions.
38	Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008 & 2012)
39	The solution should allow administrator to categorize files as safe based on Hash values (MD5) and proposed solution should be able to provide customizable sandbox to match customer's endpoint environments.
40	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection.
41	Solution must have the capability to analyze large files and must be able to support more than 40MB file size.

42	The Proposed solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing. This requirement should be based on virtual execution and should not be a Hardware or chip based function.
43	The proposed solution should have capability to scale out the detection when the bandwidth increases in future.
44	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp
45	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files and proposed solution should support atleast 5 Ethernet Interfaces.
46	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing and solution should have capabilities to scan inside password protected Archive and should have capabilities to detect Malwares and Spywares on windows and non windows platforms.
47	The proposed solution should have option to configure unrestricted internet for sandboxes and proposed solution must have capabilities to detect Mac, Linux and mobile malwares.
48	The Proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..)
49	The Proposed solution should be able to Identify suspicious embedded object in document file like OLE & Macro extraction, Shellcode & exploit matching
50	The Proposed solution should have option to share Indicators of compromise for mitigation and clean up with AV endpoint and Web gateway to block threat at web gateway level. Anti-APT solution should share intelligence with endpoint and security web gateway solution, similarly endpoint and security web gateway should submit files to anti-APT solution for analysis and all three solution should manage through single management console.
51	The proposed solution should have the option to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geo-map, chart , tree-map/pivot table.
52	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.
53	The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.
54	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.
55	The proposed solution shall support Remote administration using SSH/HTTPS and proposed solution shall support CLI, GUI/Web based Administration Console

2(B)	Secure Web Gateway and Content Filtering solution
Sr.No	**Functional Requirement**
1	Should be an integrated solution to provide HTTP/FTP/HTTPS/IM AntiVirus, Content Filtering, Categorized URL Filtering and Web Proxy Caching
2	Should Software appliance on bare metal hardware. As a virtual machine with Vmware ESX/ESXi and Microsoft HyperV & Should be Embedded OS - hardened and performance tumed, provided by OEM, low maintenance with CLI interface and Should be Software Virtual Appliance
3	Should support Forward Proxy, Reverse Proxy, Transparent, Bridge Mode, WCCP, ICAP
4	Should Support external Load balancer as High Availability option and HA in Transparent Bridge Mode
5	WRS Page Analysis (Content Scan), WRS/URL Feedback Option, HTTPS Scanning, Should support Automatic URL Updates, Proactive Web Threats (real-time)
6	Should support atlest 30 Languages and should support User-Defined Categories with Dynamic Classification, Real-time Page Analysis (content scan)
7	Should support Customized HTML Block/Warning Page and Should Support Global and Per Policy Whitelisting with URL Blacklisting
8	Should have Proprietary AV Scanning technology from same OEM and Application Control to identify popular web applications & allow administrators to create policies to monitor or control them.
9	General Pattern String Match, Web Site Match, URL Key Word Match, Per Policy White List, Approved Lists - URL, Approved Lists - Filename, File Object-type Filtering - File type blocking with MIME Content Type, True File Type Matching and Blocking
10	Quota Filtering, Thumbnail / Image Blocking, Compressed File Filtering - Should Block, Pass, Quarantine
11	Should have following FTP Scanning functionality, Reverse FTP Proxy, Passive FTP Support, Active FTP Support, Should Support IP Address based FTP Access Control, FTP Port Filtering
12	Should have following HTTPS Scanning functionality and Decrypt HTTPS traffic from selected Web categories
13	Should have following AV and Spyware scanning capability, Cloud and Signature based Antivirus, Cloud and Signature based Spyware, Phishing - PhishTrap and Cloud-based Web Reputation, Pharming - Web Reputation and URL Filtering, Bots, Cloud and Signature based Keylogging
14	Heuristic Scanning, Signature Matching, Customizable File Filters for Scanning, Large file handling, Compressed File Support - with block, bypass and quarantine modes
15	Quarantine File Support, Real-time Page Analysis (content scan), Automatic Signature Updates, Incremental Updates, Rollback Updates, Solution should be able to detect and block Brute Force Attacks against Passwords, Manual and Automated Updates, Botnet Detection Technology
16	Solution should have Web cache acceleration with File Cache, Dynamic Object Cache and Static Object Cache and Selective Category Logging, full URL Logging
17	The Solution should have captive portal page to authenticate the users instead of the traditional browser popup that asks for the username and password, The captive portal page should be fully customizable by the customer to reflect their

	needs.
18	If there is no LDAP account or the Web Gateway Security couldn't auto detect the user's UserID from LDAP, the web Gateway Solution should present the Captive Portal authentication page for login credential
19	Solution should support Network Packet Capturing so Administrators can analyze traffic with a feature that allows packet captures for selected interfaces or a single interface.
20	Should be Virtual/Software appliance solution and support following Server System, VMware ESX v4.0/4.1 and Hyper-V Support
21	Should integrate with Anti-APT solution to receive IOC's and both solution should have central management console for central visibility.

5.4.3 Installation

Installation should be carried out by OEM as per The Client's requirements

5.4.4 Implementation: Commissioning and Testing

The OEM/Vendor would carry out the Commissioning and Testing of the entire Security Architecture once the installation is complete.

5.4.5 Training

The Training should be provided by the authorized premium training partner* of the OEM. The contents of the course should be of expert level and training duration should be of minimum five days for 12 nos of The client's IT Professionals. The training should lead to one time expert level examination for the OEM certification.

Note

a) *Authorized Premium Training Partner of OEM : OEM certified security training professional and should be graded and meant for this solution*

b) Training has to be conducted both at Delhi and Mumbai with batch size of 12 each

c) ***Infrastructure for Training:*** The location and classrooms will be provided by Air India Ltd. Agency to arrange lecturer and training material.

5.4.6 Licenses: The Client has approx. 6500 users and there could be approx. 4000 concurrent users. The Device Hardware should support these many users. The licensing should preferable be device based rather than users/IP based.

5.4.7 Payment Terms and Schedule

a) Performance Bank Guarantee

1. A PBG of 5 % of value of the agreement would be furnished by the bidder in the form of a Bank Guarantee as per the format provided in this RFP from State Bank of India or any Nationalized Banks or scheduled bank approved by the Reserve Bank of India and acceptable to the Client. The PBG should be furnished within 15 days from the signing of the agreement and should be valid till the entire term of the agreement and for an additional period of six months after the completion of term of agreement including warranty obligations. Bid security would be refunded to the successful bidder on receipt of Performance Bank Guarantee.
2. All incidental charges whatsoever such as premium; commission etc. with respect to the performance bank guarantee shall be borne by the bidder. If the project implementation/go-live is delayed, the PBG shall be extended by the bidder/ for such additional duration. The performance bank guarantee may be discharged/ returned by Air India Ltd. upon being satisfied that there has been due performance of the obligations of the bidder under the agreement. However, no interest shall be payable on the performance bank guarantee.
3. In the event of the bidder being unable to service the agreement for whatever reason, Air India Ltd. would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of Air India Ltd. under the agreement in the matter, the proceeds of the PBG shall be payable to Air India Ltd. as compensation for any loss resulting from the bidder's failure to perform/comply its obligations under the agreement. Air India Ltd. shall notify the bidder in writing of the exercise of its right to receive such compensation within 7 (Seven) days, indicating the contractual obligation(s) for which the bidder is in default.

