भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

REQUEST FOR PROPOSAL FOR ENGAGING AGENCY FOR SECURITY OPERATIONS CENTER (SOC) SERVICES

Tender Reference Number: RFP:2012-13/0025 dated 16.01.2013

National Payments Corporation of India
13th Floor, R Tech Park,
Off Western Express Highway,
Nirlon Complex, Near HUB mall ,
Goregaon-East, Mumbai – 400063
Tel: +91-22-40508500
email- itprocurement@npci.org.in
Website: www.npci.org.in

Copyright Notice

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to Bidder or applicants whether verbally or in documentary form by or on behalf of National Payments Corporation of India (NPCI), is provided to the Bidder on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by NPCI to any parties other than the applicants who are qualified to submit the Bids ("Bidders"). The purpose of this RFP document is to provide Bidder with information to assist the formulation of their proposals. This RFP document does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP document and where necessary obtain independent advice. NPCI makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP document. NPCI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP document.

Important Detail about RFP

Note: Bids will be opened in the presence of the Bidders' representatives who choose to attend Bid opening meeting.

Checklist

The following items must be checked before the bid is submitted:

1. Demand Draft / Pay Order of INR 5,618 (Rupees Five thousand Six Hundred Eighteen Only) inclusive of taxes, in Envelope – 'A' towered cost of RFP.
2. Demand Draft / Banker's Cheque / Bank Guarantee of INR 2,00,000/- (Rupees Two Lakh Only) towards Bid Security in Envelope – 'A' Earnest Money Deposit (EMD)
3. Eligible, Technical and Commercial Bids prepared in accordance with the RFP document.
4. Envelope 'A' Eligibility Criteria Response.
5. Envelope 'B' Technical Response
6. Envelope 'C' Commercial Bid.
7. Eligibility, Technical and Commercial Bids prepared in accordance with the RFP document.
8. Copy of this RFP document duly sealed and signed by the authorized signatory on every page and enclosed with Envelope – 'B'.
9. All the pages of Eligibility Criteria Response, Technical Bid and Commercial Bid and any other documents submitted duly sealed and signed by the authorized signatory.
10. All relevant certifications, audit reports, to be enclosed to support claims made in the Bid must be in relevant Envelopes.
11. Prices to be quoted in Indian Rupees (INR).

Table of Contents

Abbreviations and Acronyms

The following abbreviations and acronyms defined in this RFP are as under

SOC – Security Operations Center

AMC – Annual Maintenance Contract

BG – Bank Guarantee

DR – Disaster Recovery

EMD – Earnest Money Deposit

HA – High Availability

IPO – Intellectual Property Owner

IPR – Intellectual Property Rights

NPCI – National Payments Corporation of India

OEM – Original Equipment Manufacturer

RFP – Request for Proposal in Context

PBG – Proforma Bank Guarantee

SI – System Integrator

SME – Subject Matter Expert

WAN – Wide Area Network

CISA – Certified Information Systems Auditor

CISSP – Certified Information Systems Security Professional

CISM – Certified Information Systems Manager

CEH – Certified Ethical Hacker

CRISC – Certified Risk and Information Systems Control

Section 1 – BID Schedule and Address

Sr. No.	Description	Detailed Information
1	Name of Project	Engaging Agency for SOC Services
2	Tender Reference Number	NPCI:RFP:2012-13/0025 dated 16.01.2013
3	Date of release of Bidding Document (Document can be downloaded from NPCI website)	16.01.2013
4	Last date and time of receiving Bidder Pre-bid clarifications in writing	01.02.2013, 6.30 PM
5	Pre Bid Meeting	NO
6	Address for Bid submission	National Payments Corporation of India 13th Floor, R Tech Park, Off Western Express Highway, Nirlon Complex, Near HUB mall , Goregaon-East, Mumbai – 400063
7	Last date and time for Bid Submission	11.02.2013, 3.00PM
8	a) Date and Time of Opening Envelope A & B i.e. Eligibility criteria & Technical Response b) Date and time of opening Envelope C i.e. Commercial Bid	11.02.2013, 3.30 PM Will be intimated later to the eligible & technical qualify Bidders.
9	Place for Eligibility, Technical & Commercial Bid Opening.	National Payments Corporation of India 13th Floor, R Tech Park, Off Western Express Highway, Nirlon Complex, Near HUB mall , Goregaon-East, Mumbai – 400063
10	Name and Address for communication	Head IT Procurement National Payments Corporation of India 13th Floor, R Tech Park, off western express highway, Nirlon Complex, Near HUB mall , Goregaon-East, Mumbai – 400063
11	Bid Related Queries	**Ms. Amit Sahasrabudhe +91 8108108689** Email: amit.sahasrabudhe@npci.org.in **Mr. Vinay Tiwari +91 8108122828** Email: vinay.tiwari@npci.org.in **Mr. Prashant Awale: +91 8108108650** Email:prashant.awale@npci.org.in
12	Bid Cost	Rs 5,618.00 (inclusive of Service Tax @ 12.36%)
13	Bid Security	Rs.2,00,000/-

Note: 1. Bids will be opened in the presence of the Bidders' representatives who choose to attend.
2. Date and Time & address for Commercial Bid Opening will be intimated later to the eligible Bidders.
3. Bid Cost: DD shall be made in favor of "National Payments Corporation of India" of amount Rs Rs.5,618.00 (i.e. Rs.5,000.00 +Service Tax@12.36%) (Non-Refundable) payable at Mumbai.

Section 2 - Introduction

2.1. About NPCI

National Payments Corporation of India (NPCI) is a Company incorporated under Section 25 of the Companies Act, 1956 with its Registered Office in Mumbai, India. NPCI is promoted by 10 banks in India under the aegis of the Indian Banks' Association with majority shareholding by Public Sector Banks.

The 10 promoter banks are State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Bank of India, Union Bank of India, ICICI Bank Ltd, HDFC Bank Ltd, Citibank N.A, and HSBC. The vision, mission and objectives of NPCI are to operate for the benefit of all the Member Banks and the common man at large.

2.2. Objective of this RFP

NPCI has various business verticals to process variety of retail payments prevailing in India today. NPCI has implemented multiple strategic applications that are supporting country's banking & finance industry.
NPCI has implemented state of the art security technologies and has a strong team managing the same. NPCI intends to further strengthen its Information Systems Security by engaging a suitable Security Operations Center (SOC) security partner for managing a world-class, state-of-the-art SOC along with the required processes for its applications and infrastructure.

2.3. Cost of the RFP

The Bidder shall bear all costs associated with the preparation and submission of its bid and NPCI shall, in no case, be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

The Bidders shall submit the bids at NPCI's office on 13th Floor, R Tech Park, Off Western Express Highway, Nirlon Complex, Near HUB Mall, Goregaon-East, Mumbai- 400063, along with non-refundable amount of Rs. 5,618.00 (Inclusive service tax@12.36%) (INR Five thousand six hundred and eighteen only), payable in the form of Demand Draft/Pay order from any scheduled commercial bank in India favouring **"NATIONAL PAYMENTS CORPORATION OF INDIA"** payable at Mumbai in **envelope A**- Eligibility Criteria Response. This RFP document is non-transferable and the cost of RFP documents is non-refundable.

2.4. Due Diligence

The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. Also the grounds for rejection of Bid should not be questioned after the final declaration of the successful Bidder.

The Bidder is requested to carefully examine the RFP documents and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, Bidder should seek necessary clarifications by e-mail as mentioned in Section-1.

2.5. Ownership of this RFP

The content of this RFP is a copy right material of National Payments Corporation of India. No part or material of this RFP document should be published on paper or electronic media without prior written permission from NPCI.

Section 3 - Scope of Work

Security Operations Center (SOC) Services

Service Provider shall supply of skilled manpower for Security Operations Center (SOC) operations over a period of three years at NPCI location as detailed in this section. All Resources should be on the payrolls of the bidder. Service provider shall ensure uptime & availability of SIEM & Security Tools. Service provider resources are expected to deliver SOC services including but not limited to performance monitoring, performance tuning, optimization, and maintenance of SIEM & security tools, also SIEM log backup, troubleshooting, security monitoring, security product management, vulnerability assessment and penetration testing, application security testing and Malware Monitoring. The detailed SOC Reports' formats will be discussed and finalized with L1 bidder.

Note – To avoid conflict of interest the service provider who has implemented the SIEM & Security Tools cannot participate in this RFP.

The selected SOC partner under this RFP will deliver services, as per the following service categories:

3.1. Security Monitoring Services:

This service will help NPCI to monitor for security events throughout its network by analysis of logs from servers, devices and key applications in NPCI. The security monitoring service will have following components:

a. 24X7 log monitoring for identified devices and applications.

b. Rapid response to incidents & forensics.

3.2. Security Product Management:

This service will help NPCI to centralize the management of security products like RSA enVision, ARCON ARCOS, Tripwire, RSA DLP, RSA SecureID and to have tight control on the security rules. Services will also include Security products procured in future. The services will include-

a. Configuration, fault, performance and availability management

b. Co-ordination with internal teams for rule base management

3.3. Vulnerability Management Services:

This service will help NPCI to centrally assess and mitigate the security risks in its network, servers & devices on a continuous basis. The service will include-

a. Set up a baseline security level for NPCI assets.

b. Conduct VAPT and Application Security tests as in when required. Bidder has to provide tools / utilities and skilled resources to conducting them. The bidder's (SOC) team has to provide steps for closure of findings & provide reports on daily basis till closure.

c. Assess the current environment against this baseline on a periodic basis

d. Ensure that the baseline is maintained on an ongoing basis and hence assets are secured against risks.

e. Track the mitigation and coordinate with asset owners for closure of security gaps.

f. The Bidder should perform the Application Security Scans. The team has to report and certify the application go live.

3.4. Malware Monitoring Services:

This service will help Organization mitigate the website related risks on continuous basis. The service will include-

a. 24X7 malware scanning of critical websites

b. Coordinate rapid response

c. Forensics analysis

3.5. SIEM & Security Tools implementation GAP Analysis Services (onetime)

The Bidder should perform gap analysis of the SIEM & Security Tools implementation to ensure it meets best practices and NPCI requirements.

3.6. SOC Skilled Manpower Requirement:

Type of Engineer/ Requirements	**SOC L1 Support Engineers**	**SOC L2 Support Engineers**	**Total**
Mumbai/Hyderabad Location	5	2	7
Skills, Requirements	- B.E. /B.Tech. - Minimum of two years' experience SOC services conducting security device administration & management. - Minimum 1 year in operating a SIEM product and other security tools. - CEH certified Preferred.	- B.E. /B.Tech. - Total 5 Years of experience out of which, minimum 3 years' experience in SOC services conducting security device administration & management and minimum 2 years in SIEM tool & other security tools. - Certification in at least one industry leading SIEM product and other leading certifications in security, such as CISA, CEH, CISSP, CISM, CRISC.	

Please Note: -

1. Exact SOC location i.e. Mumbai or Hyderabad will be decided by NPCI based on the commercial offers.
2. The SOC skilled manpower requirement is for 7 Resources. However, NPCI reserves the right to increase / decrease this number, anytime during the contract period.
3. The Bidder is expected to quote for the supply of manpower for minimum of these 7 Resources for SOC operations. The job descriptions, responsibilities and skill sets are as per this document.
4. The L1 resources are expected to work in three shifts 24 X 7. L2 resources are expected to work in 2 shifts to cover maximum peak business hours.

3.7. Single Point of Contact

The short listed L1 Bidder shall appoint a single point of contact with whom NPCI will deal with for any activity pertaining to the requirements of this RFP.

Section 4 – Eligibility Criteria

4.1. Pre-requisite

The Bidder should possess the requisite experience, resources and capabilities in providing the services necessary to meet the requirements, as described in the tender document. The bidder must also possess the technical know-how and the financial wherewithal that would be required to successfully implement the replication solution and support services sought by NPCI for the entire period of the contract. The Bid must be complete in all respects and should cover the entire scope of work as stipulated in the document. Bidders not meeting the Eligibility Criteria will not be considered for further evaluation.

The invitation to bid is open to all Bidders who qualify the Eligibility Criteria as given below:

4.2. Eligibility Criteria

1. The bidder should be a Company registered under the Companies Act 1956 for the last 3 years.
2. The Bidder should have minimum annual turnover of Rs. 25 Cr. per year in the last 3 financial years i.e. 2009-10, 2010-11 and 2011-12 (or Calendar year 2009, 2010, 2011 or the Bidder's financial years).
3. The Bidder should be a profit (profit after tax) making company in the last financial year i.e. 2011-12 (or Calendar year 2011 or the Bidder's financial year).
4. Bidder should have experience in SOC management for minimum 3 years in servicing banks / financial institutions.
5. Bidder should provide satisfactory performance certificates from two customers to whom the bidder is currently providing SOC services (24*7) for similar requirements, at least 1 year as on 01 January 2013.
6. The Bidder should not be currently blacklisted by any bank / institution in India or abroad.

Failure to provide the desired information and documents may lead to disqualification of the Bidder.

Section 5 – Instruction to Bidders

A The Bidding Document

5.1. RFP

a) RFP shall mean Request for Proposal.
b) Bid, Tender and RFP are interchangeably used to mean the same.
c) The Bidder is expected to examine all instructions, forms, Terms and Conditions and technical specifications in the Bidding Document. Submission of a Bid not responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of its Bid without any further reference to the Bidder.
d) NPCI reserves the right to take any decision with regard to RFP process for addressing any situation which is not explicitly covered in the RFP document.
e) The Bidder must disclose any actual or potential conflict of interest with NPCI.

5.2. Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its Bid, and NPCI will in no case be responsible or liable for those costs.

5.3. Content of Bidding Document

The Bid shall be in one envelope containing 3 separate envelopes, i.e. Envelopes A, B and C. The contents of the Envelopes are given in clause 5.14.

5.4. Clarifications of Bidding Documents

A prospective Bidder requiring any clarification of the Bidding Documents may notify NPCI in writing at NPCI's address or through email any time prior to the deadline for receiving such queries as mentioned in Section 1.

The Bidders shall submit the queries only in the format given below:

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remark (if any)

Replies to all the clarifications, modifications received through mail and email will be posted on NPCI's website. Any modification to the Bidding Documents which may become necessary as a result of such queries shall be made by NPCI by issuing an Addendum, which will be hosted on NPCI's website.

5.5. Amendment of Bidding Documents

At any time prior to the deadline for submission of bids, NPCI, may, for any reason, whether at its own initiative or in response to a clarification requested by a Bidder, amend the Bidding Documents.

Amendments will be provided in the form of Addenda/corrigenda to the Bidding Documents, which will be posted in NPCI's website. Addenda will be binding on Bidders. It will be assumed that the amendments contained in such Addenda/corrigenda had been taken into account by the Bidder in its Bid.

In order to afford Bidders reasonable time in which to take the amendment into account in preparing their bids, NPCI may, at its discretion, extend the deadline for the submission of bids, in which case, the extended deadline will be posted in NPCI's website.

From the date of issue, the Addenda to the tender shall be deemed to form an integral part of the RFP.

B Preparation of Bid

5.6. Bid Price

Prices quoted in the Bid should include all costs including all applicable taxes, duties levies, VAT/Sales Tax/Service Tax, fees etc. whatsoever, except Octroi.

The VAT/Sales Tax/Service Tax should be shown separately in the Price Schedule.