b) Payment Terms

- The payments will be made as per the mutually agreed payment terms
- The payment as fixed will be made only after deliverables are delivered and completion of required installation and services as detailed in this Tender.
- No advance payment shall be paid to the selected Bidder under any circumstances.
- The selected Bidder will submit invoice(s) along with required documents including proof of completion of implementation.
- The invoices and the supporting documents submitted by the selected Bidder will have to be certified by Air India designated official along with required documents including proof of completion

- Except as otherwise provided all payments under the contract would be made (subject to applicable Liquidated Damages, Penalties as per SLAs defined) by Air India within 30 (thirty) days from the date of receipt of the certified invoices.
- It is clarified that whenever under the contract any sum of money is recoverable from the selected Bidder, Air India shall recover / deduct such sum from the payments due to the selected Bidder and/or Security Deposit/Performance Bank Guarantee held by Air India.
- In the event of the said Security Deposit/Performance Bank Guarantee being sufficient, the balance of total amount recoverable shall be deducted from any sum due to the selected Bidder under the Contract. Should this amount be insufficient to cover the said full amount recoverable, the selected Bidder shall pay to Air India on demand the balance amount, if any, within 14 (fourteen) days of the demand along with the interest @1.5% (one point five percent) p.m. from the due date specified in the demand notice. If any amount due to Air India is so set off against the Security Deposit/Performance Bank Guarantee, the selected Bidder shall be obligated to ensure that the Security Deposit / Performance Bank Guarantee is restored to its original value within 7 (seven) working days from such set off. Non restoration of Security Deposit/Performance Bank Guarantee will be treated as event of default leading to right of Air India to take appropriate remedial action against the selected Bidder, including termination of the contract.

5.4.8 Taxes

The Agency shall include all local taxes and duties on amounts payable by the Agency under the Agreement. All taxes (GST) and other impositions as applicable in India shall be paid by Agency.

5.4.9 Contract Value

a) The Contract Value is the lump sum Fee to be paid by the The Client to Agency as per agreed upon terms of payment .
b) Contract value will remain fixed for the entire Contract period, except changes in the Tax Laws.

5.4.10 Time Frame: To be indicated by the Bidder (Implementation schedule to be given in the Format in Tech-4- Work/Implementation schedule).

5.4.11 Operational Modalities

Any checks of operational modalities will be taken care by a team of Air India Ltd.

5.4.12 Warranty & Support:

a) Support case response should be within Two hour and should be accessible 24x7x365 for support.

b) Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
c) Bidder should quote mentioning manufacturer's warranty, Subscriptions and part number and provide minimum 5 (Five) years full replacement warranty from the date of successful commissioning.

5.4.13 Reporting Mechanism:

The Selected Agency will furnish periodical reports to the client. The reporting mechanism/periodicity will be decided mutually between the client and Agency.

Bank Guarantee Format (Bid Security)

To
The President of India

WHEREAS …….
(name and address of the supplier) (Hereinafter called "the supplier") has undertaken in pursuance of contract no …….. dated …….. to supply (description of goods and services) (hereinafter called "the contract").

AND WHEREAS it has been stipulated by you in the said contract that the supplier shall furnish you with a bank guarantee by a scheduled commercial recognized by you for a sum specified therein as security for compliance with its obligations in accordance with the contract;

AND WHEREAS we have agreed to give the supplier such a bank guarantee;

NOW THEREFORE we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of …… (amount of the guarantee in words and figures), and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed thereunder or of any of the contract documents which may be made between you and the supplier shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

Notwithstanding anything contained herein:

A. Our liability under this guarantee shall not exceed Rs …… (Amount of the bank guarantee) …… (in words)
B. This bank guarantee shall be valid upto _____ & unless a suit for action to enforce a claim under guarantee is filed against us within six months from the date of expiry of guarantee.
C. We are liable to pay the guaranteed amount or any parts thereof under this bank guarantee only and only if you serve upon us a written claim or demand or before _____

This guarantee shall be valid until the ……..day of ……, 201…

(Signature of the authorized officer of the Bank)
……

Name and designation of the officer ……

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

DRAFT

SECTION 6:

STANDARD FORM OF CONTRACT

draft

CONTRACT FOR SERVICES

between

The Air India Ltd

and

[**Name of the Agency**]

Dated: _____

for

Supply, Installation, Commissioning and Implementation of IT Security Solutions for The Client

(On Non-judicial Stamp Paper)

6.1 Form of Agreement

This Agreement is made at _____ (place) on the _____ day of the (month and year) between **(the name of Client)**, a Company registered under the Companies Registration Act, 1956 and having its registered office at _____–through Shri _____ (hereinafter referred to as "**The Client/ Name of Company"** which expression shall unless repugnant to the context thereof include its successor) as of One Part AND a Company / _____ registered under the _____ Act, and (hereinafter referred to as "**Agency"** which expression shall unless repugnant to the context thereof include its successors) as of the Other Part.

WHEREAS

(a) The Agency, having represented to **The Client** that it has the required professional skills, personnel and technical resources, has offered to carry out the services in response to the Tender Notice called 'Request for Proposal' dated_____ issued by **The Client**;

(b) **The Client** has accepted the Proposal dated _____ submitted by the Agency to provide the services on the terms and conditions set forth in this Agreement.

(c)

NOW, THEREFORE IN CONSIDERATION OF THE MUTUAL CONVENANTS HEREIN CONTAINED, IT IS HEREBY AGREED between the Parties as follows:

1. The following documents shall be deemed to form an integral part of this Agreement:
    a. General Conditions of Contract
    b. Terms of Reference
    c. The following Appendices:
        i. Description of Services/ Scope of Work at **Appendix-1**
        ii. Reporting Requirements at **Appendix-2**
        iii. Total Bid Value at **Appendix-3**
        iv. Responsibilities of The Client at **Appendix-4**
        v. Bidder's Compliance/ Declaration –**Appendix-5**:
            a) Self Declaration – Non Eligibility – Form-A
            b) Self Declaration – Scope of Work – Form –B
            c) Bidder's compliance for Technical Specifications – Form -C
        vi. Performance Bank Gurantee –**Appendix-6**:

d. Agency's Proposal dated _____read with agreed Minutes dated _____

e. Letter of Intent dated _____ issued by The Client

f. Certification/Authentication (if any)

2. The mutual rights and obligations of The Client. and the Agency shall be as set forth in this Agreement, in particular:

a. The SCOPE OF WORK will be as per Terms of Reference of Section 5.

b. The activities and the deliverables against each activity would be as per Section 5

c. The Agency shall carry out and complete the Services within the time frame indicated in RFP in accordance with the provisions of this Agreement;

d. Detailed terms and conditions of this Agreement are contained in the Contract Documents mentioned in Para 1 above. The same are to be read harmoniously

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be signed in their respective names as of the day and year first above written.

Signed by _____

1. For and on behalf of [**The Client]**

(i) [Authorized Representative]

(ii)

2. For and on behalf of [**Agency**]

[Authorized Representative]

In presence of (Witnesses)

(i)

(ii)

6.2 General Conditions of Contract

General Provisions

6.2.1 *Definitions*:

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

a) "Applicable Law" means the laws and any other instruments having the force of law in India.
b) "*Client*" means _____(Name of Client) with which the Agency signs the Agreement for the Solution Provider
c) *"Agency"* means any entity or person selected to provide the Services to The Client under the Contract.
d) *"Contract"* means the Agreement signed by the Parties and all the Contract documents listed in its Clause 1 of the Agreement.
e) *"Data Sheet"* means such part of the RFP used to reflect assignment conditions.
f) *"Day"* means calendar day.
g) *"Effective Date"* means the date on which this Agreement comes into force.
h) *"GCC"* means these General Conditions of Contract.
i) *"Government"* means the Government of India
j) "*Indian Currency*" means Indian Rupees (INR).
k) "*Instructions to Bidders"* (Section 2 of the RFP) means the document which provides Bidders with all information needed to prepare their Proposals.
l) "*In writing"* means communicated in written form.
m) *"Liquidated Damages*" herein- may be specified as "LD".
n) *"Local Currency*" means Indian Rupees (INR).
o) *"LOI"* means the Letter of Intent issued by The Client conveying its acceptance of the proposal of the successful bidder.
p) *"Party"* means The Client or the Agency, as the case may be, and "*Parties"* means both of them.
q) *"Personnel*" means Technical Experts/Professionals and support staff provided by the Agency and assigned to perform the Services or any part thereof.
r) "*RFP"* means the Request for Proposal prepared and published by The Client for the selection of Agency.
s) *"Service / Solutions*" means the work to be performed by the Agency as per Scope of Work.
t) *"Third Party*" means any person or entity other than The Client, or the Agency.

6.2.2 Relationship between the Parties

Nothing contained herein shall be construed as establishing a relationship of master and servant or of principal and agent as between The Client and the Agency. The Agency, subject to this Agreement, has complete charge of Technical solutions, Personnel, performing the solutions/ Services and shall

be fully responsible for the Services performed by them on his behalf including salary to its employees.

6.2.3 Law Governing Contract

This Agreement, its meaning and interpretation, and the relation between the Parties shall be governed by the applicable laws of India.

6.2.4 Headings

The headings shall not limit, alter or affect the meaning of this Agreement.

6.2.5 Notices

a) Any notice, request or consent required or permitted to be given or made pursuant to this Agreement shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered against acknowledgement to an authorized representative of the Party to whom the communication is addressed, or when sent by registered post/courier to the addresses specified below.

   Company: _____
   Attention: _____
   Address with Communication details: _____

b) A Party may change its address for notice hereunder by giving the other Party notice in writing of such change to the address specified below.

   Company: _____
   Attention: _____
   Address with Communication details: _____

6.2.6 Location

The Services shall be performed at such locations as indicated in the TOR/LOI and, where the location of a particular task is not so specified, at such locations, as The Client may notify in writing.

6.2.7 Authorized Representatives

Any action required or permitted to be taken, and any document required or permitted to be executed under this Agreement or any amendment thereof by The Client or the Agency may be taken or executed by the officials specified below.

   Company: _____
   Attention: _____
   Address with Communication details: _____

The Agency shall issue Power of Attorney in favor of its Authorized Representative.

6.2.8 Taxes and Duties

The Agency shall be liable to pay all direct and indirect taxes, duties, fees and other impositions levied under the laws of India, applicable at the time of submission of the Proposal.

6.2.9 Fraud and Corruption

Definitions: It is The Client's policy to require that The Client as well as the Agency observes the highest standard of ethics during the execution of the Agreement. For the purpose of this provision, the terms are set forth as follows:

a) "corrupt practice" means the offering, receiving, or soliciting, directly or indirectly, of anything of value (whether in cash or kind) to influence the action of a public official in the selection process or in execution of this Agreement;
b) "fraudulent practice" means a misrepresentation or omission of facts in order to influence the selection process or the execution of this Agreement;
c) "collusive practices" means a scheme or arrangement between two or more Companies, with or without the knowledge of The Client, designed to establish prices at artificial, noncompetitive levels;
d) "coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or affect the execution of this Agreement.

Measures to be taken by The Client

e) The Client may terminate the Agreement if it comes to know at any point of time that representatives of the Agency were engaged in corrupt, fraudulent, collusive or coercive practices during the selection process or the execution of the Agreement The Client after issue of Show Cause Notice to the Agency may declare the Agency ineligible for award of this Contract, if it at any point of time comes to know that the Agency has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for, or in executing, any The Client -financed activity.

6.2.10 Commencement, Completion, Modification and Termination of Agreement

a) ***Effectiveness of Agreement***: This Agreement shall come into force on _____.
b) Unless otherwise terminated under the provisions of any other relevant clauses, this Agreement shall be deemed to have been expired on completion of its terms on _____.
c) ***Entire Agreement****:* This Agreement contains all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any other statement, representation, promise or agreement not set forth herein.
d) ***Modifications or Variations****:*
    - Any modification or variation of the terms and conditions of this Agreement, including any modification or variation of the scope of the Services, may only be made by written agreement between the Parties. However, each Party shall give due consideration to any proposals for modification or variation made by the other Party and cost implication thereof.

- In cases of substantial modifications or variations, a supplementary Agreement between The Client and Agency is required.

e) ***Force Majeure***

i. For the purposes of this Agreement , "Force Majeure" means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable and not brought about by or at the instance of the Party claiming to be affected by such events and which has caused the non-performance or delay in performance, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood or other extreme adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by Government.

ii. Force Majeure shall not include (i) any event which is caused by the negligence or intentional action of a Party or by or of such Party's agents or employees, nor (ii) any event which a diligent Party could reasonably have been expected both to take into account at the time of the signing of the Agreement, and avoid or overcome with utmost persistent effort in the carrying out its obligations hereunder.

iii. Force Majeure shall not include insufficiency of funds or manpower or inability to make any payment required for execution of services under this Agreement.

iv. No Breach of Agreement: The failure of a Party to fulfill any of its obligations hereunder shall not be considered to be a breach of, or default under, this Agreement insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event has taken all possible precautions, due care and all Measures, with the objective of carrying out the terms and conditions of this Agreement.

v. Measures to be taken:

- A Party affected by an event of Force Majeure shall continue to perform its obligations under the Agreement as far as is reasonably practical, and shall take all reasonable measures to minimize the consequences of any event of Force Majeure.
- A Party affected by an event of Force Majeure shall notify the other Party of such event as soon as possible, and in any case not later than fourteen (14) days following the occurrence of such event, providing sufficient and satisfactory evidence of the nature and cause of such event, and shall similarly give written notice of the restoration of normal conditions as soon as possible.
- Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

- During the period of their inability to perform the Services as a result of an event of Force Majeure, the Agency, upon instructions by The Client , shall either: (i) Demobilize or (ii) continue with the Services to the extent possible.
- In the case of disagreement between the Parties as to the existence or extent of Force Majeure, the matter shall be settled according to Clause 6.2.18 hereunder.