5.7. Earnest Money Deposit (EMD) / Bid Security

The Bidder shall submit Earnest Money Deposit of Rs.2 lakhs (Rupees two lakhs only) in the form of a Demand Draft / Pay order from a scheduled bank in India in favor of "National Payments Corporation of India" payable at Mumbai, or by way of a Bank Guarantee valid for 180 days issued by a scheduled commercial bank as per format in Annexure A1 or A2.

No interest will be paid on the EMD.

5.8. Return of EMD

a) EMDs furnished by all unsuccessful Bidders will be returned on the expiration of the bid validity / finalization of successful Bidder, whichever is earlier.
b) The EMD of successful Bidder shall be returned / refunded after furnishing Performance Bank Guarantee as required in this RFP.

5.9. Forfeiture of EMD

The EMD made by the Bidder will be forfeited if:

a) The Bidder withdraws his Bid before opening of the bids.
b) The Bidder withdraws his Bid after opening of the bids but before Notification of Award.
c) The selected Bidder withdraws his bid / proposal before furnishing Performance Guarantee.
d) The Bidder violates any of the provisions of the RFP up to submission of Performance Bank Guarantee.
e) If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the Bidder turns out to be incorrect and/or conceals or suppresses material information.
f) Failure to accept the order by the Selected Bidder within 7 days from the date of receipt of the Notification of Award / Purchase Order makes the EMD liable for

forfeiture at the discretion of NPCI. However NPCI reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.

g) Failure to submit the Performance Bank Guarantee within the stipulated period makes the EMD liable for forfeiture. In such instance, NPCI at its discretion may cancel the Order placed on the selected bidder without giving any notice.

5.10. Period of Validity of Bids

Bids shall remain valid for a period of 180 days after the date of Bid opening as mentioned in Section 1 or as may be extended from time to time. NPCI holds the right to reject a bid valid for a period shorter than 180 days as non-responsive, without any correspondence.

5.11. Extension of Period of Validity

In exceptional circumstances, prior to expiry of the bid validity period, NPCI may request the Bidders' consent to an extension of the validity period. The request and response shall be made in writing. Extension of validity period by the Bidder should be unconditional and irrevocable. The EMD / Bank Guarantee provided shall also be suitably extended. A Bidder may refuse the request without forfeiting the bid Security.

5.12. Format of Bid

The Bidders shall prepare one hard copy of the entire Bid and one 'soft copy' of the Technical Bid marking it as "Technical Bid – Soft Copy".

5.13. Signing of Bid

The Bid shall be signed by a person or persons duly authorized to sign on behalf of the Bidder.

All pages of the bid, except for printed instruction manuals and specification sheets shall be initialed by the person or persons signing the bid.

The Bid shall contain no interlineations, erasures, or overwriting, except to correct errors made by the Bidder, in which case such corrections shall be initialed by the person or persons signing the Bid.

The Bid shall be signed by a person or persons duly authorized to bind the Bidder to the contract. Such authority shall be either in the form of a written and duly stamped Power of Attorney (Annexure G) or a Board Resolution duly certified by the company's competent authority, extract of which duly certified as true copy should accompany the Bid.

C Submission of Bid

5.14. 3-Envelope Bidding process

The Bid shall be prepared in 3 different envelopes, Envelope A, Envelope B & Envelope C.

Each of the 3 Envelopes shall then be sealed and put into an outer envelope marked as ***'Request for Proposal (RFP) for Engaging Agency for SOC Services.'***

The inner and outer envelopes shall

a) be addressed to NPCI at the address mentioned in Section 1

b) The inner envelopes shall indicate the name and address of the Bidder.
c) If the outer envelope is not sealed and marked as indicated, NPCI will assume no responsibility for the Bid's misplacement or premature opening.

5.15. Contents of the 3 Envelopes

Envelope 'A' should be super scribed as **'Eligibility Criteria'**. The following documents duly placed in a file shall be inserted inside Envelope A:

a) Cost of Bid document in the form of Demand Draft/Pay order drawn in favour of "National Payments Corporation of India" for Rs.5,618. 00 (i.e. Rs. Five thousand six hundred and eighteen only inclusive of Service Tax @ 12.36%)
b) Bid Earnest Money in the form of Demand Draft / Pay Order – Annexure A1.
OR
Bid Earnest Money in the form of Bank Guarantee – Annexure A2.
c) Bid Offer form (without price) – Annexure B.
d) Bidder Information – Annexure C
e) Eligibility Criteria Response Sheet – Annexure D
f) Declaration of Acceptance of Terms and Conditions – Annexure E
g) Declaration of Acceptance of the Scope of Work – Annexure F
h) Power of Attorney or Board Resolution for Signing of Bid – Annexure G
i) Letter of Undertaking – Annexure H
j) Pre-Qualification Bid Letter – Annexure I
k) Declaration Regarding Clean Track by Bidder – Annexure J

l) Last three years audited balanced sheet and profit and loss statements.
m) Satisfactory performance certificates from two customers to whom the bidder is currently providing SOC services.
n) Satisfactory documentation in respect of 7 SOC resources with minimum 5 years' experience with their bio-data and credentials.

Envelope 'B' should be super scribed as **'Technical Bid'**:

The following documents duly placed in a file, shall be inserted inside Envelope B:

a) Technical Specifications– Annexure T
b) Bidders Experience – Annexure T1
c) Client details for Reference– Annexure T2
d) Line item wise Masked Price Bid.
e) RFP document sealed and signed by authorized signatory.

The Technical Bid envelope shall not include any financial information. If the Technical Bid contains any financial information the entire Bid will be rejected.

Envelope 'C' should be super scribed as **'Commercial Bid'**:

a) Commercial Offer Form – Annexure C1
b) Commercial Proposal – Annexure C2

(The commercial proposal should be inclusive of all taxes such as value added tax, sales tax, service tax, excise, duties etc.) Octroi, if applicable, shall be paid at actual against original receipt

5.16. Bid Submission

Bids sealed in accordance with the Instructions to Bidders should be delivered at the address as mentioned in the Section 1.

The offers should be made strictly as per the formats given in the RFP.

5.17. Bid Currency

All prices shall be expressed in Indian Rupees only.

5.18. Bid Language

The Bid shall be in English Language.

5.19. Rejection of Bid

The Bid is liable to be rejected if:

a) The document doesn't bear signature of authorized person.
b) It is received through Telegram/Fax/E-mail.
c) It is received after expiry of the due date and time stipulated for Bid submission.
d) Incomplete/incorrect Bids, including non -submission or non-furnishing of requisite documents / Conditional Bids / Bids not conforming to the terms and conditions stipulated in this Request for Proposal are liable for rejection by NPCI.

No Bid shall be rejected at bid opening, except for late bids.

5.20. Deadline for Submission

The last date of submission of bids is given in Section1, unless amended by NPCI through its website.

5.21. Extension of Deadline for submission of Bid

NPCI may, at its discretion, extend this deadline for submission of bids by amending the Bidding Documents which will be intimated through NPCI website, in which case all rights and obligations of NPCI and Bidders will thereafter be subject to the deadline as extended.

5.22. Late Bid

Bids received after the scheduled time will not be accepted by NPCI under any circumstances. NPCI will not be responsible for any delay due to postal service or any other means.

5.23. Modifications and Withdrawal of Bids

Bids once submitted will be treated, as final and no further correspondence will be entertained on this.

No Bid will be modified after the deadline for submission of bids.

5.24. Right to Reject, Accept/Cancel the bid

NPCI reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever.

NPCI does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender, any time during the tender process, without assigning any reason whatsoever. NPCI also has the right to re-issue the Tender without the Bidders having the right to object to such re-issue.

5.25. RFP Abandonment

NPCI may at its discretion abandon this RFP process any time before Notification of Award or Purchase Order.

5.26. Bid Evaluation Process

The Bid Evaluation will be carried out in 2 stages:

Stage 1 - Envelopes A & B will be evaluated. Only those Bidders who have submitted all the required forms and papers and comply with the eligibility and technical criteria will be considered for further evaluation.

Stage 2 - Envelope C will be evaluated for those Bidders who qualify the Eligibility Criteria and Technical Criteria in Stage 1.

5.27. Contacting NPCI

From the time of bid opening to the time of Contract award, if any Bidder wishes to contact NPCI for seeking any clarification in any matter related to the bid, it should do so in writing by seeking such clarification/s from an authorized person. Any attempt to contact NPCI with a view to canvas for a bid or put any pressure on any official of the NPCI may entail disqualification of the concerned Bidder or his Bid.

Section 6 – Bid Opening

6.1. Opening of Bids

Bids will be opened in 2 stages:

a. Stage 1 – In stage 1 only Envelopes A & B will be opened
b. Stage 2 – In stage 2 only Envelope C will be opened

6.2. Stage 1 - Opening of Envelopes A & B

NPCI will open Envelopes 'A' & 'B' in the presence of Bidders' representative(s) who choose to be present on the date, time and address mentioned in Section 1 or as amended by NPCI from time to time.

The representatives of the Bidders have to produce an authorization letter / identity card from the Bidders by way of letter or email to represent them at the time of opening of bids. Only one representative will be allowed to represent each Bidder. In case the Bidders' representatives are not present at the time of opening of Bids, the Bids will still be opened at the scheduled time at the sole discretion of NPCI.

The Bidders' representatives who are present shall sign the register evidencing their attendance. In the event of the specified date of bid opening being declared a holiday for NPCI, the bids shall be opened at the appointed time and place on next working day.

Only those Bids which meet eligibility and technical criteria will qualify for commercial evaluation.

6.3. Stage 2 - Opening of Envelope C

Those Bidders who meet the eligibility criteria and technical criteria will be intimated by email, the date, time and address for opening of the Commercial Bids.

The representatives of the Bidder have to produce an authorization letter from the Bidders by way of letter or email to represent them at the time of opening of bids. Only one representative will be allowed to represent each Bidder. In case the Bidders' representatives are not present at the time of opening of Bids, the Bids will still be opened at the scheduled time at the sole discretion of NPCI.

The Bidders' representatives who are present shall sign the register evidencing their attendance. In the event of the specified date of Bid opening being declared a holiday for NPCI, the Bids shall be opened at the appointed time and place on next working day.

Section 7 – Bid Evaluation

7.1. Preliminary Examination of Bids

The evaluation process would consider whether the bidder has requisite prior experience and expertise to address NPCI's requirements and objectives. NPCI will examine the bids to determine whether they are complete, whether required information has been provided as underlined in the Bid document, whether the documents have been properly signed, and whether bids are generally in order.

Eligibility and compliance to all the forms and Annexure would be the next level of evaluation. Only those Bids which comply to the Eligibility Criteria will be taken up for further technical evaluation.

NPCI may waive any minor informality, non-conformity or irregularity in the Bid that does not constitute a material deviation provided such waiver does not prejudice or affect the relative ranking of any Bidder.

To assist in the examination, evaluation and comparison of bids NPCI may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the Bid shall be sought, offered or permitted.

Written replies submitted in response to the clarifications sought by NPCI, if any, will be reviewed.

NPCI may interact with the Customer references submitted by Bidder, if required.

If a Bid is not substantially responsive, it will be rejected by NPCI and may not subsequently be made responsive by the Bidder by correction of the nonconformity. NPCI's determination of bid responsiveness will be based on the content of the bid itself.

Evaluation of Technical Bids

The Technical Evaluation will be based on the following broad parameters:

a) Compliance to Scope of Work (requirements) as specified in the RFP.
b) To assist in the examination, evaluation and comparison of bids NPCI may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.
c) Written replies submitted in response to the clarifications sought by NPCI, if any, will be reviewed.
d) Presentations on the skills, services provided etc., from the short-listed Bidders. Such presentations will become part of the technical evaluation.
e) NPCI may interact with the Customer references submitted by bidder, if required.
f) Documentary evidence for the scope of work already executed by the bidder.
g) The bidder should have experienced and skilled professionals having certifications (e.g. BCCP, CBCP, CISA, CISSP, and CISM) to carry out SOC Operations at NPCI. Comparison of Skilled resources will be done based on the no. of resources with desired certifications.

Technical Evaluation Scoring Matrix:

Sr. No.	Description	Marks
1	Customer references provided	10
2	Bidders credentials	10
3	Experience and past performance on similar contracts	10
4	Product Expertise (RSA enVision and Security Tools)	20
5	Compliance to Technical Requirement As mentioned in Section - 9	50
	Total Marks for Technical Evaluation	**100**

Technical Specifications Compliance Matrix is given in Annexure – T.

Bidders scoring equal to or more than 70% will qualify for Commercial Bid opening.

7.2. Evaluation of Commercial Bids

7.2.1 Commercial bids of only the Bidders who have cleared the technical evaluation will be opened and evaluated.

7.2.2 Arithmetic errors in the Bids submitted shall be treated as follows:

a) Where there is a discrepancy between the amounts in figures and in words, the amount in words shall govern; and
b) Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of the NPCI, there is obviously a gross error such as a misplacement of a decimal point, in which case the line item total will govern.
c) Where there is a discrepancy between the amount mentioned in the bid and the line item total present in the Commercial Bid, the amount obtained on totaling the line items in the Commercial Bid will govern.

7.3. Successful Evaluated Bidder

After completing internal approval process, Bidder whose Bid Price is the lowest will be declared as successful evaluated bidder who will be called L1 Bidder.

Section 8 – Terms and Conditions

8.1. Definitions

"Contract" means the Contract Agreement entered into between NPCI and the Bidder.

"Contract Period" means the period mentioned in the Contract.

"Contract Price" means the price or prices arrived at which will form the Contract Agreement.

"Intellectual Property Rights (IPR)" means any and all copyright, moral rights, trademark, patent and other intellectual and proprietary rights, title and interests worldwide whether vested contingent, or future, including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from extract or re-utilize data from, manufacture, introduce into circulation, publish, enter into computer memory, otherwise use any portion or copy in whole or in part, in any form, directly or indirectly, or authorize or assign others to do so.

"Bidders" means bidder selected through this RFP process.

"Project" means the entire scope of work as defined in the RFP.

8.2. Notification of Award or Purchase Order

After selection of the L1 Bidder and after obtaining internal approvals and prior to expiration of the period of Bid validity, NPCI will send Notification of Award or Purchase Order to the selected Bidder.

Upon the successful Bidder accepting the Purchase Order and signing the contract and NDA, NPCI will promptly notify each unsuccessful Bidder and will discharge all remaining EMDs, if any.

8.3. Award of contract

NPCI will award the Contract to the successful Bidder after the completion of NPCI's internal procedure who has been determined to qualify to perform the Contract satisfactorily, and whose bid has been determined to be responsive, and is the lowest evaluated Bid.

8.4. Term of Contract

Initially, the contract shall be for the period of 3 years from the date of commencement of the engagement and renewable on annual basis. Renewal of the engagement would inter-alia, be based on the quality of SOC services provided, which would be reviewed every 6 months.

8.5. Signing or Acceptance of Contract

The successful Bidder shall accept the Notification of Award or Purchase Order within 5 days of receipt of the same. Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award.

8.6. Contract Amendments

No variation in or modifications of the terms of the contract shall be made except by the written amendments signed by the parties.