f) Suspension

The Client may, by written notice of suspension to the Agency , suspend all rights of Agency, hereunder if the Agency fails to perform any of its obligations under this Contract, including the carrying out of the Services, provided that such notice of suspension (i) shall specify the nature of the failure, and (ii) shall allow the Agency to remedy such failure, if capable of being remedied, within a period not exceeding thirty (30) days after receipt by the Agency of such notice of suspension.

g) Termination:

A. By The Client : The Client may terminate this Agreement in case of the occurrence of any of the events specified in paragraphs (i) through (viii) of this Clause.

i. If the Agency fails to remedy a failure in the performance of its obligations hereunder, as specified in a notice issued by The Client , within thirty (30) days of receipt of such notice or within such further period as The Client may have subsequently approved in writing.
ii. If the Agency becomes insolvent or goes into compulsory liquidation.
iii. If the Agency, in the judgment of The Client, has engaged in corrupt or fraudulent practices in competing for or in executing this Agreement
iv. If the Agency submits to The Client a false statement which has a material effect on the rights, obligations or interests of The Client.
v. If the Agency places itself in position of conflict of interest or fails to disclose promptly any conflict of interest to The Client.
vi. If the Agency fails to provide the quality Services as envisaged under this Agreement. The Client shall in writing give opportunity to the Agency to improve the quality of the Services and take decision if the quality does not improve.
vii. If, as the result of Force Majeure, the Agency is unable to perform a material portion of the Services for a period of within sixty (60) days.

In such an occurrence The Client shall give a not less than thirty (30) days' written advance notice before terminating the Agreement of Agency.

B. By the Agency: The Agency may terminate this Agreement, by not less than thirty (30) days' written notice to The Client, in case of the occurrence of any of the events specified in here under:

i. If The Client fails to pay any money due to the Agency pursuant to this Agreement and not subject to dispute pursuant to Clause 6.2.18 hereof within forty-five (45) days after receiving written notice from the Agency that such payment is overdue.

ii. If, as the result of Force Majeure, the Agency is unable to perform a material portion of the Services for a period of within sixty (60) days.

iii. If The Client fails to comply within 60 days with any final decision reached as a result of Arbitration pursuant to Clause 6.2.18 hereof.

iv. If The Client is in material breach of its obligations pursuant to this Agreement and has not remedied the same within forty-five (45) days (or such longer period as the Agency may have subsequently approved in writing) following the receipt by The Client of the Agency's notice specifying such breach.

C. Cessation of Rights and Obligations: Upon termination of this Agreement pursuant to Clauses 6.2.10(g) hereof, or upon expiration of this Agreement all rights and obligations of the Parties hereunder shall cease, except (i) such rights and obligations as may have accrued on the date of termination or expiration, (ii) the obligation of confidentiality set forth in Clause 6.2.11(d) hereof, (iii) the obligation to pay Damages or Liquidated Damages, permit inspection, copying and auditing of their accounts and records as set forth in, and (iv) any right which a Party may have under the Law.

D. Cessation of Services: Upon termination of this Agreement by notice of either Party to the other pursuant to Clauses 6.2.10(g) hereof, the Agency shall, immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close .

h) Payment upon Termination: Upon termination of this Agreement pursuant to Clause 6.2.10(g) hereof, The Client shall make the following payments to the Agency:

i. If the Agreement is terminated pursuant of Clause 6.2.10(g) [A] (i) to (vi), the Agency shall not be entitled to receive any agreed fees upon termination of the Agreement. However, The Client may consider giving part fee for the part satisfactorily performed on the basis of Quantum Merit as assessed by it, if such part is of economic utility to The Client. Under such circumstances, upon termination, The Client may also impose liquidated damages as per the provisions of Clause 6.2.19 hereof. The Agency will be required to pay any such liquidated damages and compensation as permissible under Contract Act to The Client within Thirty (30) days of termination date.

ii. In the event of termination under 6.2.10(g) [A] (vii) & [B] (i)), the payment schedule as specified in this Agreement shall not apply and the costs of architecture and Services delivered by Agency and the cost of demobilization of Agency teams will be decided and paid by The Client to the Agency.

Disputes about Events of Termination: If either Party disputes whether an event specified in paragraphs (i) through (viii) of Clause 6.2.10(g)[A] or in para (ii) through (iv) in Clause 6.2.10(g) [B] hereof has occurred, such Party may, if it chosen within forty-five (45) days after receipt of notice of termination from the other Party, may seek settlement under Clause 6.2.18 hereof.

6.2.11 Obligations of the Agency

a) ***Standard of Performance:*** The Agency shall perform the activities and Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Agency shall always act, in respect of any matter relating to this Agreement or to the Services, as faithful adviser to The Client, and shall at all times support and safeguard The Client legitimate interests in its dealings.

b) ***Conflict of Interests***: The Agency shall hold The Client's interests paramount and strictly avoid conflict of interest with other assignments or their own corporate interests. If during the period of this Contract, a conflict of interest arises for any reasons, the Agency shall promptly disclose the same to The Client and seek its instructions for compliance.

c) ***Prohibition of Conflicting Activities***: The Agency shall not engage, and shall cause their Personnel not to engage, either directly or indirectly, in any business or professional activities that would conflict with the activities assigned to them under this Agreement.

d) ***Confidentiality***: Except with the prior written consent of The Client, the Agency and the Personnel of itshall not at any time communicate to any person or entity any confidential information acquired in the course of the Services.

e) ***Statutory requirements by the Agency***: The Agency is liable to extend the benefits as provided under the various statutory and labour laws and other relevant applicable laws.

f) ***Agency's actions requiring prior approval***: The Agency will have the right to recruit and terminate the staff except for the Project Manager which may be done in consultation with The Client.

g) ***Reporting Obligations***: The Agency shall submit to The Client the reports and documents (agreed to be submitted between The Client and Agency) hereto, in the form, in the numbers and within the time periods mutually agreed.

6.2.12 Agencys' Personnel

The Agency shall employ and provide at its own cost such qualified and experienced Personnel as are required to carry out the Services. Their salaries, claims, insurance, damages, compensation, travel etc. will be the liability of the Agency and The Client will in no way be responsible for any such claims/damages.

6.2.13 Obligations of The Client

a) *Assistance and Exemptions:* Unless otherwise specified, The Client shall use its best efforts to provide to the Agency and its personnel such assistance to facilitate performance of the Contract as may be considered necessary.

b) *Change in the Applicable Law Related to Taxes and Duties*: If, after the date of this Agreement, there is any change of rate of levy under the existing applicable Laws of India with respect to taxes and duties, which are directly payable by the Agency for providing the services i.e. VAT or Service Tax or any such other applicable tax from time to time, which

increase or decreases the cost incurred by the Agency in performing the Services, or, in case of any new or fresh tax or levy imposed after submission of the Proposal the Agency shall be entitled to reimbursement on submission of proof of payment of such Tax or Levy.

c) The other duties of The Client, if any, shall be as mutually agreed between The Client and the Agency.

6.2.14 Payments to the Agency

a) *Currency of Payment*: All payments shall be made in Indian Rupees (INR).

6.2.15 Deductions

All payments to the Agency shall be subject to the deductions of tax at source under the relevant provisions of the Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which The Client may have paid or incurred, for which under the provisions of the Agreement, the Agency is liable, the same shall be deducted by The Client from any dues to the Agency.

6.2.16 Fairness and Good Faith

a) ***Good Faith***: The Parties undertake to act in good faith with respect to each other's rights under this Agreement and to adopt all reasonable measures to ensure the realization of the objectives of this Agreement.

b) ***Operation of the Contract***: The Parties recognize that it may not be possible to provide for every contingency which may arise during the life of the Agreement, and the Parties hereby agree that it is their intention that this Contract shall operate fairly as between them, and without detriment to the interest of either of them, and that, if during the term of this Contract either Party believes that this Contract is operating unfairly, the Parties will make their best efforts to agree on such action as may be necessary to remove the cause or causes of such non-fairness, but no failure to agree on any action pursuant to this Clause may give rise to a dispute subject to Arbitration in accordance with Clause 6.2.18 hereof.

6.2.17 Settlement of Disputes

a) ***Amicable Settlement***: Performance of the Agreement is governed by the terms & conditions of the Agreement, in case of dispute arises between the Parties regarding any matter under the Agreement, either Party of the Agreement may send a written Notice of Dispute to the other Party. The Party receiving the Notice of Dispute will consider the Notice and respond to it in writing within Thirty (30) days after receipt. If that Party fails to respond within Thirty (30) days, or the dispute cannot be amicably settled within Sixty (60) days following the response of that Party, clause 6.2.18(b) shall become applicable.

b) ***Arbitration***: In the case of dispute arising upon or in relation to or in connection with the Agreement between The Client and the Agency, which has not been settled amicably, any Party may refer the dispute for Arbitration under Arbitration and Conciliation Act, 1996. Such disputes shall be referred to an Arbitral Tribunal consisting of 3 (three) arbitrators, one each to be appointed by The Client and the Agency, the third arbitrator shall be chosen by the two arbitrators so appointed by the Parties which shall act as Presiding Arbitrator. In

case of failure of the two arbitrators, appointed by the Parties to reach a consensus regarding the appointment of the third arbitrator within a period of Thirty (30) days from the date of appointment of the two arbitrators, the Presiding arbitrator shall be appointed by The Client Ltd. The Arbitration and Conciliation Act, 1996 and any statutory modification or re-enactment thereof, shall apply to these Arbitration proceedings.

c) Arbitration proceedings shall be held in India at New Delhi and the language of the Arbitration proceedings and that of all documents and communications between the Parties shall be English.

d) The decision of the majority of arbitrators shall be final and binding upon both Parties. The expenses of the arbitrators as determined by the arbitrators shall be shared equally by The Client and the Agency. However, the expenses incurred by each Party in connection with the preparation, presentation shall be borne by the Party itself. All Arbitration awards shall be in writing and shall state the reasons for the award.

e) Notwithstanding any references to arbitration, the parties shall continue to perform their respective work/ obligation under the Agreement.

6.2.18 Performance Bank Gurantee

1. A PBG of 5 % of value of the agreement would be furnished by the bidder in the form of a Bank Guarantee as per the format provided in this RFP from Nationalized Banks or scheduled Indian bank, approved by the Reserve Bank of India and acceptable to the client. The PBG should be furnished within 15 days from the signing of the agreement and should be valid till the entire term of the agreement and for an **additional period of six months** after the completion of term of agreement including warranty obligations. Bid security would be refunded to the successful bidder on receipt of Performance Bank Guarantee.

2. All incidental charges whatsoever such as premium; commission etc. with respect to the performance bank guarantee shall be borne by the bidder. If the project implementation/go-live is delayed, the PBG shall be extended by the bidder/ for such additional duration. The performance bank guarantee may be discharged/ returned by Air India Ltd. upon being satisfied that there has been due performance of the obligations of the bidder under the agreement. However, no interest shall be payable on the performance bank guarantee.

3. In the event of the bidder being unable to service the agreement for whatever reason, Air India Ltd. would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of Air India Ltd. under the agreement in the matter, the proceeds of the PBG shall be payable to Air India Ltd. as compensation for any loss resulting from the bidder's failure to perform/comply its obligations under the agreement. Air India Ltd. shall notify the bidder in writing of the exercise of its right to receive such compensation within 7 (Seven) days, indicating the contractual obligation(s) for which the bidder is in default.

6.2.19 Taxes

a) The Agency shall include all local taxes and duties on amounts payable by the Agency under the Agreement. All taxes (GST) and other impositions as applicable in India shall be paid by Agency.

6.2.20 Contract Value

a) The Contract Value is the lump sum Fee to be paid by the The Client to Agency as per agreed upon terms of payment .

b) Contract value will remain fixed for the entire Contract period, except changes in the Tax Laws.

6.2.21 Payment Terms

- The payments will be made as per the mutually agreed payment terms
- The payment as fixed will be made only after deliverables are delivered and completion of required installation and services as detailed in this Tender.
- No advance payment shall be paid to the selected Bidder under any circumstances.
- The selected Bidder will submit invoice(s) along with required documents including proof of completion of implementation.
- The invoices and the supporting documents submitted by the selected Bidder will have to be certified by Air India designated official along with required
- documents including proof of completion
- Except as otherwise provided all payments under the contract would be made (subject to applicable Liquidated Damages, Penalties as per SLAs defined) by Air India within 30 (thirty) days from the date of receipt of the certified invoices.
- It is clarified that whenever under the contract any sum of money is recoverable from the selected Bidder, Air India shall recover / deduct such sum from the payments due to the selected Bidder and/or Security Deposit/Performance Bank Guarantee held by Air India.
- In the event of the said Security Deposit/Performance Bank Guarantee being sufficient, the balance of total amount recoverable shall be deducted from any sum due to the selected Bidder under the Contract. Should this amount be insufficient to cover the said full amount recoverable, the selected Bidder shall pay to Air India on demand the balance amount, if any, within 14 (fourteen) days of the demand along with the interest @1.5% (one point five percent) p.m. from the due date specified in the demand notice. If any amount due to Air India is so set off against the Security Deposit/Performance Bank Guarantee, the selected Bidder shall be obligated to ensure that the Security Deposit / Performance Bank Guarantee is restored to its

original value within 7 (seven) working days from such set off. Non restoration of Security Deposit/Performance Bank Guarantee will be treated as event of default leading to right of Air India to take appropriate remedial action against the selected Bidder, including termination of the contract.