8.7. Performance Bank Guarantee

Performance Bank Guarantee shall be equal to 10 % of the PO value valid for the contract period of the PO. Successful Bidder will submit Performance Bank Guarantee as per NPCI format attached vide Annexure-K hereto, within 14 days of receipt of the Notification of Award or Purchase Order. Upon the receipt of Performance Bank Guarantee, NPCI will discharge EMD of the Successful Bidder.

8.8. Taxes and Duties

All taxes deductible at source, if any, at the time of release of payments, shall be deducted at source as per then prevailing rates while making any payment.

Commercial Bid should be inclusive of all taxes, duties, charges and levies of State or Central Governments as applicable, VAT/Sales Tax/Service Tax, insurance, service taxes etc. Octroi, if applicable shall be paid extra at actual against original Octroi receipt.

The benefits realized by the Bidder due to lower rates of taxes, duties, charges and levies shall be passed on by the selected Bidder to NPCI.

8.9. Delivery Schedule:

The services should start within 1 week from the date of Notification of Award of Contract or Purchase Order.

8.10. Penalty for Default in Delivery

In case the SOC services not provided within 1 week from the date of Notification of Award of Contract or Purchase Order, penalty would be imposed at a rate of INR 5000/- for every week of delay, subject to a maximum penalty of Rs 25,000.00. If the SOC services are not provided even after five weeks from the date of Notification of Award of Contract or Purchase Order, the Notification of Award of Contract or Purchase Order is liable to be cancelled at the option of NPCI.

8.11. Service Level

SOC services should be available for 24x7 operations. Onsite L1 support should be in three shifts covering 24x7 & L2 support should be in two shifts to cover maximum peak business hours. Offsite support shall be covering the period where the onsite engineer escalates for more help to resolve issues, if any. (For more details refer scope of work)

Service level required by NPCI is detailed in section 9 – Technical Specification of this RFP. In case of default, relevant penalty clause will be applicable for deficiency of service level percentage.

8.12. Payment Terms

Payment shall be released against monthly invoice submitted in arrears for actual resource deployed suitably attested by NPCI officials. Bidder has to provide proper substitute resource during the leave vacancy of the resource deployed. Pro-rata deduction would be made for the period of absence of the resource / substitute resource. The penalty amount will be deducted for deficiency in service levels if any for the relevant month.

8.13. Price

Price shall remain fixed during the contract period. There shall be no increase in price for any reason whatsoever. Therefore no request for any escalation of the cost / price shall be entertained.

8.14. Extension of Purchase Order & Repeat order

The term of this Contract shall be initially for a period of three years from the date of providing of SOC Services and acceptance of the same by NPCI. NPCI reserves the right to extend the contract by every year subsequently. NPCI has also right to place repeat order to the Bidder for any resources mentioned in this Purchase Order.

8.15. Confidentiality

The Bidder shall (whether or not he submits the tender) treat the details of the documents as secret and confidential. The Successful Bidder shall execute separate NDA on the lines of the draft provided in Annexure L hereof.

8.16. Legal Compliances:

8.16.1. The Bidder confirms to NPCI that its personnel/ employees/staff are covered under the provision of various Acts enacted for the protection and benefits of workmen /employees /staff or otherwise such as Employees State Insurance Act and Employees Provident Fund Miscellaneous Provision Act etc. and such other Acts like Profession Tax Act etc. as applicable and that Bidder is duly registered under the provisions of the said Acts and is complying with the provisions of the Acts.

8.16.2. The Bidder shall allow NPCI as well as regulatory authorities to verify books in so far as they relate to compliance with the provisions of these Acts and shall provide on demand by NPCI & regulatory authorities such documentary proof as may be necessary to confirm compliance in this regard. NPCI shall not be responsible in any event to the employees of Bidder for any of their outstanding claims or liability in that regard. NPCI shall not be responsible for any claim or demand made by such personnel for their dues outstanding against Bidder.

8.17. Compliance of Labour and other Law:

The Bidder shall comply with all the statutory requirements as are applicable from time to time and shall be solely responsible for fulfilment of all legal obligations under various statutes including Contract Labour (Regulation and Abolition) Act 1970, Minimum Wages Act, Workmen Compensation Act, EPF & Miscellaneous Provisions Act, Shop and Establishment Act etc. Bidder shall keep NPCI indemnified against any dues/compensation or any other liability of any nature whatsoever due to non-fulfilment of any of the statutory provision under any statute/byelaws/ notification etc. including industrial laws. NPCI shall have full right to recover any claim and liability incurred towards payment of any dues, compensation or cost from Bidder and deducts it from its outstanding subsequent bills.

8.18. Replacement of Resource(s)

NPCI shall consider at its sole judgment that the Resource(s) provided by Bidder as unsuitable for the job for whatsoever reason, NPCI shall have the option either (1) to terminate the

Purchase Order in part or as a whole or (2) to request Bidder for prompt replacement within 15 days at its cost.

In case any key resource wants to leave from service then Bidder shall take proper handover from the candidate before leaving the job so that NPCI operations shall not be affected.

8.19. Intellectual Property Rights:

All rights, title and interest of NPCI in and to the trade names, trademark, service marks, logos, products, copy rights and other intellectual property rights shall remain the exclusive property of NPCI and Bidder shall not be entitled to use the same without the express prior written consent of NPCI. Nothing in contract including any discoveries, improvements or inventions made upon with/by the use of the Bidder or its respectively employed resources pursuant to contract shall neither vest nor shall be construed so that to vest any proprietary rights to the Bidder. Notwithstanding, anything contained in Contract, this clause shall survive indefinitely, even after termination of this Purchase Order.

8.20. Statutory Compliance:

Bidder shall comply and ensure strict compliance by his employees and agents of all applicable Central, State, Municipal and Local laws and Regulations and undertake to indemnify NPCI from and against all levies, damages, penalties and payments whatsoever as may be imposed by reason of any breach or violation of any law, rule, including but not limited to the claims against NPCI under Workmen Compensation Act, 1923, The Employees Provident Fund Act, 1952, The Purchase Order Labour (Abolition and Regulation) Act 1970, Factories Act, 1948, Minimum Wages Act and Regulations, etc. Shop and Establishment Act and any Labour Laws which would be amended/modified or any new act if it comes in force whatsoever, and all actions claim and demand arising therefrom and/or related thereto.

Bidder shall ensure to keep and maintain all the statutory registers, records as required under provisions of contract of Labour(R&A) Act,1970, Minimum Wages Act and the rules made thereunder, Employees Provident Fund Act, 1952 and keep the same available for inspection by NPCI and Government Authorities.

8.21. Facilities Provided by NPCI:

NPCI shall provide seats, with required facilities like desktop/laptop, internet, intranet & LAN Connectivity free of cost for official work. These facilities shall not be used for any personal use. In case of any misuse of the facilities, penalty as deemed fit shall be imposed and recovered from the pending bills of Bidder.

8.22. No Damage of NPCI Property

Bidder shall ensure that there is no loss or damage to the property of NPCI while executing the Contract. In case, it is found that there is any such loss/damage due to direct negligence/non-performance of duty by any personnel, the amount of loss/damage so fixed by NPCI shall be recovered from Bidder.

8.23. Indemnity

The Bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from

a) an act of omission or commission of the Bidder, its employees, its agents, or employees of its sub-contractors in the performance of the services provided by this Agreement,
b) breach of any of the terms of this Agreement or breach of any representation or warranty or false statement or false representation or inaccurate statement or assurance or covenant by the Bidder,
c) bonafide use of the deliverables and or services provided by the Bidder,
d) misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfill the scope of this project,
e) claims made by the employees, sub-contractor, sub-contractor's employees, who are deployed by the Bidder, under this Agreement,
f) breach of confidentiality obligations of the Bidder,
g) gross negligence or gross misconduct solely attributable to the Bidder or by any agency, contractor, subcontractor or any of their employees by the bidder for the purpose of any or all of the obligations under this Agreement.

The Bidder shall further indemnify NPCI against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on NPCI for malfunctioning of the equipment or software or deliverables at all points of time, provided however, NPCI notifies the Bidder in writing immediately on being aware of such claim, and the Bidder has sole control of defense and all related settlement negotiations.

Bidder shall be responsible for any loss of data, loss of life, etc, due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc, as such liabilities pose significant risk.

The Bidder shall indemnify NPCI (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:

a) Non-compliance of the Bidder with Laws / Governmental Requirements.
b) Intellectual Property infringement or misappropriation.
c) Negligence and misconduct of the Bidder, its employees, sub-contractor and agents.
d) Breach of any terms of Agreement, Representation or Warranty.
e) Act of omission or commission in performance of service.
f) Loss of data.

Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by NPCI arising out of claims made by its customers and/or regulatory authorities.

Bidder shall indemnify, protect and save NPCI against all claims, losses, costs, damages, expenses, action, suits and other proceedings, resulting from misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc., or such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act 2000 in respect of all the hardware, software and network equipment or other systems supplied by them to NPCI from whatsoever source, provided NPCI notifies the Bidder in writing as soon as practicable when NPCI becomes aware of the claim however,

a) the Bidder has sole control of the defense and all related settlement negotiations
b) NPCI provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and

c) NPCI does not make any statements or comments or representations about the claim without the prior written consent of the Bidder, except where NPCI is required by any authority/ regulator to make a comment / statement/ representation. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect, consequential and incidental damages and compensations. However indemnity would cover damages, loss or liabilities suffered by NPCI arising out of claims made by its customers and/or regulatory authorities.

8.24. Bidder's Liability

The selected Bidder will be liable for all the deliverables.

The Bidder's aggregate liability in connection with obligations undertaken as part of the Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract.

Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by NPCI arising out of claims made by its customers and/or regulatory authorities.

8.25. Liquidated Damages

Due to negligent act of the Bidder, if NPCI suffers losses, and incurs damages, the quantification of which may be difficult, the amount specified hereunder shall be construed as reasonable estimate of the damages and the Bidder shall agree to pay such liquidated damages as defined hereunder:

The total amount of liquidated damages under this Contract shall not exceed 5% of the total value of the contract.

8.26. Fraudulent and Corrupt Practice

a) "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of the project and includes collusive practice among Bidders (prior to or after bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the NPCI of the benefits of free and open competition.
b) "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressuring to influence the action of a public official in the process of project execution.
c) NPCI will reject a proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for or in executing the project.

8.27. Force Majeure

Notwithstanding the provisions of the RFP, the successful bidder or NPCI shall not be liable for penalty or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. For purposes of this clause, "Force Majeure" means an event beyond the control of the bidder and not involving NPCI or bidder's fault or negligence and not foreseeable. Such events may include, but not restricted to wars, revolutions, epidemics, natural disasters etc.

If force majeure situation arises, the bidder shall promptly notify NPCI in writing of such condition and cause thereof. Unless otherwise directed by NPCI in writing, the Bidder shall continue to perform its obligations under contract as far as possible.

8.28. Purchase Order cancellation

NPCI reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to NPCI alone;

a. Serious discrepancy observed during performance as per the scope of project

b. If the Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the Bidder/Bidder turns out to be incorrect and/or conceals or suppresses material information.

In case of order cancellation, any payments made by NPCI to the Bidder would necessarily have to be returned to NPCI with interest @15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the contract and any additional expenditure to be incurred by NPCI to appoint any other Bidder. This is after repaying the original amount paid.

8.29. Termination of Contract

a. **For Convenience**: NPCI by written notice sent to Bidder may terminate the contract in whole or in part at any time for its convenience giving one months prior notice. The notice of termination shall specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective
b. **For Insolvency**: NPCI may at any time terminate the contract by giving written notice to Bidder, if Bidder becomes bankrupt or insolvent. In this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to NPCI.
c. **For Non-Performance:** NPCI reserves its right to terminate the contract in the event of Bidder's repeated failures (say more than 3 occasions in a calendar year to maintain the service level prescribed by NPCI.

8.30. Resolution of Disputes

All disputes or differences between NPCI and the Bidder shall be settled amicably. If, however, the parties are not able to resolve them, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

NPCI and the Bidder shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the Contract.

If, NPCI and the Bidder find themselves unable to resolve amicably a Contract dispute even after a reasonably long period, either party may require that the dispute be referred for resolution to the formal mechanisms specified herein below. These mechanisms may include, but are not restricted to, conciliation, arbitration/ mediation by a third party and/or adjudication in an agreed national forum.

The dispute resolution mechanism to be applied shall be as follows:

a) In case of Dispute or difference arising between NPCI and the Bidder relating to any matter arising out of or connected with the agreement to be executed later, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. Arbitration proceedings shall be held at Mumbai, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English; In case of Dispute or difference arising between NPCI and the Supplier relating to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act,1996. Where the value of the Contract is above Rs.1.00 Crore, the arbitral tribunal shall consist of 3 arbitrators, one each to be appointed by NPCI and the Supplier. The third Arbitrator shall be chosen by mutual discussion between NPCI and the Supplier

b) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the arbitral tribunal. However, the expenses incurred by each party in connection with the preparation, presentation, etc., of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself; and

c) Where the value of the contract is Rs.1.00 Crore and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator should be appointed by agreement between the parties.

8.31. Governing Law

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

8.32. Applicable Law

The Contract to be executed between NPCI and successful Bidder shall be interpreted in accordance with the laws of the Union of India and the Bidder shall agree to submit to the courts under whose exclusive jurisdiction the Registered Office of NPCI falls.

8.33. Addresses for Notices

Following shall be address of NPCI and Bidder

NPCI address for notice purpose:

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises, Bandra-Kurla Complex, Bandra,
Mumbai – 400 051.

(Bidder’s address for notice purpose :(To be filled by the Bidder)

Section 9 – Detailed Technical Specification

9.1. Security Monitoring Services

Bidder should provide services for 24x7 remote monitoring of Operating systems, web servers, databases, network devices, security devices and business applications. The services will include review of the logs generated from servers and applications in real time to detect suspicious activities and potential attacks. Immediate response action will need to be initiated by the Bidder to stop the attacks. Bidder will provide the services using the SIEM platform procured by NPCI and through its dedicated personnel & processes based out of the Security Operations center of NPCI. The onsite team should be supported for various services by the Bidder's SOC or backend team as required.

The scope of services and its specification are given below.- Bidder proposals should include description of its process & methodology to offer these services, sample service output (log baselines, report formats), experience with similar environments and resume of skilled personnel who will be allocated towards this service.

9.1.1 Asset Scope

The assets configured and included in SIEM & Security Tools are those will be in the scope for security monitoring.

Bidder has to ensure that the services provided by it for security monitoring covers the above assets as per the service specification, deliverables and SLA described in the following section.

9.1.2 Service Specification

The security monitoring service to be provided by the Bidder should meet the following specifications.

#	Requirements
1.	Bidder should monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in NPCI environment. Monitoring should be done on 24/7 basis with onsite personnel. Bidder should provide the personnel for managing the security monitoring service as per the team specifications in scope of work.
2.	Bidder should develop, update and maintain log baselines for all platforms at NPCI that are required to be monitored.
3.	Bidder should coordinate with IT operations to implement and maintain the log baselines on production systems
4.	Bidder should detect both internal & external attacks. In addition to security attacks on IT infrastructure, Bidders should also monitor for security events on business applications, databases and also identify network behavior anomalies.