6.2.22 Transfer of Contract

Agency shall not assign or transfer the contract or any part thereof Agency shall act as an independent entity fully performing responsible for all Services under the Contract. It shall maintain complete control over its employees, who shall in no case, represent The Client or act in its name,

6.2.23 Miscellaneous Provisions

a) Any failure or delay on the part of any Party to exercise right or power under this Agreement shall not operate as waiver thereof.

b) The Agency shall notify The Client of any material change in its status as legal entity, in particular, where such change or winding up proceeding which would impact on performance of obligations under this Agreement.

c) The Agency shall at all times indemnify and keep indemnified The Client /Government of India against all claims/damages etc. for any infringement of any Intellectual Property Rights (IPR) while providing its Services under the Agreement.

d) The Agency shall at all times indemnify and keep indemnified The Client against any claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its (the Agency's) employees or agents or caused by any action, omission or operation conducted by or on behalf of the Agency.

e) The Agency shall at all times indemnify and keep indemnified The Client against any and all claims by Employees, Workman, Companies, suppliers, agent(s), employed engaged or otherwise working for the Agency, in respect of their wages, salaries, remuneration, compensation or the like.

f) All claims regarding indemnity shall survive the termination or expiry of the Contract.

g) It is acknowledged and agreed by all Parties that there is no representation of any type, implied or otherwise, of any absorption, regularization, continued engagement or concession or preference for employment of persons engaged by the Agency for any subsequent engagement, service or employment in any capacity in any office or establishment of the Government India or The Client

h) Time shall be of the essence in respect of any date or period specified in this Agreement or any notice, demand or other communication served under or pursuant to any provision of this Agreement.

APPENDIX – 1

Description of Services/ Scope of Work

The Scope of Work for the Agency/Supplier is as Follows:

1. SCOPE OF WORK (Supply & Services)

The scope of work for Supply, Installation, Commissioning, Implementation, Testing, & training for the Security Solutions are as follows:

2. Individual Solution's Technical Requirements (Hardware/software solution)

(to be included here)

[the scope of work / deliverables to be included here]

3. Installation

[the installation time schedule/ deliverables as per Client's requirements *may be included here]*

4. Implementation : Commissioning and Testing

[The installation mechanism as per agreed terms may be included here - Commissioning and Testing of the entire Security Architecture]

5. Training

[The Training Schedule/ deliverables etc included here]

Note*

The Training should be provided by the authorized premium training partner* of the OEM. The contents of the course should be of expert level and training duration should be of minimum five days for 12 nos of The client's IT Professionals. The training should lead to one time expert level examination for the OEM certification.

a) *Authorised Premium Training Partner of OEM : OEM certified security training professional and should be graded and meant for this solution*

b) Training has to be conducted both at Delhi and Mumbai with batch size of 12 each

c) ***Infrastructure for Training:*** The location and classrooms will be provided by The Client. Agency to arrange lecturer and training material.

APPENDIX – 2

Reporting Requirements/ Workplan

[Reporting mechanism to be included here]

S. **No.**	**Activity**[1]	**Months**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**n**
1									
2									
3									
4									
5									
n									

(to be provided by the Agency)

The Agency will furnish periodical reports to the The Client . The periodicity will be decided mutually between the The Client and the Agency/Supplier

APPENDIX – 3

Total Bid Value

The total bid value for the said Solution is as follows:

[Total Bid Value to be quoted here]

[Also taxes to be mentioned.]

(as quoted by the Agency/Supplier)

Payment Terms

APPENDIX – 4

Role & Responsibilities of The Client

[Responsibilities of the Client to be mentioned here]

APPENDIX – 5

Form – A : SELF DECLARATION – NON-ELIGIBILITY

[To be submitted on the letter head of the bidder]

Ref: _____ **Date: _____**

To:

The Client

In response to the RFP Tender ref no _____ dated _____ , On Behalf of _____,

I/we/ undersigned declare on the following:

(vi) Our Company/ Nor Any Director ever been convicted by any Court of Competent Jurisdiction.

(vii) No criminal case is pending before Court of Competent Jurisdiction against company/ or any Director

(viii) Not involved in theft or in non-payment of Government dues or taxes.

(ix) Not been black listed or debarred by Central Government or any Central Government Authority or any State Government or any State Government Authority.

(x) Our Agency has an unblemished past record and was not declared ineligible for corrupt or fraudulent practice either indefinitely or for a particular period of time.

I/We declare that all the statements made in this Declaration are true, complete and correct to the best of my/our knowledge and belief.

Authorized Signature

Name and Designation

Name of Agency :

With seal/stamp

Date:

Place:

Form – B : SELF DECLARATION – SCOPE OF WORK

[To be submitted on the letter head of the bidder]

Ref: _____ **Date: _____**

To:

The Client

In response to the RFP ref no _____ dated _____ ,

On Behalf of _____, I/we/undersigned declare providing complete services to **The Client**, in accordance with the Scope of Work and terms & conditions mentioned in this RFP and proposed solution's adherence/ compliance to the Scope of Work. Deviation, if any will be with the mutual Agreement with Client.

I/we/undersigned will do our best to adhere to the proposed Implementation schedule/ Work plan schedule (for supply & services) and also for timely execution of all Deliverables/milestones. The compliance sheet for technical specifications is also attached.

Authorized Signature

Name and Designation

Name of Agency :

With seal/stamp

Date:

Place:

Form –C : Bidder's compliance - General & Technical Specifications for the subject Scope of Work

[To be submitted on the letter head]

COMPLIANCE SHEET – GENERAL REQUIREMENTS (with Supporting Documents)

[To be submitted on letter head]

	Technical Solutions – Broad General Requirements for Security Architecture Project	**Compliance X / √**
1.	OEM should attain ISO 27001 Certification as well as should attain ISO for its Support Services	
2.	OEM should have support Centre in India.	
3.	The Proposed solution must cover following :– ➢ Next Generation Security Architecture-UTM (Firewall with IPS) ➢ Anti-APT Solution with Secure Web Gateway Solution	
4.	Proposed Solution must have the overall capabilities of scanning various inbound and outbound traffic like Web, File, Network etc. for Monitoring, Detection, cleaning, Analysis and Blocking of APTs and other malicious content	
5.	Proposed Solution must provide for a dedicated on-premise full-fledged sandboxing analysis solution.	
6.	Proposed Anti-APT solution should work as a single system for Network, on-premise endpoints and off-premise endpoints with full correlation capabilities	
7.	Proposed OEMs/ Vendor may use multiple devices/Appliances to fully comply for required functions for every proposed technology	
8.	Proposed OEMs for Security solution must comply to at least one of the following two requirements c. Proposed OEM must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Next Generation Firewall with IPS(UTM) published by Gartner or in Latest NSS Lab Report. d. Proposed OEM for Anti-APT must have scored equal or more than 98.5% 'Security Effectiveness' in latest NSS Breach Detection Systems (BDS) report	
9.	Bidder must ensure that the Proposed Solution is 100% compliant to all the requirements mentioned in General Requirements and Individual Solutions' Technical Requirements and also provide the proper documentation/proof to support the compliance. Any deviation, Partial Compliance or Non-Compliance will lead to rejection of the bid.	
10.	Proposed OEM must have it's own dedicated security research team and also a cloud based infrastructure for providing real-time security intelligence. Proposed OEM should have their support in India and support cases should be handled directly from the OEM.	
11.	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.	
12.	Bidder should quote mentioning manufacturer's warranty, Subscriptions and part number and provide minimum 5 (Five) years full replacement warranty from the date of successful commissioning.	

Documentary proof is essential without which the proposal may be rejected. Technical and Financial evaluation will be done only for the bidders satisfying the above criteria.