#	Requirements
5.	Bidder should monitor, detect and manage incidents for the following minimum set of IT infrastructure security events. This is indicative minimum list and is not a comprehensive/complete set of events. Bidders should indicate their event list in proposal response. Buffer Overflow attacks Port & vulnerability Scans Password cracking Worm/virus outbreak File access failures Unauthorized server/service restarts Unauthorized changes to firewall rules Unauthorized Bidder access to systems SQL injection Cross site scripting
6.	Bidder operations team at NPCI should send alerts with details of mitigation steps to designated personnel within NPCI and any identified service provider of NPCI.
7.	Bidder should provide coordinated rapid response to any security incident. Bidder should contain attack & coordinate restoration of services. While Bidder personnel will enlist support of other departments and service providers in NPCI, primary responsibility for incident response will be with the Bidder.
8.	Bidder should maintain a knowledge base of alerts, incidents and mitigation steps and this knowledge base should be updated with evolving security events within and outside NPCI. Team should send customized alerts advisories to respected teams in NPCI.
9.	Evidence for any security incident should be maintained in tamper proof manner and should be made available for legal and regulatory purposes, as required.
10.	Bidder should add/delete/modify rules, reports and dashboards based on NPCI requirements
11.	Bidder should provide MIS reports to NPCI on daily, weekly and monthly basis. Reporting requirements will be finalized with the selected Bidder. Bidder should also have the provision to provide reports on demand whenever required by NPCI.
12.	Bidder should conduct forensic analysis for security incidents to enable identification of perpetrators and their methodologies.
13.	Bidder should do root cause analysis for security incidents and coordinate implementation of controls to prevent recurrence.
14.	Bidder should carry out system administration tasks including regular backup of system, restoration, installation, health check and others

#	Requirements
15.	Bidder should manage any faults in the SIEM solution by trouble shooting and coordinating with the OEM/principle
16.	Bidder team Analyst(s) and program manager are responsible for managing the security monitoring team and ensuring satisfactory performance
17.	All deliverables including reports should undergo Quality Assurance process. Bidder team lead should define quality metrics, measurement frequency and reporting periodicity in consultation with NPCI
18.	Analyst should review reports, operating procedures, administrative activities on a daily basis to identify quality issues
19.	Analyst should submit periodic Quality Assurance reports to NPCI as per the reporting frequency designed.
20.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include 1. Managing escalations from onsite team for detection & response to new threats & complex attacks that onsite team is unable to resolve. 2. For adding new/updated threat scenarios and other best practices in NPCI's SIEM tool for detection & response based on Bidder SOC visibility & experience across other customers. 3. Forensic analysis of attacks/incidents including making available specialists, domain experts, tools.
21.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.
22.	Bidder should provide a proactive solution to identify problems.

#	Requirements
23.	Bidder should provide incident tracking and management solution, which: - Should have the feature to Log Problems. - Categorization and Prioritization of problems should be possible. - Should have feature to auto assign Tickets. - Should have facility to assign tickets based on policy and workflow rules and should have at least 5 escalation levels. - Should have a feature to cascade and Organize rules. - Users/technicians must be notified for pending requests. It should have the feature to create rules for such notifications - Should be possible to send personalized E-mails to users - Should be possible to send notification emails to the requester - Should Converge all IT help desks in your business units across buildings/complexes or countries, to function as a single help desk. - Should customize the holidays, departments, technicians /site associations, groups, business rules and SLA's as per the location's operational hours - Should Enables the requests logged in from each site to be resolved within that particular site's operational hours. - Automatically reset the end-users password without the involvement of helpdesk technicians. - - Support integration with LDAP and Active Directory

9.1.3 Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA
1.	Event monitoring	24X7 monitoring for identified assets and 24X7 response for any events Detection of internal & external attacks, suspicious events or abnormal behaviour against pre-defined baseline for network, applications and databases Recommend mitigation steps for alerts Alert categories and their prioritization and reporting format as per mutually approved process & escalation matrix	Sending alerts with mitigation steps to designated personnel: 15 min: Very high priority events 30 min: High priority events 60 min: Medium priority events Alerting method: Email/SMS/Call: Very high priority events

#	Area	Expected Output	SLA
			Email/SMS: High priority events Email: Medium Priority events
2.	Incident Management & Forensics	Coordinated rapid response to any security incident Contain attack & restore services Forensic analysis & report Root cause analysis report and long term security control identification Evidence collection and retention for legal and regulatory purpose Log retention and repository of incident knowledge base	Providing initial response to incidents: 60 min: Very high priority incidents 90 min: High priority incidents 120 min: Medium priority incidents Providing report with root cause analysis: 72 hours: Very high priority incidents 96 hours: High priority incidents 120 hours: Medium priority incidents Availability of logs relevant to reported events/ incidents for the period of: 12 months Retention of all logs for a period of one year Repository of incidents and mitigation knowledgebase
3.	Reports	Timely submission of daily, weekly and monthly reports Multiple types of reports, an indicative list is given below:- Daily reports including firewall change reconciliation, unauthorized database admin access, referrer log brand misuse reports, anti-virus policy non-compliance, unauthorized service provider access, privilege misuse/escalation Weekly reports including persistent	Daily Reports: By 12:00 PM Weekly Reports: By 10:00 AM : Monday Monthly Reports:

#	Area	Expected Output	SLA
		top attackers, attacks, attack targets, trend analysis Monthly MIS reports, executive representation for top management, trend analysis Reports as defined by NPCI from time to time.	By 5th of each month

9.2. Security Product Management

Bidder should manage security products from NPCI SOC. The product that needs to be covered include: RSA enVision, ARCON ARCOS, Tripwire, RSA DLP, RSA SecureID and any new product procured. Bidder should configure policies, manage backup/restore, manage faults and monitor performance of these products. The Bidder team should be dedicated for the same with team structure as described in the table for operations team structure in this section. The onsite team should be supported for various services by the Bidder's SOC or backend team as required.

Bidder should bring the required processes & methodologies for security product management as per the scope and service specifications given below. Bidder proposals should capture process & methodology to offer these services, sample service output (product configuration baselines, report formats), experience with similar environments and resume of skilled personnel who will be allocated towards this service.

9.2.1 Asset Scope

Please refer Section **9.1.1**.

9.2.2 Service Specification

The security device management service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	**Requirement**
1.	Management of products in scope for policies, configurations, availability, fault and capacity management during business hours
2.	Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to NPCI on a regular basis
3.	Reviews SLA's with OEM /product support and recommend measures to improve the service levels.
4.	Maintain IP addressing schemes, routing information, routing tables for security device operations

#	Requirement
5.	Provide recommendations for architecture enhancements/changes that can enhance the security posture
6.	management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
7.	Provide NPCI with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
8.	Coordinate delivery with all stake holders including help desks, network team, IT team, application team and all appropriate third parties, as necessary, for the management of products in asset scope
9.	Maintain security product configuration, based on industry best practices and as requested, for the products within the Asset Scope
10.	Maintain complete documentation and architecture layout for all products with site deployment layout
11.	Participate in technical and business planning sessions to establish security standards, architecture and project initiatives where the security products may impact or improvise the design
12.	Provide infrastructure security planning & analysis, recommendations for installation and upgrade of products in scope
13.	Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope
14.	Bidder should analyze performance reports and formulate plan for capacity addition
15.	Provide technical expertise/support for audits on the products in scope
16.	Set up and manage admin and user accounts. Perform access control on need basis
17.	Take the backup of product configuration files any time there is a change in device configuration
18.	Review the backup configuration and business continuity procedures to be followed in the event of device failure
19.	Submit the Periodic Reports on the backup status
20.	Restore configuration in the event of product crash, corruption or other failure
21.	Design and program manage new device implementations
22.	Bidder should provide backend support to the onsite team from its own SOC. Such

#	Requirement
	support at the minimum include • Escalations from onsite team for specialist support on security product categories to resolve faults, configuration related issues • Share best practices on product configuration standards & policies with onsite team
23.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.
24.	The following activities has to be carried out specifically for the DLP system in scope: 1. Identify the sensitive data that needs to be protected by DLP in discussion with NPCI. 2. Discover sensitive data by periodically scanning servers and endpoints of NPCI. 3. Design, configure and fine tune DLP policies to protect sensitive data in accordance with NPCI requirements. 4. Design and configure DLP reports and dashboard. 5. Generate daily, weekly, monthly DLP reports as required. 6. Monitor and analyze DLP alerts and perform incident management.
25.	The following activities has to be carried out specifically for the PIM solution in scope: 1. Conduct role engineering to design the access policies for servers and network devices 2. Configure and fine tune access policies for servers and network devices 3. Configure end user accounts and associated access policies and manage their privileges 4. Design and configure PIM reports and dashboard 5. Generate daily, weekly, monthly PIM reports as required 6. Monitor and analyze PIM alerts and perform incident management Analyze PIM recordings for incident analysis
26.	The following activities has to be carried out specifically for the FIM solution in scope: 1. Identify the files to be monitored across servers/network devices based on best practices, regulatory/standards requirements and NPCI requirements. 2. Identify configuration audit requirements 3. Design, configure and fine tune the FIM and Configuration audit policies for the identified files and configuration items to be monitored. 4. Design and configure FIM reports and dashboard. 5. Generate daily, weekly, monthly FIM reports as required. 6. Monitor and analyze FIM alerts and perform incident management.
27.	Create or migrate users from LDAP/ User repository to the Two factor authentication server

#	Requirement
28.	Carry out token life-cycle management procedures such as 1. User Token provisioning procedure 2. Modification of two-factor authentication privileges for end user owing to change in job role 3. Token revocation on exit or termination Carry out Help desk procedures such as 1. Reporting lost tokens 2. Returning faulty, damaged or expired tokens 3. Enabling emergency access for permanently lost, damaged or expired tokens 4. Inventory management

9.2.3 Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA
1.	Architecture planning, review & redesign (as required from time to time)	1. Plan & review placement of servers in the network segments 2. Plan & review Device segmentation 3. Plan & review authentication schemes 4. Plan & review integration with other security components 5. Oversight for new device implementation	Completion of activities within mutually agreed upon timelines
2.	Policy & user Management	1. Risk Analysis and policy design 2. Configuration of polices 3. Document policy change 4. Policy optimization for all the Devices 5. Audit policy for exceptions 6. Set up and manage admin and user accounts as per policies of NPCI 7. Interact with network team for managing escalations with NOC	Emergency Changes: ▪ 30 min: Acknowledgement of change request ▪ 60 min: Implementation of change requests Routine Changes: ▪ 4 hours: Acknowledgement of change requests ▪ 8 hours: Implementation of change requests

3.	Availability and Configuration Management	1. Backup & restoration of configuration 2. Periodic review the backup configuration and business continuity procedures to be followed in the event of Device failure 3. Monitor the availability of devices 4. Root cause analysis for failure/ downtime of security devices 5. Maintain IP addressing schemes, routing information, routing tables, for the Device operations 6. Detailed analysis of miss-configurations, OS/application failures 7. Comply with NPCI policies & regulations applicable to NPCI 8. Tracking the SLA with product Bidder or reseller, maintenance contract, required license, software subscription for all hardware & software components of Devices.	• Periodic Backup as per NPCI's policy • Backup before and after implementation of any change • Quarterly report on maintenance contract & software subscription
4.	Fault Management	1. Open a case with device supplier in the event of hardware component or system failure or bugs 2. Co-ordinate with device supplier/OEM for solution 3. Review the device supplier/OEM SLA for recommending measures to improve the service levels 4. Track AMC renewal dates 5. Root cause analysis for any failures / downtimes	- Open a ticket within 30 minutes of problem identification - Status update every 4 hours to NPCI personnel - Quarterly review of Bidder SLA
5.	Device	1. Prepare and review capacity plans for security devices and	- Quarterly analysis report as

	migration/update	recommend upgrades as required. 2. Provide security infrastructure analysis, recommendations for installation and upgrade 3. Prepare specifications, architecture and detailed plan for migration/upgrade 4. Test migration/upgrade plan in staging environment	per NPCI's specified format - Version upgrades within 3 months from release of new version

9.3. Vulnerability Management Services

Vulnerabilities in an asset, including missing patches and insecure configuration, can lead to security compromises. NPCI plans to set up a strong vulnerability management process that is centralized and continuous for assessing security gaps across its IT infrastructure.

Under vulnerability management plan, NPCI requires risk based vulnerability scanning and secure configuration assessments. The frequency and depth of scan and assessments will be determined by the asset criticality and its risk exposure. NPCI requires the Bidder to execute vulnerability assessments both scanning & configuration assessments, as per the scope given below, from the NPCI's SOC. Bidder should deploy its team processes and methodologies at NPCI's SOC for carrying out the activities. The Bidder team should be dedicated for the same with team structure as described in the table for operations team structure in this section. The onsite team should be supported for various services by the Bidder's SOC or backend team as required.

Bidder proposals should capture process & methodology to offer these services, sample service output (baselines, report formats), experience with similar environments and resume of skilled personnel who will be allocated towards this service.

9.3.1 Asset Scope

All the present and future application platforms of NPCI are in scope for scanning & configuration assessment.

9.3.2 Service Specification

The Vulnerability management service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	Requirements
1.	Bidder should conduct scanning & configuration assessments as per frequency defined in the asset scope table
2.	Configuration assessments should check for compliance against the secure baseline and SANS, NIST, CIS, NPCI baselines, CERT-IN, RBI guidelines as updated from time to time.

#	Requirements
3.	Configuration assessment of OS should check for the items given below. This is a minimum indicative list and Bidders are encouraged to check for more settings in line with best practices (SANS, NIST, CIS, NPCI baselines, CERT-IN, RBI): - Shares with insecure permission - Permissions to critical system files and folders - Audit log settings - Space allocated for Event Viewer logs - SNMP community strings - Password and account lockout policies - Non-essential services check - TCP/IP stack settings - User rights assignment - Latest Service Pack installation - Latest security patches installation - Antivirus software
4.	Configuration assessment of database should check for the items given below. This is a minimum indicative list, Bidders are encouraged to check for more settings in line with best practices(SANS, NIST, CIS, NPCI policies, CERT-IN, RBI) - Default passwords - DBLINK Encrypt Login Option - Allocation of Unlimited Table space - Temporary and Default Table space Management - Unrestricted access to services - Web based access to database using iSQL * Plus - Run time modification of the listener service - Look for latest version - Test for secure authentication mechanism - Latest version not installed
5.	Configuration assessment of network & security devices should check for the items given below. This is a minimum indicative list, Bidders are encouraged to check for more settings in line with best practices(SANS, NIST, CIS, NPCI Baselines, RBI) - Access Control - System Authentication – remote administration security, password security - Auditing and Logging - Insecure Dynamic Routing Configuration - Insecure Service Configuration – Unnecessary services running, SNMP service security - Insecure TCP/IP Parameters – source routing, IP directed broadcasts, UDP broadcast forwarding - Latest version not used
6.	Scanning should check for the items given below. This is a minimum indicative list, Bidders are encouraged to check for more settings in line with best practices including PCI, OSSTM, NPCI Baselines, CERT-IN, RBI - Tests for default passwords

#	Requirements
	- Tests for DoS vulnerabilities - Test for buffer overflows - Test for directory Traversal - Test for insecure services such as SNMP - Check for vulnerabilities based on version of device/server - Test for SQL, XSS and other web application related vulnerabilities - Check for weak encryption - Check for SMTP related vulnerabilities such as open mail relay - Check for strong authentication scheme - Test for sample and default applications/pages - Check for DNS related vulnerabilities such as DNS cache poisoning and snooping - Test for information disclosure such as internal IP disclosure - Look for potential backdoors - Check for older vulnerable version - Remote code execution - Weak SSL Certificate and Ciphers - Missing patches and versions
7.	The Bidder team should work with NPCI personnel or its other outsourced partners for remediation of vulnerabilities. Bidder team should provide support for testing recommendations in UAT, prepare plan for implementation in production and provide support for production rollout
8.	Bidder should conduct a confirmatory audit to confirm the remediation action that has been taken by relevant operations teams at NPCI
9.	All deliverables including reports should undergo Quality Assurance process. Project Manager should define quality metrics, measurement frequency and reporting periodicity in consultation with NPCI
10.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include 1 Escalations from onsite team for specialist support on detected vulnerabilities & solutions for mitigation. 2 Share best practices on configuration standards, new vulnerability checks with onsite team.
11.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.

9.3.3 Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA
1.	Secure Configuration assessment	Carry out secure configuration assessments as per the asset list, frequency provided and test criteria. Submit assessment reports, containing the following 1. Executive summary 2. Benchmark with SANS, NIST, CIS, NPCI Policies, CERT-IN, RBI 3. Categorization of vulnerabilities based on risk level 4. Details of security vulnerabilities 5. Emergency quick-fix solution for discovered vulnerabilities 6. Long-term solution for discovered vulnerabilities 7. Post correction assessment findings	Meet assessment periodicity given in asset scope section Meet quality criteria defined by NPCI on configuration checks and report formats
2.	Vulnerability Scanning	1. Carry out vulnerability scanning and asset discovery scanning as per the asset list, frequency provided and test criteria. 2. Submit report containing the following 3. Executive summary 4. Benchmark with PCI, OSSTM 5. Categorization of vulnerabilities based on risk level 6. Details of security vulnerabilities 7. Emergency quick-fix solution for discovered vulnerabilities 8. Long-term solution for discovered vulnerabilities 9. Post correction assessment findings	Meet scanning periodicity given in asset scope section Meet quality criteria defined by NPCI on scanning checks and report formats
3.	Mitigation support	Bidder should track mitigation for the reporting findings of scanning and assessment activities.	Updated information on mitigation status. Timely query resolution on mitigation recommendations

9.4. Malware Monitoring Services

Bidder should provide an online solution for malware scanning for scanning NPCI's web sites.

Bidder should bring the required tools, processes and methodologies. Bidder should protect the Organization from license & IP related issues. Bidder proposals should capture process & methodology to

offer these services, tool description, sample service output (report formats), experience with similar environments and resume of skilled personnel who will be allocated towards this service.

9.4.1 Asset Scope

All unique web sites / web applications hosted by NPCI.

9.4.2 Service Specification

The web malware scanning service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	Description
1.	24X7 monitoring for Malicious Mobile Code(MMC) and malware infection of websites as given in asset scope
2.	Real time detection of MMC/malware infection/injection
3.	Solution should be a tool based automated solution including the following features: - Spider sites in scope on a continuous basis. - Detect & alert for malware infection. - Baseline website and detect malicious changes to website. - Detect malicious links including ones pointing to other sites with malware or ones that are pointing to malware uploaded in the same site. - Detect malicious java scripts, flash content. - Analyze HTML tags for malicious entries. - Check URLs against global blacklist databases. - Scan spider pages with industry leading anti-virus/anti-spyware. - Support reporting in different formats including PDF reports.
4.	Solution should be implemented onsite at NPCI and integrate with all websites under the scope.
5.	Solution should support scanning to a depth of at least two pages and expanded to higher depth based on risk level of the site.
6.	Solution should support scanning of static and dynamic links.
7.	Bidder should report and engage the team to takedown MMC/malware injection server once it is identified as the source after proper approval.
8.	Bidder should manage incidents for MMC/malware infection/injection including solution, coordination for recovery in the shortest possible time.
9.	Solution should be independent of application platform of the website.

#	Description
10.	Bidder should provide online security dashboard to capture security status of monitored websites and also to track mitigation status of infected sites
11.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include Alert & support onsite team in scenarios where there is a sudden increase in phishing or malware attacks across other Organizations as seen by Bidder SOC Any software development work for automation of workflows, integration with service desk or development of dashboard/ reporting templates or testing tool development
12.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.

9.4.3 Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA
1.	Malware scanning services	Alert Organization on web based malware on NPCI sites being monitored Alert Organization of existence of Blacklisted links on NPCI sites being monitored Alert Organization of potentially malicious website changes on NPCI sites being monitored Incident Management for malware incidents including providing emergency response, identify root cause and provide solution, coordinate with Organization's Bidders as needed	Inform NPCI team via Email/SMS within 30 min of detection of malware, unauthorized change or Blacklisted Link First level incident management response within 60 minutes of alerting NPCI team
2.	Security Dashboard	Online dashboard to capture security status of monitored websites and also to track mitigation status of infected sites	Deliver and maintain the dashboard as required by the Organization Upgrade and provide new features to support evolving needs at the Organization within agreed upon

#	Area	Expected Output	SLA
			time. Update with new data as required

9.5. SIEM & Security Tools implementation GAP analysis Services (onetime)

#	Description
1.	The Bidder should perform gap analysis of the SIEM implementation to ensure it meets best practices and NPCI requirements.
2.	The audit should check the adequacy of log baselines for the devices being monitored.
3.	The audit should check if the use cases meet best practices and NPCI requirements.
4.	The audit should check if the SIEM is implementation has met all system requirements specified by the OEM.
5.	The audit should check if SIEM configuration is as per best practices and NPCI requirements.
6.	Ensure that log collection server installation and configuration is proper.
7.	Identify the level of logs to be enabled across the different components of IT infrastructure.
8.	Support the IT team with the required information to bridge the gap.
9.	Define the required rules, alerts, reports and dashboards as relevant to meet the highest levels of security for NPCI.
10.	Suggest Event correlation design which includes the attributes like events, asset, vulnerability, business value in the threat calculation.
11.	Recommend method of making Evidence for any security incident available for legal and regulatory purposes.

9.6. Reporting

NPCI requires Bidders to provide relevant consolidated as well as individual reports of all activities performed by the Bidder to the top management of NPCI.

The security reporting service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	**Description**
1.	Bidder should provide detailed MIS reports to NPCI on a monthly basis

2.	Bidder should provide quarterly update through a senior resource on activities, security posture of NPCI to key stakeholders

Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below.

#	Area	Expected Output	SLA
1.	Consolidated MIS report across all services rendered	NCPI Security Status	Activity snapshot
2.	- Operational Enhancements	Issues & Action Items	Presenting regular status reports

9.7. Other Requirements

#	Description
1.	Selected Bidder should conduct security training (not certification training) for NPCI's nominated persons once in six months for maximum of 10 participants per session. This training program would cover mutually agreed training agenda on the e-security products & technologies.
2.	Bidder should provide quarterly management briefing to NPCI's senior management team on the project benefits, security risks and global threats facing financial institutions.
3.	Bidder should provide relevant support for external and internal security audits that NPCI is subject to from time to time
4.	Bidder should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time
5.	Bidder should prepare the SOC operations for compliance and certification to the standards of ISO 27001, ISO 20000, BS 25999 and PCI DSS
6.	Project plan for delivering these services and resource ramp up required for project execution will be mutually decided by Bidder & NPCI. NPCI will approve all such plans and project execution should be carried out only based on approval from NPCI
7.	All architecture design, report formats and implementation methodology mentioned in this RFP should be in consultation with NPCI and should be approved before finalization.
8.	All personnel to be deployed under the contract for the full period of service will need to be approved by NPCI. NPCI reserves the right to reject any person and ask for suitable replacement.
9.	Bidder should provide background clearance certificate from reputed agencies for all personnel deployed at NPCI. NPCI may also carry out background checks on personnel deployed at NPCI by itself or any appointed agency, if required. Bidder should provide support as required for such background checks.

#	Description
10.	No part of the service should be outsourced by the Bidder to any third party or contractors for execution. All personnel provided by the Bidder will have to be full time employees of the Bidder.
11.	Bidder will submit detailed SLA compliance report on a quarterly basis. SLA report will be discussed with nominated personnel from NPCI and any breach of SLA will lead to service penalties.
12.	For any slippage in SLA in a quarter by the Bidder, it should create a rectification plan and get it approved by NPCI. If the same SLA is not met in subsequent quarter, NPCI will impose a service penalty, equivalent to 15 days of additional service (pertaining to the said SLA) to be provided by the Bidder at no cost to NPCI. If the particular SLA violation is not rectified in 3rd quarter, NPCI will impose financial penalty equivalent to 10% of the service cost. Detailed clauses on SLA and penalty will be entered into during the contracting phase with selected Bidder.
13.	Apart from SLA reviews, NPCI may also conduct performance reviews at mutually agreed schedules, dates and locations and representatives from both NPCI and Service Provider should attend such performance review meetings
14.	For any major or repeated failure of SLA or any deficiency in the service performance that causes or is likely to cause significant impact to NPCI's operation or reputation, NPCI reserves the right to impose, including cancellation of whole or part of contract, irrespective of any SLA penalty mentioned above.
15.	NPCI should be able to verify performance of each of the above services. Bidder should maintain evidence, logs or proof of such performance throughout the contract period
16.	NPCI reserves the right to audit the Bidder either by itself or through any appointed entity. Bidder must provide full cooperation for audit of services in the scope of this RFP.
17.	The prices quoted by the Bidder should be all inclusive of people cost, cost of processes, methodologies and tools used by the Bidder and the cost of backend services provided from its own SOC. Any out of station (outside city) travel expenses for the onsite team of the Bidder for executing NPCI's work will be borne by NPCI.
18.	Selected Bidder has to provide Performance Bank Guarantee equivalent to the cost of services for one year, valid for 5 years from a Public Sector Organization before claiming the first payment
19.	Cancellation of Order: NPCI reserves its right to cancel the Purchase Order at any time, in the event of breach of contract or serious deficiency in the service or for any other reason. In addition to the cancellation of Purchase order, NPCI reserves the right to invoke the Bank Guarantee given by the Service Provider to recover the damages
20.	Service Transition: Bidder should provide smooth transition of services to another Bidder or internal to NPCI as and when the current contract is terminated. This will include transfer of skills and operating processes and procedures. Bidder should maintain documented processes and procedures for all service delivery to ensure smooth internal or external transition.

#	Description
21.	Indemnity: The Service Provider shall indemnify, protect and save NPCI against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to software licenses, patent, trademarks, copyrights etc. or such other statutory infringements or any actions of the employees or agents or deficiency of service of the Service Provider
22.	IPR: For any licensed software used by the Bidder for performing service or developing software for NPCI, it should have the right to use as well as the right to license for outsourced services or third party software development. Any license or IPR violation on the part of the outsourced Bidder should not put NPCI at risk. NPCI should reserve the right to audit the license usage of the Bidder or ask for a Bidder undertaking on non-violation of IPR
23.	All documentation, service processes, data and methodologies developed by the resources deployed at NPCI and for the services delivered to NPCI will become the property of NPCI. NPCI will retain intellectual rights over such property.
24.	Restrictions: The Bidder must provide professional, objective and impartial advice and at all times hold NPCI's interest paramount, without any consideration for future work, and strictly avoid conflicts with other assignments or their own corporate interests. Bidders shall not be hired for any assignment that would be in conflict with their prior or current obligations, or that may place them in a position of not being able to carry out the assignment in the best interest of NPCI.

Section 10 - Documents forms to be put in Envelope 'A'

Annexure A1 - Bidder's Letter for EMD / Bid Security

To

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises,
BandraKurla Complex
Bandra, Mumbai – 400 051.

Subject: RFP No. NPCI: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*."

We have enclosed an EMD in the form of a Demand Draft No._____ issued by the branch of the _____Bank, for the sum of Rs.2 lakh (Rupees Two lakh only). This EMD is as required by clauses 5.7 of the Instructions to Bidders of the above referred RFP.

Thanking you,

Yours faithfully,

(Signature of the Bidder)
Printed Name:
Designation:
Seal:
Date:
Business Address:

Annexure A2 - Bid Security (Bank Guarantee)

_____
[Bank's Name, and Address of Issuing Branch or Office]

National Payments Corporation of India,
C-9 8th Floor, RBI Premises,
BandraKurla Complex,
Mumbai – 400 051

Date: _____

BID GUARANTEE No.: _____

We have been informed that_____ (hereinafter called "the Bidder") has submitted to you its bid dated (hereinafter called "the Bid") for the execution of _____under

Subject: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*."

Furthermore, we understand that, according to your conditions, bids must be supported by a bank guarantee.

At the request of the Bidder, we _____hereby irrevocably undertake to pay you without any demur or protest, any sum or sums not exceeding in total an amount of Rs.2,00,000/-(Rupees Two lakhs only) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of the terms of the Request for Proposal.

_____
[signature(s)]

Annexure B - Bid Offer Form (without Price)

(Bidder's Letter Head)

OFFER LETTER

Date:

To

The Chief Executive Officer
National Payments Corporation of India
C-9, 8th Floor, RBI Premises,
BandraKurla Complex, Bandra (East),
Mumbai – 400 051

Dear Sir,

Subject: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*."

We have examined the above referred RFP document. As per the terms and conditions specified in the RFP document, and in accordance with the schedule of prices indicated in the commercial bid and made part of this offer.
We acknowledge having received the following addenda / corrigenda to the RFP document.

Addendum No. / Corrigendum No.	Dated

While submitting this bid, we certify that:

1. Prices have been quoted in INR.
2. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP.
3. We have not induced nor attempted to induce any other bidder to submit or not submit a bid for restricting competition.
4. We agree that the rates / quotes, terms and conditions furnished in this RFP are for NPCI and its Associates.

If our offer is accepted, we undertake, to start the assignment under the scope immediately after receipt of your order. We have taken note of Penalty clauses in the RFP and agree to abide by the same. We also note that NPCI reserves the right to cancel the order and order cancellation clause as per terms and condition would be applicable. We understand that for delays not attributable to us or on account of uncontrollable circumstances, penalties will not be levied and that the decision of NPCI will be final and binding on us.

We agree to abide by this offer till 180 days from the last date stipulated by NPCI for submission of bid, and our offer shall remain binding upon us and may be accepted by NPCI any time before the expiry of that period.

Until a formal contract is prepared and executed with the selected bidder, this offer will be binding on us. We also certify that the information/data/particulars furnished in our bid are factually correct. We also accept that in the event of any information / data / particulars are found to be incorrect, NPCI will have the right to disqualify /blacklist us and forfeit bid security.

We undertake to comply with the terms and conditions of the bid document. We understand that NPCI may reject any or all of the offers without assigning any reason whatsoever.

As security for the due performance and observance of the undertaking and obligation of the bid we submit herewith Demand Draft bearing no. _____dated _____ drawn in favor of "National Payments Corporation of India" or Bank Guarantee valid for ____days for an amount of Rs.2,00,000 (Rs. Two Lakhs Only) payable at Mumbai.