Authorized Signatory

_____

<*Company Name*>

Seal/stamp of Bidder:
Date:

Proposed Individual Solution – Technical Compliance

[to be submitted on letterhead]

SOLUTION 'A' : Next Generation Security Architecture-UTM (Firewall with IPS)

Solution's Technical Requirements

S. No	Functional Requirement	Bidder's Compliance	Remarks
1	**Basic Criteria**		
a)	OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services		
b)	OEM should have support Centre in India.		
c)	Appliance should have ICSA certification for Firewall.		
d)	The proposed solution should support High Availability Active-Active mode		
e)	Appliance Throughput		
f)	Firewall throughput of 100,000 Gbps		
g)	Minimum 17 Gbps of Antivirus Throughput		
h)	Minimum 30,000,000 Concurrent sessions		
i)	Minimum 22 Gbps of IPS throughput		
j)	Minimum 300,000 New Sessions/second		
k)	Minimum 11 Gbps of IPsec VPN throughput		
l)	Minimum of 5000 IPsec Site to Site tunnel support and 700 SSL VPN user support. License for the same should be included in the BOM.		
m)	Minimum of 8 x GBE Interfaces and 2 x GE SFP and 4 x 10 GE SFPwith expansion slot to accommodate more ports if required.		
n)	Should have minimum of 500 GB SSD drives in RAID		
2	**General Features**		
a)	Should be appliance based and rack mountable		
b)	Identity based Firewall		
c)	Intrusion Prevention System		
d)	Gateway Anti-virus		
e)	Gateway Anti-spam with DLP functionality		
f)	Web Content & Application Filtering		
g)	Web Application Firewall		
h)	Bandwidth Management		
i)	Inbuilt-on Appliance Reporting		
j)	High Availability (Active-Active & Active-Passive)		
k)	Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round Robin Balance, Server Load Balancing.		
l)	Support for user authentication over SMS.		
m)	Country Based Blocking, FQDN support and should support MIX mode deployment		

n)	4 Eye Authentication feature for data integrity.		
o)	Should have an integrated wireless controller and should be able to manage multiple wireless access points centrally from web admin console.		
3	**Gateway Antivirus, Anti-Spyware and Anti-Spam**		
	Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management, DLP engine with automatic scanning of emails and attachments for sensitive data		
4	**Web and Application Filtering:**		
	URL, Keyword, File type block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL, block P2P application, anonymous proxies, Customized block on group basis. Minimum of 89 categories with more than 160 million URLS supported. 2000+ application support categorized into Characteristics, Technology, Category and Risk Level.		
	The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS.		
5	**Wireless Security and Control:**		
	Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported Aps		
6	**Security Features**		
	Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection		
7	**Web Application Firewall (WAF):**		
	Should have an option of WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.		
8	**Advance Threat Protection:**		
	Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)		

9	**VPN:**		
	IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.		
10	**Load Balance:**		
	For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.		
11	**Bandwidth Management:**		
	Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.		
12	**Monitoring and Reporting System:**		
a)	· Includes Integrated Web Based reporting,, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1200+ drilled down reports on the appliance.		
b)	· Should provide User Threat Quotient (UTQ) report for actionable security intelligence, helping Administrators identify risky users with ease within the organization's network.		
c)	License for UTM (Unified Threat Management)		
d)	· One Year round the clock support for Gate Way Antivirus, spyware, Anti-Spam, WAF, content and application filtering. IPS, reporting and support, Upgrades.		
e)	· License period will be counted after activation.		

Documentary proof is essential without which the proposal may be rejected. Technical and Financial evaluation will be done only for the bidders satisfying the above criteria.

Authorized Signatory

_____

<*Company Name*>

Seal/stamp of Bidder:

Date:

SOLUTION 'B' - ON-PREMISE ANTI-APT SOLUTION WITH SECURE WEB GATEWAY

[to be submitted on letterhead]

(A)	**Anti-APT Solution**		
Sr.No	**Functional Requirement**	**Bidder's Compliance**	**Remarks**
1	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.		
2	The proposed solution should support the native CEF,LEEF format for SIEM log integration		
3	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects.		
4	Solution must be custom built Anti-APT solution and must not have network perimeter security component part devices like firewall and IDS/IPS		
5	Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network		
7	Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance threats.		
8	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.		
9	Solution should provide risk based alerts or logs to help prioritize remediation effort.		
10	Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.		
11	*The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox.*		
12	The proposed solution should use customizable OS sandboxes for detecting zeroday malwares, This should not be a CPU or chip based function.		
13	Solution should have ability to interrupt malicious communication.		
14	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth.		
15	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.		
16	Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.		
17	Solution deployment should cause limited interruption to the current network environment.		

18	The proposed solution should able to work with the existing technologies for advance threat protection through web protocol.		
19	The proposed solution should be able to detect lateral movement (East-West) of the attacker without the need of installing agents on endpoint/server machines.		
20	The proposed solution should support at least 100+ protocols for inspection.		
21	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.		
22	The Proposed solution should be able to support up to 5 network segments on a single appliance.		
23	The proposed solution should be able to identify and help understand the severity and stage of each attack.		
24	The proposed solution should have built in capabilities to add exceptions for detections.		
25	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.		
26	The proposed solution should support Multiple protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device		
27	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.		
28	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.		
29	The Proposed solution must provide a web service interface/API for customer to customize integration.		
30	The Proposed solution must have capabilities to correlate the detections on the device itself.		
31	The Proposed solution should support remote packet capturing for Kerberos traffic from the remote location for analysis.		
32	The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session.		
33	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.		
34	The proposed solution should integrate with web security solution to block threats coming via HTTP, HTTPs and FTP		
35	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, ransomeware protection, C&C detection, ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero		

	day malwares by sharing Indicators of Compromise.		
36	The proposed solution should be able to run atleast 60 parallel sandboxes for analysis of payload and on-premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis		
37	Endpoints should be able to submit suspicious files directly to the on-premise customized sandbox solution without the need to be intercepted by network based security solutions.		
38	Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008 & 2012)		
39	The solution should allow administrator to categorize files as safe based on Hash values (MD5) and proposed solution should be able to provide customizable sandbox to match customer's endpoint environments.		
40	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection.		
41	Solution must have the capability to analyze large files and must be able to support more than 40MB file size.		
42	The Proposed solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing. This requirement should be based on virtual execution and should not be a Hardware or chip based function.		
43	The proposed solution should have capability to scale out the detection when the bandwidth increases in future.		
44	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp		
45	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files and proposed solution should support atleast 5 Ethernet Interfaces.		
46	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing and solution should have capabilities to scan inside password protected Archive and should have capabilities to detect Malwares and Spywares on windows and non windows platforms.		
47	The proposed solution should have option to configure unrestricted internet for sandboxes and proposed solution must have capabilities to detect Mac, Linux and mobile malwares.		
48	The Proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..)		
49	The Proposed solution should be able to Identify suspicious embedded object in document file like OLE & Macro extraction, Shell code & exploit matching		

50	The Proposed solution should have option to share Indicators of compromise for mitigation and clean up with AV endpoint and Web gateway to block threat at web gateway level. Anti-APT solution should share intelligence with endpoint and security web gateway solution, similarly endpoint and security web gateway should submit files to anti-APT solution for analysis and all three solution should manage through single management console.		
52	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.		
53	The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.		
54	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.		
55	The proposed solution shall support Remote administration using SSH/HTTPS and proposed solution shall support CLI, GUI/Web based Administration Console		