Yours sincerely,

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Company/Firm:

Address

Annexure C - Bidder's Information

Details of the Bidder				
1	Name of the Bidder (Prime)			
2	Address of the Bidder			
3	Status of the Company (Public Ltd/ Pvt. Ltd)			
4	Details of Incorporation of the Company.	Date:		
		Ref#		
6	Valid Sales tax registration no.			
7	Valid Service tax registration no.			
8	Permanent Account Number (PAN)			
9	Name & Designation of the contact person to whom all references shall be made regarding this tender			
10	Telephone No. (with STD Code)			
11	E-Mail of the contact person:			
12	Fax No. (with STD Code)			
13	Website			
Financial Details (as per audited Balance Sheets) (in Cr)				
14	Year	2009-10	2010-11	2011-12
15	Net worth			
16	Turn Over			
17	PAT			

SOC Team Details Checklist: -

Attested documents need to be submitted for L1 Support and L2 Support SOC Engineers	Verified Attached (Y/N)
Experience letter with relative no. of years of experience	Yes/No
Detailed Bio-Data	Yes/No
All Credentials acquired by individual engineers respectively for L1 & L2 support	Yes/No

Signature: _____.
Name:_____-
Designation:_____

Date: _____, Place _____

Annexure D - Eligibility Criteria Response

S.no.	Eligibility Criteria	Response Document
1	The bidder should be a Company registered under the Companies Act 1956 for the last 3 years.	Registration Certificate
2	The Bidder should have minimum annual turnover of Rs. 25 Cr. per year in the last 3 financial years i.e. 2009-10, 2010-11 and 2011-12 (or Calendar year 2009, 2010, 2011 or the Bidder's financial years).	This must be supported by audited financial statements (Reports) for the financial years i.e. 2009-10, 2010-11 and 2011-12 (or Calendar year 2009, 2010, 2011 or the Bidder's financial years).
3	The Bidder should be a profit (profit after tax) making company in the last financial year i.e. 2011-12 (or Calendar year 2011 or the Bidder's financial year).	This must be supported by audited financial statements (Reports) for the financial year 2011-12 or Calendar year 2011 or the Bidders' last financial year.
4	Bidder should have experience in SOC management for minimum 3 years in servicing banks / financial institutions.	Experience Letter.
5	Bidder should provide satisfactory performance certificates from two customers to whom the bidder is currently providing SOC services (24*7) for similar requirements, at least 1 year as on 01 January 2013.	Customer reference letters
6	The Bidder should not be currently blacklisted by any bank / institution in India or abroad.	Self Declaration

Signature: _____

Name: _____ Designation: _____

Date: _____ Place: _____

Annexure E – Declaration for Acceptance of RFP Terms and Conditions

To

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises,
Bandra Kurla Complex
Bandra, Mumbai – 400 051.

Sir,

Subject: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*."

I have carefully gone through the Terms & Conditions contained in the above referred RFP document. I declare that all the provisions of this RFP are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure F – Declaration for Acceptance of Scope of Work

To

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises,
Bandra Kurla Complex
Bandra, Mumbai – 400 051.

Sir,
Re: Subject: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*."
.

I have carefully gone through the Scope of Work contained in the above referred RFP document. I declare that all the provisions of this RFP are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure G – Format Power of Attorney

(On Stamp paper of relevant value)

Know all men by the present, we _____ (name of the company and address of the registered office) do hereby appoint and authorize Mr _____ (full name and residential address) who is presently employed with us holding the position of _____ as our attorney, to do in our name and on our behalf, deed and things necessary in connection with or incidental to our proposal for "_____" in response to the RFP No. _____by NPCI, including signing and submission of all the documents and providing information/responses to NPCI in all the matter in connection with our bid.

We hereby agree to ratify all deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all deeds and things done by our aforesaid attorney shall always be deemed to have been done by us.

Dated this _____ day of _____ 2012.
For _____.
(Signature)
(Name Designation and Address)

Accepted
Signature)
(Name Designation)
Date:
Business Address:

Annexure H - Letter of Undertaking

(On Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises,
Bandra Kurla Complex
Bandra(E), Mumbai – 400 051.

Sir,

Reg.: Our bid for Request for Proposal (RFP) for ***Engaging Agency for SOC Services dated 16.01.2013***

We submit our Bid Document herewith.

We understand that

• You are not bound to accept the lowest or any bid received by you, and you may reject all or any bid.

• If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by you to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.

• If our bid is accepted, we are to be jointly and severally responsible for the due performance of the contract.

Dated at_____this _____day of _____2013.

Yours faithfully

For_____

Signature:_____

Name:_____

Annexure I - Pre-Qualification Bid Letter

To

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises,
Bandra Kurla Complex
Bandra(E), Mumbai – 400 051.

Subject: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*".

We, the undersigned Bidders, having read and examined in detail all the RFP documents do hereby propose to provide the services as specified in the RFP document Dated <DD/MM/YYYY> along with the following:

a. EARNEST MONEY DEPOSIT (EMD)

We have enclosed an EMD in the form of a Demand Draft / Bank Guarantee for the sum of Rs. _____/- (Rupees _____only). This EMD is liable to be forfeited in accordance with the provisions of the *Terms and Conditions* of the Contract.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief. We understand that our bid is binding on us and that you are not bound to accept a bid you receive.
Thanking you,
Yours faithfully,

(Signature of the Bidder)
Printed Name:
Designation:
Seal:
Date:
Business Address:

Annexure J - Declaration regarding Clean Track by Bidder

(On Bidder's Letterhead)

To

The Chief Executive Officer
National Payments Corporation of India,
C-9, 8th Floor, RBI Premises,
Bandra (E), Mumbai – 400 051.

Sir,

Re: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for "*Request for Proposal (RFP) for Engaging Agency for SOC Services*."

I have carefully gone through the Terms and Conditions contained in the above referred RFP. I hereby declare that my company/firm is not currently debarred/black listed by any Government / Semi Government organizations/ Institutions in India or abroad. I further certify that I am competent officer in my company/firm to make this declaration.

Or

I declare the following

No.	Country in which the company is debarred/blacklisted/case is pending	Black listed/debarred by Government / Semi Government organizations/ Institutions	Reason	Since when and for how long

(NOTE: In case the company/firm was blacklisted previously, please provide the details regarding Period for which the company/firm was blacklisted and the reason/s for the same)

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Section 11 – To be put in Envelope ‘ B’

Annexure T: Technical Specifications Compliance Matrix

1. Security Monitoring Services

Service Specification

The security monitoring service to be provided by the Bidder should meet the following specifications.

#	Requirements	Compliance (Yes/No)	Remarks
1.	Bidder should monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in NPCI environment. Monitoring should be done on 24/7 basis with onsite personnel. Bidder should provide the personnel for managing the security monitoring service as per the team specifications in scope of work.		
2.	Bidder should develop, update and maintain log baselines for all platforms at NPCI that are required to be monitored.		
3.	Bidder should coordinate with IT operations to implement and maintain the log baselines on production systems		
4.	Bidder should detect both internal & external attacks. In addition to security attacks on IT infrastructure, Bidders should also monitor for security events on business applications, databases and also identify network behavior anomalies.		

#	Requirements	Compliance (Yes/No)	Remarks
5.	Bidder should monitor, detect and manage incidents for the following minimum set of IT infrastructure security events. This is indicative minimum list and is not a comprehensive/complete set of events. Bidders should indicate their event list in proposal response. Buffer Overflow attacks Port & vulnerability Scans Password cracking Worm/virus outbreak File access failures Unauthorized server/service restarts Unauthorized changes to firewall rules Unauthorized Bidder access to systems SQL injection Cross site scripting		
6.	Bidder operations team at NPCI should send alerts with details of mitigation steps to designated personnel within NPCI and any identified service provider of NPCI.		
7.	Bidder should provide coordinated rapid response to any security incident. Bidder should contain attack & coordinate restoration of services. While Bidder personnel will enlist support of other departments and service providers in NPCI, primary responsibility for incident response will be with the Bidder.		
8.	Bidder should maintain a knowledge base of alerts, incidents and mitigation steps and this knowledge base should be updated with evolving security events within and outside NPCI. Team should send customized alerts advisories to respected teams in NPCI.		
9.	Evidence for any security incident should be maintained in tamper proof manner and should be made available for legal and regulatory purposes, as required.		

#	Requirements	Compliance (Yes/No)	Remarks
10.	Bidder should add/delete/modify rules, reports and dashboards based on NPCI requirements		
11.	Bidder should provide MIS reports to NPCI on daily, weekly and monthly basis. Reporting requirements will be finalized with the selected Bidder. Bidder should also have the provision to provide reports on demand whenever required by NPCI.		
12.	Bidder should conduct forensic analysis for security incidents to enable identification of perpetrators and their methodologies.		
13.	Bidder should do root cause analysis for security incidents and coordinate implementation of controls to prevent recurrence.		
14.	Bidder should carry out system administration tasks including regular backup of system, restoration, installation, health check and others		
15.	Bidder should manage any faults in the SIEM solution by trouble shooting and coordinating with the OEM/principle		
16.	Bidder team Analyst(s) and program manager are responsible for managing the security monitoring team and ensuring satisfactory performance		
17.	All deliverables including reports should undergo Quality Assurance process. Bidder team lead should define quality metrics, measurement frequency and reporting periodicity in consultation with NPCI		
18.	Analyst should review reports, operating procedures, administrative activities on a daily basis to identify quality issues		
19.	Analyst should submit periodic Quality Assurance reports to NPCI as per the reporting frequency designed.		

#	Requirements	Compliance (Yes/No)	Remarks
20.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include 1. Managing escalations from onsite team for detection & response to new threats & complex attacks that onsite team is unable to resolve. 2. For adding new/updated threat scenarios and other best practices in NPCI's SIEM tool for detection & response based on Bidder SOC visibility & experience across other customers. 3. Forensic analysis of attacks/incidents including making available specialists, domain experts, tools.		
21.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.		
22.	Bidder should provide a proactive solution to identify problems.		

#	Requirements	Compliance (Yes/No)	Remarks
23.	Bidder should provide incident tracking and management solution, which: - Should have the feature to Log Problems. - Categorization and Prioritization of problems should be possible. - Should have feature to auto assign Tickets. - Should have facility to assign tickets based on policy and workflow rules and should have at least 5 escalation levels. - Should have a feature to cascade and Organize rules. - Users/technicians must be notified for pending requests. It should have the feature to create rules for such notifications - Should be possible to send personalized E-mails to users - Should be possible to send notification emails to the requester - Should Converge all IT help desks in your business units across buildings/complexes or countries, to function as a single help desk. - Should customize the holidays, departments, technicians /site associations, groups, business rules and SLA's as per the location's operational hours - Should Enables the requests logged in from each site to be resolved within that particular site's operational hours. - Automatically reset the end-users password without the involvement of helpdesk technicians. - - Support integration with LDAP and Active Directory		

Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
1.	Event monitoring	24X7 monitoring for identified assets and 24X7 response for any events	Sending alerts with mitigation steps to designated personnel:		

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
		Detection of internal & external attacks, suspicious events or abnormal behaviour against pre-defined baseline for network, applications and databases Recommend mitigation steps for alerts Alert categories and their prioritization and reporting format as per mutually approved process & escalation matrix	15 min: Very high priority events 30 min: High priority events 60 min: Medium priority events Alerting method: Email/SMS/Call: Very high priority events Email/SMS: High priority events Email: Medium Priority events		
2.	Incident Management & Forensics	Coordinated rapid response to any security incident Contain attack & restore services Forensic analysis & report Root cause analysis report and long term security control identification Evidence collection and retention for legal and regulatory purpose Log retention and repository of incident knowledge base	Providing initial response to incidents: 60 min: Very high priority incidents 90 min: High priority incidents 120 min: Medium priority incidents Providing report with root cause analysis: 72 hours: Very high priority incidents 96 hours: High priority incidents 120 hours: Medium priority incidents		

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
			Availability of logs relevant to reported events/ incidents for the period of: 12 months Retention of all logs for a period of one year Repository of incidents and mitigation knowledgebase		
3.	Reports	Timely submission of daily, weekly and monthly reports Multiple types of reports, an indicative list is given below:- Daily reports including firewall change reconciliation, unauthorized database admin access, referrer log brand misuse reports, anti-virus policy non-compliance, unauthorized service provider access, privilege misuse/escalation Weekly reports including persistent top attackers, attacks, attack targets, trend analysis Monthly MIS reports, executive representation for top management, trend analysis Reports as defined by NPCI from time to time.	Daily Reports: By 12:00 PM Weekly Reports: By 10:00 AM : Monday Monthly Reports: By 5th of each month		

2. Security Product Management

Service Specification

The security device management service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	Requirement	Compliance (F/P/N)	Remarks
1.	Management of products in scope for policies, configurations, availability, fault and capacity management during business hours		
2.	Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to NPCI on a regular basis		
3.	Reviews SLA's with OEM /product support and recommend measures to improve the service levels.		
4.	Maintain IP addressing schemes, routing information, routing tables for security device operations		
5.	Provide recommendations for architecture enhancements/changes that can enhance the security posture		
6.	management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks		
7.	Provide NPCI with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages		
8.	Coordinate delivery with all stake holders including help desks, network team, IT team, application team and all appropriate third parties, as necessary, for the management of products in asset scope		
9.	Maintain security product configuration, based on industry best practices and as requested, for the products within the Asset Scope		
10.	Maintain complete documentation and architecture layout for all products with site deployment layout		
11.	Participate in technical and business planning sessions		

#	Requirement	Compliance (F/P/N)	Remarks
	to establish security standards, architecture and project initiatives where the security products may impact or improvise the design		
12.	Provide infrastructure security planning & analysis, recommendations for installation and upgrade of products in scope		
13.	Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope		
14.	Bidder should analyze performance reports and formulate plan for capacity addition		
15.	Provide technical expertise/support for audits on the products in scope		
16.	Set up and manage admin and user accounts. Perform access control on need basis		
17.	Take the backup of product configuration files any time there is a change in device configuration		
18.	Review the backup configuration and business continuity procedures to be followed in the event of device failure		
19.	Submit the Periodic Reports on the backup status		
20.	Restore configuration in the event of product crash, corruption or other failure		
21.	Design and program manage new device implementations		
22.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include • Escalations from onsite team for specialist support on security product categories to resolve faults, configuration related issues • Share best practices on product configuration standards & policies with onsite team		

#	Requirement	Compliance (F/P/N)	Remarks
23.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.		
24.	The following activities has to be carried out specifically for the DLP system in scope: 7. Identify the sensitive data that needs to be protected by DLP in discussion with NPCI. 8. Discover sensitive data by periodically scanning servers and endpoints of NPCI. 9. Design, configure and fine tune DLP policies to protect sensitive data in accordance with NPCI requirements. 10. Design and configure DLP reports and dashboard. 11. Generate daily, weekly, monthly DLP reports as required. 12. Monitor and analyze DLP alerts and perform incident management.		
25.	The following activities has to be carried out specifically for the PIM solution in scope: 7. Conduct role engineering to design the access policies for servers and network devices 8. Configure and fine tune access policies for servers and network devices 9. Configure end user accounts and associated access policies and manage their privileges 10. Design and configure PIM reports and dashboard 11. Generate daily, weekly, monthly PIM reports as required 12. Monitor and analyze PIM alerts and perform incident management Analyze PIM recordings for incident analysis		
26.	The following activities has to be carried out specifically for the FIM solution in scope: 7. Identify the files to be monitored across servers/network devices based on best practices, regulatory/standards requirements and NPCI requirements. 8. Identify configuration audit requirements 9. Design, configure and fine tune the FIM and Configuration audit policies for the identified files		