Secure Web Gateway and Content Filtering solution

(B)	**Secure Web Gateway and Content Filtering solution**		
Sr.No	**Functional Requirement**	**Bidder's Compliance**	**Remarks**
1	Should be an integrated solution to provide HTTP/FTP/HTTPS/IM Antivirus, Content Filtering, Categorized URL Filtering and Web Proxy Caching		
2	Should Software appliance on bare metal hardware. As a virtual machine with Vmware ESX/ESXi and Microsoft HyperV & Should be Embedded OS - hardened and performance tumed, provided by OEM, low maintenance with CLI interface and Should be Software Virtual Appliance		
3	Should support Forward Proxy, Reverse Proxy, Transparent, Bridge Mode, WCCP, ICAP		
4	Should Support external Load balancer as High Availability option and HA in Transparent Bridge Mode		
5	WRS Page Analysis (Content Scan), WRS/URL Feedback Option, HTTPS Scanning, Should support Automatic URL Updates, Proactive Web Threats (real-time)		
6	Should support atlest 30 Languages and should support User-Defined Categories with Dynamic Classification, Real-time Page Analysis (content scan)		
7	Should support Customized HTML Block/Warning Page and Should Support Global and Per Policy Whitelisting with URL Blacklisting		
8	Should have Proprietary AV Scanning technology from same OEM and Application Control to identify popular web applications & allow administrators to create policies to monitor or control them.		
9	General Pattern String Match, Web Site Match, URL Key Word Match, Per Policy White List, Approved Lists - URL, Approved Lists - Filename, File Object-type Filtering - File type blocking with MIME Content Type, True File Type Matching and Blocking		

(B)	**Secure Web Gateway and Content Filtering solution**		
10	Quota Filtering, Thumbnail / Image Blocking, Compressed File Filtering - Should Block, Pass, Quarantine		
11	Should have following FTP Scanning functionality, Reverse FTP Proxy, Passive FTP Support, Active FTP Support, Should Support IP Address based FTP Access Control, FTP Port Filtering		
12	Should have following HTTPS Scanning functionality and Decrypt HTTPS traffic from selected Web categories		
13	Should have following AV and Spyware scanning capability, Cloud and Signature based Antivirus, Cloud and Signature based Spyware, Phishing - PhishTrap and Cloud-based Web Reputation, Pharming - Web Reputation and URL Filtering, Bots, Cloud and Signature based Keylogging		
14	Heuristic Scanning, Signature Matching, Customizable File Filters for Scanning, Large file handling, Compressed File Support - with block, bypass and quarantine modes		
15	Quarantine File Support, Real-time Page Analysis (content scan), Automatic Signature Updates, Incremental Updates, Rollback Updates, Solution should be able to detect and block Brute Force Attacks against Passwords, Manual and Automated Updates, Botnet Detection Technology		
16	Solution should have Web cache acceleration with File Cache, Dynamic Object Cache and Static Object Cache and Selective Category Logging, full URL Logging		
17	The Solution should have captive portal page to authenticate the users instead of the traditional browser popup that asks for the username and password, The captive portal page should be fully customizable by the customer to reflect their needs.		
18	If there is no LDAP account or the Web Gateway Security couldn't auto detect the user's UserID from LDAP, the web Gateway Solution should present the Captive Portal authentication page for login credential		
19	Solution should support Network Packet Capturing so Administrators can analyze traffic with a feature that allows packet captures for selected interfaces or a single interface.		
20	Should be Virtual/Software appliance solution and support following Server System, VMware ESX v4.0/4.1 and Hyper-V Support		
21	Should integrate with Anti-APT solution to receive IOC's and both solution should have central management console for central visibility.		

Authorised Signatures

Agency/Supplier's Name:

Name & Designation

With seal/stamp

Date:
Place:

APPENDIX – 6

BANK GUARANTEE (PERFORMANCE BANK GUARANTEE)

(To be stamped in accordance with Stamp Act)

Bank Guarantee No. …….

Date ……..

To

[Air India's Name & Address]

Dear Sirs,

In consideration of the …….. [Air India's Name]……. (herein after referred to as the Air India Ltd.,' which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators and assigns) having awarded to M/s. ……..[Agency's Name] ……..with its Registered/Head Office at …… (Hereinafter referred to as the Agency', which expression shall unless repugnant to the context or meaning thereof, include its successors administrators, executors and assigns), a Agreement by issue of Air India's Notification of Award No. …….. Dated …….. and the same having been unequivocally accepted by the

Agency, resulting in to a agreement bearing No…….. dated …….. Valued at…….. for …… and the Agency having agreed to provide a Performance Guarantee for the faithful performance of the entire Agreement equivalent to ….. (*) ….. % (……. percent) of the said value of the Agreement to the Air India Ltd..

We …….. [Name & Address of the Bank] ……. having its Head Office at …….. (hereinafter referred to as the 'Bank', which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns) do hereby guarantee and undertake to pay the Air India Ltd., on demand any and all monies payable by the Agency to the extent of …….. (*) ……. as aforesaid at any time upto …… (@) …… [days/month/year] without any demur, reservation, context, recourse or protest and/or without any reference to the Agency. Any such demand made by Air India on the Bank shall be conclusive and binding notwithstanding any difference between Air India and the Agency or any dispute pending before any Court, Tribunal, Arbitrator or any other authority. The Bank undertakes not to revoke this guarantee

during its currency without previous consent of Air India and further agrees that the guarantee herein contained shall continue to be enforceable till the Air India discharges this guarantee.

The Air India shall have the fullest liberty, without affecting in any way the liability of the Bank under this guarantee, from time to time to extend the time for performance of the agreement by the Agency. The Air India shall have the fullest liberty, without affecting this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Agency, and to exercise the same at any time in any manner, and either to enforce or to forbear to enforce any covenants, contained or implied, in the Agreement between the Air India and the Agency or any other course or remedy or security available to the Air India Ltd.. The Bank shall not be released of its obligations under these presents by any exercise by the Air India of its liberty with reference to the matters omission or commission on the part of the Owner or any other indulgence shown by the Air India or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the Bank.

The Bank also agrees that the Air India at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Agency and notwithstanding any security or other guarantee that the Air India may have in relation to the Agency's liabilities.

Notwithstanding anything contained hereinabove, our liability under this guarantee is restricted to …….. (*) …….. and it shall remain in force up to and including…….. (@) …… and shall be extended from time to time for such period, as may be desired by M/s…….. [Agency's Name] …….. on whose behalf this guarantee has been given.

In witness where of the Bank, through its authorized officer, has set its hand and stamp on this

…… day of …….. 2017 at …… This …….. day of …….. 2017 at ……..

……

(Signature)

(Designation with Bank Stamp)

Attorney as per Power of

Attorney No……

Dated …….

(Official Address):

WITNESS

……..

(Signature)

(Name)

Notes:

(*) This sum shall be five percent (5%) of the value of the contract.

(@) This date will be one year after the completion of term of agreement including warranty obligations.

The stamp papers of appropriate value shall be purchased in the name of Guarantee issuing Bank.

**********END OF DOCUMENT**********