#	Requirement	Compliance (F/P/N)	Remarks
	and configuration items to be monitored. 10. Design and configure FIM reports and dashboard. 11. Generate daily, weekly, monthly FIM reports as required. 12. Monitor and analyze FIM alerts and perform incident management.		
27.	Create or migrate users from LDAP/ User repository to the Two factor authentication server		
28.	Carry out token life-cycle management procedures such as 4. User Token provisioning procedure 5. Modification of two-factor authentication privileges for end user owing to change in job role 6. Token revocation on exit or termination Carry out Help desk procedures such as 5. Reporting lost tokens 6. Returning faulty, damaged or expired tokens 7. Enabling emergency access for permanently lost, damaged or expired tokens 8. Inventory management		

Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
1.	Architecture planning, review & redesign (as required from time to time)	6. Plan & review placement of servers in the network segments 7. Plan & review Device segmentation 8. Plan & review authentication schemes 9. Plan & review integration with other security	Completion of activities within mutually agreed upon timelines		

		components 10. Oversight for new device implementation			
2.	Policy & user Management	8. Risk Analysis and policy design 9. Configuration of polices 10. Document policy change 11. Policy optimization for all the Devices 12. Audit policy for exceptions 13. Set up and manage admin and user accounts as per policies of NPCI 14. Interact with network team for managing escalations with NOC	Emergency Changes: ▪ 30 min: Acknowledgement of change request ▪ 60 min: Implementation of change requests Routine Changes: ▪ 4 hours: Acknowledgement of change requests ▪ 8 hours: Implementation of change requests		
3.	Availability and Configuration Management	9. Backup & restoration of configuration 10. Periodic review the backup configuration and business continuity procedures to be followed in the event of Device failure 11. Monitor the availability of devices 12. Root cause analysis for failure/ downtime of security devices 13. Maintain IP addressing schemes, routing information, routing tables, for the Device operations 14. Detailed analysis of miss-configurations, OS/application failures	• Periodic Backup as per NPCI's policy • Backup before and after implementation of any change • Quarterly report on maintenance contract & software subscription		

		15. Comply with NPCI policies & regulations applicable to NPCI 16. Tracking the SLA with product Bidder or reseller, maintenance contract, required license, software subscription for all hardware & software components of Devices.			
4.	Fault Management	6. Open a case with device supplier in the event of hardware component or system failure or bugs 7. Co-ordinate with device supplier/OEM for solution 8. Review the device supplier/OEM SLA for recommending measures to improve the service levels 9. Track AMC renewal dates 10. Root cause analysis for any failures / downtimes	- Open a ticket within 30 minutes of problem identification - Status update every 4 hours to NPCI personnel - Quarterly review of Bidder SLA		
5.	Device migration/update	5. Prepare and review capacity plans for security devices and recommend upgrades as required. 6. Provide security infrastructure analysis, recommendations for installation and upgrade 7. Prepare specifications, architecture and detailed plan for migration/upgrade 8. Test migration/upgrade plan in staging environment	- Quarterly analysis report as per NPCI's specified format - Version upgrades within 3 months from release of new version		

3. Vulnerability Management Services

Service Specification

The Vulnerability management service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	Requirements	Compliance (F/P/N)	Remarks
1.	Bidder should conduct scanning & configuration assessments as per frequency defined in the asset scope table		
2.	Configuration assessments should check for compliance against the secure baseline and SANS, NIST, CIS, NPCI baselines, CERT-IN, RBI guidelines as updated from time to time.		
3.	Configuration assessment of OS should check for the items given below. This is a minimum indicative list and Bidders are encouraged to check for more settings in line with best practices (SANS, NIST, CIS, NPCI baselines, CERT-IN, RBI): - Shares with insecure permission - Permissions to critical system files and folders - Audit log settings - Space allocated for Event Viewer logs - SNMP community strings - Password and account lockout policies - Non-essential services check - TCP/IP stack settings - User rights assignment - Latest Service Pack installation - Latest security patches installation - Antivirus software		
4.	Configuration assessment of database should check for the items given below. This is a minimum indicative list, Bidders are encouraged to check for more settings in line with best practices(SANS, NIST, CIS, NPCI policies, CERT-IN, RBI) - Default passwords - DBLINK Encrypt Login Option - Allocation of Unlimited Table space - Temporary and Default Table space Management		

#	Requirements	Compliance (F/P/N)	Remarks
	- Unrestricted access to services - Web based access to database using iSQL * Plus - Run time modification of the listener service - Look for latest version - Test for secure authentication mechanism - Latest version not installed		
5.	Configuration assessment of network & security devices should check for the items given below. This is a minimum indicative list, Bidders are encouraged to check for more settings in line with best practices(SANS, NIST, CIS, NPCI Baselines, RBI) - Access Control - System Authentication – remote administration security, password security - Auditing and Logging - Insecure Dynamic Routing Configuration - Insecure Service Configuration – Unnecessary services running, SNMP service security - Insecure TCP/IP Parameters – source routing, IP directed broadcasts, UDP broadcast forwarding - Latest version not used		
6.	Scanning should check for the items given below. This is a minimum indicative list, Bidders are encouraged to check for more settings in line with best practices including PCI, OSSTM, NPCI Baselines, CERT-IN, RBI - Tests for default passwords - Tests for DoS vulnerabilities - Test for buffer overflows - Test for directory Traversal - Test for insecure services such as SNMP - Check for vulnerabilities based on version of device/server - Test for SQL, XSS and other web application related vulnerabilities - Check for weak encryption - Check for SMTP related vulnerabilities such as open mail relay - Check for strong authentication scheme - Test for sample and default applications/pages - Check for DNS related vulnerabilities such as		

#	Requirements	Compliance (F/P/N)	Remarks
	DNS cache poisoning and snooping - Test for information disclosure such as internal IP disclosure - Look for potential backdoors - Check for older vulnerable version - Remote code execution - Weak SSL Certificate and Ciphers - Missing patches and versions		
7.	The Bidder team should work with NPCI personnel or its other outsourced partners for remediation of vulnerabilities. Bidder team should provide support for testing recommendations in UAT, prepare plan for implementation in production and provide support for production rollout		
8.	Bidder should conduct a confirmatory audit to confirm the remediation action that has been taken by relevant operations teams at NPCI		
9.	All deliverables including reports should undergo Quality Assurance process. Project Manager should define quality metrics, measurement frequency and reporting periodicity in consultation with NPCI		
10.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include 3 Escalations from onsite team for specialist support on detected vulnerabilities & solutions for mitigation. 4 Share best practices on configuration standards, new vulnerability checks with onsite team.		
11.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.		

Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
1.	Secure Configuration assessment	Carry out secure configuration assessments as per the asset list, frequency provided and test criteria. Submit assessment reports, containing the following 8. Executive summary 9. Benchmark with SANS, NIST, CIS, NPCI Policies, CERT-IN, RBI 10. Categorization of vulnerabilities based on risk level 11. Details of security vulnerabilities 12. Emergency quick-fix solution for discovered vulnerabilities 13. Long-term solution for discovered vulnerabilities 14. Post correction assessment findings	Meet assessment periodicity given in asset scope section Meet quality criteria defined by NPCI on configuration checks and report formats		
2.	Vulnerability Scanning	10. Carry out vulnerability scanning and asset discovery scanning as per the asset list, frequency provided and test criteria. 11. Submit report containing the following 12. Executive summary 13. Benchmark with PCI, OSSTM 14. Categorization of vulnerabilities based on risk level 15. Details of security vulnerabilities 16. Emergency quick-fix solution for discovered vulnerabilities	Meet scanning periodicity given in asset scope section Meet quality criteria defined by NPCI on scanning checks and report formats		

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
		17. Long-term solution for discovered vulnerabilities 18. Post correction assessment findings			
3.	Mitigation support	Bidder should track mitigation for the reporting findings of scanning and assessment activities.	Updated information on mitigation status. Timely query resolution on mitigation recommendations		

4. Malware Monitoring Services

Service Specification

The web malware scanning service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	Description	Compliance (F/P/N)	Remarks
1.	24X7 monitoring for Malicious Mobile Code(MMC) and malware infection of websites as given in asset scope		
2.	Real time detection of MMC/malware infection/injection		

#	Description	Compliance (F/P/N)	Remarks
3.	Solution should be a tool based automated solution including the following features: - Spider sites in scope on a continuous basis. - Detect & alert for malware infection. - Baseline website and detect malicious changes to website. - Detect malicious links including ones pointing to other sites with malware or ones that are pointing to malware uploaded in the same site. - Detect malicious java scripts, flash content. - Analyze HTML tags for malicious entries. - Check URLs against global blacklist databases. - Scan spider pages with industry leading anti-virus/anti-spyware. - Support reporting in different formats including PDF reports.		
4.	Solution should be implemented onsite at NPCI and integrate with all websites under the scope.		
5.	Solution should support scanning to a depth of at least two pages and expanded to higher depth based on risk level of the site.		
6.	Solution should support scanning of static and dynamic links.		
7.	Bidder should report and engage the team to takedown MMC/malware injection server once it is identified as the source after proper approval.		
8.	Bidder should manage incidents for MMC/malware infection/injection including solution, coordination for recovery in the shortest possible time.		
9.	Solution should be independent of application platform of the website.		
10.	Bidder should provide online security dashboard to capture security status of monitored websites and also to track mitigation status of infected sites		

#	Description	Compliance (F/P/N)	Remarks
11.	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include Alert & support onsite team in scenarios where there is a sudden increase in phishing or malware attacks across other Organizations as seen by Bidder SOC Any software development work for automation of workflows, integration with service desk or development of dashboard/ reporting templates or testing tool development		
12.	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources.		

Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
1.	**Malware scanning services**	**Alert Organization on web based malware on NPCI sites being monitored** **Alert Organization of existence of Blacklisted links on NPCI sites being monitored** **Alert Organization of potentially malicious website changes on NPCI sites being monitored** **Incident Management for malware incidents including providing emergency response, identify root cause and provide solution, coordinate with Organization's Bidders as needed**	**Inform NPCI team via Email/SMS within 30 min of detection of malware, unauthorized change or Blacklisted Link** **First level incident management response within 60 minutes of alerting NPCI team**		

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
2.	**Security Dashboard**	**Online dashboard to capture security status of monitored websites and also to track mitigation status of infected sites**	**Deliver and maintain the dashboard as required by the Organization** **Upgrade and provide new features to support evolving needs at the Organization within agreed upon time.** **Update with new data as required**		

5. SIEM & Security Tools implementation GAP analysis Services (Onetime)

#	Description	Compliance (F/P/N)	Remarks
1.	The Bidder should perform gap analysis of the SIEM implementation to ensure it meets best practices and NPCI requirements.		
2.	The audit should check the adequacy of log baselines for the devices being monitored.		
3.	The audit should check if the use cases meet best practices and NPCI requirements.		
4.	The audit should check if the SIEM is implementation has met all system requirements specified by the OEM.		
5.	The audit should check if SIEM configuration is as per best practices and NPCI requirements.		
6.	Ensure that log collection server installation and configuration is proper.		
7.	Identify the level of logs to be enabled across the different components of IT infrastructure.		
8.	Support the IT team with the required information to bridge the gap.		
9.	Define the required rules, alerts, reports and dashboards as relevant to meet the highest levels of security for NPCI.		
10.	Suggest Event correlation design which includes the attributes like events, asset, vulnerability, business value in the threat calculation.		

11.	Recommend method of making Evidence for any security incident available for legal and regulatory purposes.		

6. Reporting

NPCI requires Bidders to provide relevant consolidated as well as individual reports of all activities performed by the Bidder to the top management of NPCI.

The security reporting service to be provided by the Bidder should meet the following specifications. Bidder should provide compliance status and remarks for any deviations.

#	Description	Compliance (F/P/N)	Remarks
1.	Bidder should provide detailed MIS reports to NPCI on a monthly basis		
2.	Bidder should provide quarterly update through a senior resource on activities, security posture of NPCI to key stakeholders		

Deliverables

Bidder should meet the service specifications mentioned above. Along with meeting service specifications Bidder should provide the following Deliverables as per SLA mentioned below.

#	Area	Expected Output	SLA	Compliance (F/P/N)	Remarks
1.	Consolidated MIS report across all services rendered	NCPI Security Status	Activity snapshot		
2.	- Operational Enhancements	Issues & Action Items	Presenting regular status reports		

7. Other Requirements

#	Description	Compliance (F/P/N)	Remarks
1.	Selected Bidder should conduct security training (not certification training) for NPCI's nominated persons once in six months for maximum of 10 participants per session. This training program would cover mutually agreed training agenda on the e-security products & technologies.		
2.	Bidder should provide quarterly management briefing to NPCI's senior management team on the project benefits, security risks and global threats facing financial institutions.		
3.	Bidder should provide relevant support for external and internal security audits that NPCI is subject to from time to time		
4.	Bidder should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time		
5.	Bidder should prepare the SOC operations for compliance and certification to the standards of ISO 27001, ISO 20000, BS 25999 and PCI DSS		
6.	Project plan for delivering these services and resource ramp up required for project execution will be mutually decided by Bidder & NPCI. NPCI will approve all such plans and project execution should be carried out only based on approval from NPCI		
7.	All architecture design, report formats and implementation methodology mentioned in this RFP should be in consultation with NPCI and should be approved before finalization.		
8.	All personnel to be deployed under the contract for the full period of service will need to be approved by NPCI. NPCI reserves the right to reject any person and ask for suitable replacement.		
9.	Bidder should provide background clearance certificate from reputed agencies for all personnel deployed at NPCI. NPCI may also carry out background checks on personnel deployed at NPCI by itself or any appointed agency, if required. Bidder should provide support as required for such background checks.		
10.	No part of the service should be outsourced by the Bidder to any third party or contractors for execution. All personnel provided by the Bidder will have to be full time employees of the Bidder.		

#	Description	Compliance (F/P/N)	Remarks
11.	Bidder will submit detailed SLA compliance report on a quarterly basis. SLA report will be discussed with nominated personnel from NPCI and any breach of SLA will lead to service penalties.		
12.	For any slippage in SLA in a quarter by the Bidder, it should create a rectification plan and get it approved by NPCI. If the same SLA is not met in subsequent quarter, NPCI will impose a service penalty, equivalent to 15 days of additional service (pertaining to the said SLA) to be provided by the Bidder at no cost to NPCI. If the particular SLA violation is not rectified in 3rd quarter, NPCI will impose financial penalty equivalent to 10% of the service cost. Detailed clauses on SLA and penalty will be entered into during the contracting phase with selected Bidder.		
13.	Apart from SLA reviews, NPCI may also conduct performance reviews at mutually agreed schedules, dates and locations and representatives from both NPCI and Service Provider should attend such performance review meetings		
14.	For any major or repeated failure of SLA or any deficiency in the service performance that causes or is likely to cause significant impact to NPCI's operation or reputation, NPCI reserves the right to impose, including cancellation of whole or part of contract, irrespective of any SLA penalty mentioned above.		
15.	NPCI should be able to verify performance of each of the above services. Bidder should maintain evidence, logs or proof of such performance throughout the contract period		
16.	NPCI reserves the right to audit the Bidder either by itself or through any appointed entity. Bidder must provide full cooperation for audit of services in the scope of this RFP.		
17.	The prices quoted by the Bidder should be all inclusive of people cost, cost of processes, methodologies and tools used by the Bidder and the cost of backend services provided from its own SOC. Any out of station (outside city) travel expenses for the onsite team of the Bidder for executing NPCI's work will be borne by NPCI.		
18.	Selected Bidder has to provide Performance Bank Guarantee equivalent to the cost of services for one year, valid for 5 years from a Public Sector Organization before claiming the first payment		

#	Description	Compliance (F/P/N)	Remarks
19.	Cancellation of Order: NPCI reserves its right to cancel the Purchase Order at any time, in the event of breach of contract or serious deficiency in the service or for any other reason. In addition to the cancellation of Purchase order, NPCI reserves the right to invoke the Bank Guarantee given by the Service Provider to recover the damages		
20.	Service Transition: Bidder should provide smooth transition of services to another Bidder or internal to NPCI as and when the current contract is terminated. This will include transfer of skills and operating processes and procedures. Bidder should maintain documented processes and procedures for all service delivery to ensure smooth internal or external transition.		
21.	Indemnity: The Service Provider shall indemnify, protect and save NPCI against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to software licenses, patent, trademarks, copyrights etc. or such other statutory infringements or any actions of the employees or agents or deficiency of service of the Service Provider		
22.	IPR: For any licensed software used by the Bidder for performing service or developing software for NPCI, it should have the right to use as well as the right to license for outsourced services or third party software development. Any license or IPR violation on the part of the outsourced Bidder should not put NPCI at risk. NPCI should reserve the right to audit the license usage of the Bidder or ask for a Bidder undertaking on non-violation of IPR		
23.	All documentation, service processes, data and methodologies developed by the resources deployed at NPCI and for the services delivered to NPCI will become the property of NPCI. NPCI will retain intellectual rights over such property.		
24.	Restrictions: The Bidder must provide professional, objective and impartial advice and at all times hold NPCI's interest paramount, without any consideration for future work, and strictly avoid conflicts with other assignments or their own corporate interests. Bidders shall not be hired for any assignment that would be in conflict with their prior or current obligations, or that may place them in a position of not being able to carry out the assignment in the best interest of NPCI.		

Annexure T1 - Bidder's Experience

A - Bidder's Organization

[Provide here a brief description of the background and organization of your firm/company. The brief description should include ownership details, date and place of incorporation of the company/firm, objectives of the company/firm etc.

B - Bidder's Experience

[Using the format below for each Project for which your company/firm was legally contracted either individually as a corporate entity for supplying licenses and implementing replication solution :

Sr.No.	Particulars	Details
1.	Name of the Project	
2.	Approximate cost of contract/Project cost	
3.	Institute /Company	
4.	Duration of Project (months)	

Note: Please provide documentary evidence from the client wherever applicable.

Signature: _____

Name: _____

Designation: _____

Date: _____ Place _____

Annexure T2 - Client Details

Provide details the client details wherever available:

S. No.	Name of Institution	Contact Person Name and Designation	Contact Details with e-mail	Preferable time to contact

Signature: _____.

Name:_____-

Designation:_____

Date: _____, Place _____

Date: _____, Place _____

Section 12 – To be put in Envelope ‘ B’

Annexure C1 - Commercial Offer Form

(Bidder’s Letter Head)

(To be included in Commercial Bid Envelope only)

To Date:

NPCI

Dear Sirs,

Re: RFP No. NPCI: RFP: 2012-13/0025 dated 16.01.2013 for “*Request for Proposal (RFP) for Engaging Agency for SOC Services*.”

Having examined the Bidding Documents placed along with the above referred RFP, we, the undersigned, offer to provide the required services in conformity with the said Bidding documents for the sum of Rs……(Rupees all inclusive and except octroi) or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We agree to abide by the Bid and the rates quoted therein for the orders awarded by NPCI up to the period prescribed in the Bid which shall remain binding upon us. Until a formal contract is signed with the selected bidder, this Bid shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We have complied with all the terms and conditions of the RFP. We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this…… Day of……..2013.

(Signature)

(Name) (In the capacity of)

Duly authorized to sign Bid for and on behalf of

Annexure C2 - Commercial Format

Table A: -

Charges Engaging Agency for SOC Services at Mumbai (All figures in Rs.)							
#	**Role**	**Number of resources to be deployed (A)**	**Unit Price per month (B)**	**Tax (C)**	**Total Price per resource per month (D = B + C)**	**Total for one year**	**Total for three years**
1	SOC L1 Support Engineers (5 resources required for 24x7 SOC Operation)	L S					
2	SOC L2 Support Engineers	2					
	Total Cost						

Table B: -

Charges Engaging Agency for SOC Services at Hyderabad (All figures in Rs.)							
#	**Role**	**Number of resources to be deployed (A)**	**Unit Price per month (B)**	**Tax (C)**	**Total Price per resource per month (D = B + C)**	**Total for one year**	**Total for three years**
1	SOC L1 Support Engineers (5 resources required for 24x7 SOC Operation)	L S					
2	SOC L2 Support Engineers	2					
	Total Cost						

L1 Resources for 24x7 Operations – Please quote price per month, taxes, total monthly price, price for one year and price for three years.

L2 Resources – Please quote price per resource per month, taxes, total monthly price, price for one year and price for three years.

Table C: -

Sr. No.	**Service Area**	**Service Onetime Price (in Rs)**
1	SIEM & Security Tools implementation GAP analysis Services (One Time)	
2	Tax	
	Total Cost	

TCO (Totals of Table A + B + C)	

Annexure K – Proforma of Bank Guarantee

Date

Beneficiery:NATIONAL PAYMENTS CORPORATION OF INDIA

(Please insert complete address)

Performance Bank Guarantee No:

We have been informed that----------(hereinafter called "the Supplier") has received the purchase order no. **"----------" dated ----------** issued by National Payments Corporation of India (**NPCI**), for **----------** (hereinafter called "the Purchase Order").

Furthermore,we understand that, according to the conditions of the Purchase order, a Performance Bank Guarantee is required.

At the request of the Supplier,We ----------(name of the Bank), the issuing Bank to furnish the details of its incorporation, and having its registered office at ---------- ---------- and, for the purposes of this Guarantee and where claims are payable, acting through its ---- branch presently situated at ---------- ---------- (hereinafter referred to as "**Bank**" which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns),hereby irrevocably undertake to pay you without any demur or objection any sum(s) not exceeding in total an amount of **Rs.---------- (in figures) (Rupees---------(in words)------- only)**upon receipt by us of your first demand in writingon or before ---------(Date)declaring the Supplier to be in default under the purchase order, without caveat or argument, or your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

Please note that you may, if you so require, independently seek confirmation with –(Bank Name & Issuing branch address)----------, that this Bank Guarantee has been duly and validly issued.

Notwithstanding anything contained in the foregoing:

(i) The liability of ---------- (Bank), under this Bank Guarantee is restricted to a maximum total amount of Rs. ----------<Amount in figures and words>.

(ii) The liability of ---------- (Bank), under this Bank Guarantee is finally discharged if no claim is made on behalf of NPCI within three months of the expiry of the validity period of this Bank Guarantee viz.from ---------.

(iii) Our liability pursuant to this Bank Guarantee is conditional upon the receipt of a valid and duly executed written claim or demand, by ---------- (Bank)---------- ---------- (Address), delivered by hand, courier or registered post, or by fax prior to close of banking business hours on ---------- (Date) failing which all rights under this Bank Guarantee shall be forfeited and ---------- (Bank), shall stand absolutely and unequivocally discharged of all of its obligations hereunder. This Bank Guarantee shall be governed by and construed in accordance with the laws of India and competent courts in the city of Mumbai shall have exclusive jurisdiction.

Kindly return the original of this Bank Guarantee to ---------- ---------- (Bank & Its Address), upon the earlier of (a) its discharge by payment of

claims aggregating to Rs. -------- <Amount in figures & words>. (b) Fulfillment of the purpose for which this Bank Guarantee was issued; or (c) <Claim Expiry Date>

All claims under this Bank Guarantee will be made payable at ---------- (Bank & Its Address).

{Signature of the Authorized representatives of the Bank}

Annexure L - Non-Disclosure Agreement

This Agreement is made and entered on this -------- day of ----------, 2011 (**"Effective Date"**) between

NATIONAL PAYMENTS CORPORATION OF INDIA, a company incorporated in India under Section 25 of the Companies Act, 1956 and having its registered office at **C-9, 8th Floor, RBI Premises**, **Bandra-Kurla Complex, Bandra (East) Mumbai-400 051** (Hereinafter referred to as "NPCI", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns);

AND

_____, a company registered in _____and having its registered office at _____ (Hereinafter referred to as "-------", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns).

The term "Disclosing Party" refers to the party disclosing the confidential information to the other party of this Agreement and the term "Receiving Party" means the party to this Agreement which is receiving the confidential information from the Disclosing Party.

NPCI and ----- shall hereinafter be jointly referred to as the "Parties" and individually as a "Party".

NOW THEREFORE

In consideration of the mutual protection of information herein by the parties hereto and such additional promises and understandings as are hereinafter set forth, the parties agree as follows:

Article 1: Purpose

The purpose of this Agreement is to maintain in confidence the various Confidential Information, which is provided between NPCI and ------ to perform the considerations (hereinafter called "Purpose") set forth in below:

(STATE THE PURPOSE)

Article 2: DEFINITION

For purposes of this Agreement, "**Confidential Information**" means the terms and conditions, and with respect to either party, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to the Purpose (including, but not limited to, information identified as being proprietary and/or confidential or pertaining to, pricing, marketing plans or strategy, volumes, services rendered, customers and suppliers lists, financial or technical or service matters or data, employee/agent/ consultant/officer/director related personal or sensitive data and any information which might reasonably be presumed to be proprietary or confidential in nature) excluding any such information which (i) is known to the public (through no act or omission of the Receiving Party in violation of this Agreement); (ii) is lawfully acquired by the Receiving Party from an independent source having no obligation to maintain the confidentiality of such information; (iii) was known to the Receiving Party prior to its disclosure under this Agreement; (iv) was or is independently developed by the Receiving Party without breach of this Agreement; or (v) is required to be disclosed by governmental or judicial order, in which case Receiving Party shall give the Disclosing Party prompt written notice, where possible, and use

reasonable efforts to ensure that such disclosure is accorded confidential treatment and also to enable the Disclosing Party to seek a protective order or other appropriate remedy at Disclosing Party's sole costs. Confidential Information disclosed orally shall only be considered Confidential Information if: (i) identified as confidential, proprietary or the like at the time of disclosure, and (ii) confirmed in writing within Seven (7) days of disclosure.

Article 3: NO LICENSES

This Agreement does not obligate either party to disclose any particular proprietary information; to purchase, sell, license, transfer, or otherwise dispose of any technology, services, or products; or to enter into any other form of business, contract or arrangement. Furthermore, nothing contained hereunder shall be construed as creating, conveying, transferring, granting or conferring by one party on the other party any rights, license or authority in or to the Confidential Information disclosed under this Agreement.

Article 4: DISCLOSURE

1. Receiving Party agrees and undertakes that it shall not, without first obtaining the written consent of the Disclosing Party, disclose or make available to any person, reproduce or transmit in any manner, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except both parties may disclose any Confidential Information to their Affiliates, directors, officers, employees or advisors of their own or of Affiliates on a "need to know" basis to enable them to evaluate such Confidential Information in connection with the negotiation of the possible business relationship; provided that such persons have been informed of, and agree to be bound by obligations which are at least as strict as the recipient's obligations hereunder. For the purpose of this Agreement, Affiliates shall mean, with respect to any party, any other person directly or indirectly Controlling, Controlled by, or under direct or indirect common Control with, such party. "Control", "Controlled" or "Controlling" shall mean, with respect to any person, any circumstance in which such person is controlled by another person by virtue of the latter person controlling the composition of the Board of Directors or owning the largest or controlling percentage of the voting securities of such person or by way of contractual relationship or otherwise.

2. The Receiving Party shall use the same degree of care and protection to protect the Confidential Information received by it from the Disclosing Party as it uses to protect its own Confidential Information of a like nature, and in no event such degree of care and protection shall be of less than a reasonable degree of care.

3. The Disclosing Party shall not be in any way responsible for any decisions or commitments made by Receiving Party in relying on the Disclosing Party's Confidential Information.

Article 5: RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

The parties agree that upon termination/expiry of this Agreement or at any time during its currency, at the request of the Disclosing Party, the Receiving Party shall promptly deliver to the Disclosing Party the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Receiving Party or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

Article 6: INDEPENDENT DEVELOPMENT AND RESIDUALS

Both parties acknowledge that the Confidential Information coming to the knowledge of the other may relate to and/or have implications regarding the future strategies, plans, business activities, methods, processes and or information of the parties, which afford them certain competitive and

strategic advantage. Accordingly, nothing in this Agreement will prohibit the Receiving Party from developing or having developed for it products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in the Confidential Information provided that the Receiving Party does not violate any of its obligations under this Agreement in connection with such development.

Article 7: INJUNCTIVE RELIEF

The parties hereto acknowledge and agree that in the event of a breach or threatened breach by the other of the provisions of this Agreement, the party not in breach will have no adequate remedy in money or damages and accordingly the party not in breach shall be entitled to injunctive relief against such breach or threatened breach by the party in breach.

Article 8: NON-WAIVER

No failure or delay by either party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement thereof or the exercise of enforcement of any other right, remedy or power.

Article 9: JURISDICTION

If any dispute arises between the parties hereto during the subsistence or thereafter, in connection with or arising out of this Agreement, the dispute shall be referred to arbitration under the Indian Arbitration and Conciliation Act, 1996 by a sole arbitrator mutually agreed upon. In the absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrators, one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. Arbitration shall be held in Mumbai, India. The proceedings of arbitration shall be in the English language. The arbitrator's award shall be final and binding on the parties.

Article 10: GOVERNING LAW

This Agreement shall be governed exclusively by the laws of India and jurisdiction shall be vested exclusively in the courts at Mumbai in India.

Article 11: NON-ASSIGNMENT

This Agreement shall not be amended, modified, assigned or transferred by either party without the prior written consent of the other party.

Article 12: TERM

This Agreement shall remain valid from the date last written below until the termination or expiry of this Agreement. The obligations of each Party hereunder will continue and be binding irrespective of whether the termination / expiry of the Agreement for a period of three years after the termination / expiry of this Agreement.

Article 13: INTELLECTUAL PROPERTY RIGHTS

Neither Party will use or permit the use of the other Party's names, logos, trademarks or other identifying data, or otherwise discuss or make reference to such other Party or infringe Patent, Copyrights, in any notices to third Parties, any promotional or marketing material or in any press release or other public announcement or advertisement, however characterized, without such other Party's prior written consent.

Article 14: GENERAL

1. Nothing in this Agreement is intended to confer any rights/remedies under or by reason of this Agreement on any third party.

2. This Agreement and the confidentiality obligations of the Parties under this Agreement supersedes all prior discussions and writings with respect to the Confidential Information and constitutes the entire Agreement between the parties with respect to the subject matter hereof. If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provisions or part(s) thereof shall be stricken from this Agreement.

3. Any breach of any provision of this Agreement by a party hereto shall not affect the other party's non-disclosure and non-use obligations under this Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement by their duly authorized representatives as of the Effective Date written above.

NATIONAL PAYMENTS CORPORATION OF INDIA	**Successful Bidder Name**
By:	By:
Name:	Name:
Designation:	Designation: