**THE CLEARING CORPORATION OF INDIA LTD**

# REQUEST FOR PROPOSAL

**FOR**

Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed

**RFP No: CCIL/IT/RFP/SG/26/082** **Dated: 04-August 2026**

Office Address: CCIL Bhavan, S. K. Bole Road, Dadar (W), Mumbai – 400028

Website: https://www.ccilindia.com

## Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to contractors whether verbally or in documentary form by or on behalf of The Clearing Corporation of India Limited (CCIL), is provided to the contractors on the terms and conditions set out in this RFP document.

This RFP document is not an agreement by CCIL to any parties other than the applicants who are qualified to submit the proposal. The purpose of this RFP document is to provide contractors with information to assist the formulation of their proposal. This RFP document does not claim to contain all the information each contractor may require. Each contractor 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. CCIL 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. CCIL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP document.

Prospective contractors shall regularly visit CCIL's website, www.ccilindia.com for any changes / development in relation to this RFP.

---

The content and RFP are intellectual property of CCIL. No part or material of this RFP document should be published on paper or on electronic media without prior written permission from CCIL.

# Contents


1. INTRODUCTION ..... 6
2. PURPOSE OF RFP ..... 7
3. RFP SCHEDULE ..... 7
4. INSTRUCTIONS FOR SUBMITTING PROPOSAL ..... 8
5. PREQUALIFICATION/ELIGIBILITY CRITERIA ..... 10
6. SCOPE OF WORK/COVERAGE ..... 11
7. EXPECTED DELIVERABLES / OUTCOMES ..... 17
8. ROLES AND RESPONSIBILITY MATRIX ..... 23
9. PROPOSAL EVALUATION AND RIGHT TO NEGOTIATE ..... 24
10. COMMERCIAL PROPOSAL ..... 25
11. TIME TO DELIVER ..... 26
12. GENERAL TERMS & CONDITIONS ..... 26
13. DUE DILIGENCE ..... 27
14. COST OF RFP DOCUMENT ..... 27
15. LANGUAGE OF PROPOSAL ..... 28
16. PROPOSAL CURRENCY ..... 28
17. PROPOSAL EVALUATION ..... 28
18. PROPOSAL REJECTION ..... 28
19. PROPOSAL TERMS & SUBMISSION INSTRUCTIONS ..... 29
20. PRICE NEGOTIATION ..... 29
21. PAYMENT TO MSME ..... 29
22. LIABILITY ..... 29
23. LIQUIDATED DAMAGES FOR DELAY IN DELIVERABLES ..... 30
24. SERVICE LEVEL EXPECTATIONS ..... 30
25. TERMINATION OF CONTRACT ..... 31
26. NOTICES ..... 32
27. MATTERS FOR CONSULTATION ..... 32
28. HEADINGS ..... 32
29. PUBLICITY ..... 33
30. APPLICABLE LAW ..... 33
31. INSOLVENCY ..... 33
32. UNFAIR MEANS ..... 33
33. COPYRIGHTS, PATENTS AND OTHER PROPRIETARY RIGHTS ..... 34
34. CONFIDENTIAL NATURE OF DOCUMENTS AND INFORMATION ..... 34
35. COMPLIANCE WITH RULES AND REGULATIONS ..... 35
36. ENVIRONMENT, SOCIAL AND GOVERNANCE PRINCIPLES ..... 35

37. VARIATIONS ..... 36
38. IS SECURITY ..... 36
39. ENTIRE RFP ..... 37
40. NO AGENCY ..... 37
41. CONTRACT AMENDMENTS ..... 37
42. QUALITY ASSURANCE AND COMMITMENTS ..... 37
43. REMEDIES ..... 38
44. WAIVER OF REMEDIES ..... 38
45. RETURN OF INFORMATION ..... 38
46. ABSENCE OF LITIGATION ..... 38
47. INDEMNITY ..... 39
48. LIMITATION OF LIABILITY ..... 41
49. COUNTERPARTS ..... 41
50. ADMISSION AND WORKING AT THE SITE ..... 41
51. INDEPENDENT CONTRACTOR ..... 42
52. ANTI-CORRUPTION CLAUSE ..... 42
53. FORCE MAJEURE ..... 42
54. LEGAL BINDING: ..... 43
55. NO THIRD-PARTY BENEFICIARY ..... 43
56. DISPUTES ..... 44
57. CONTRACTOR TO INFORM ITSELF ..... 44
58. INJUNCTIVE RELIEF ..... 44
59. OBLIGATION TO DISCLOSE ..... 45
60. RIGHT TO AUDIT ..... 45
61. ASSIGNMENT ..... 45
62. RELATED PARTY DISCLOSURE ..... 45
63. FINAL PAYMENT ..... 46
64. ESCALATION MATRIX ..... 46
65. CONTRACTOR'S REPRESENTATION ..... 46
66. CONFIDENTIAL NATURE OF DOCUMENTS AND INFORMATION ..... 47
67. WARRANTY ..... 48
68. NO INFRINGEMENT ..... 49
69. ARBITRATION ..... 49
70. GOVERNING LAW AND JURISDICTION ..... 49
71. BACKGROUND VERIFICATION ..... 50
72. MANDATORY DISCLOSURE OF CYBER INCIDENTS/IS INCIDENTS ..... 50
73. IMPLEMENTATION OF SECURITY MEASURES ..... 50

**74. CONTRACT AWARD .....50**
**75. QUERIES AND CLARIFICATIONS .....51**

## 1. Introduction

a. Clearing Corporation of India Ltd. (CCIL) (CIN: U65990MH2001PLC131804) was set up in April, 2001 to provide guaranteed clearing and settlement functions for transactions in Money, G-Secs, Foreign Exchange and Derivative markets. The introduction of guaranteed clearing and settlement led to significant improvement in the market efficiency, transparency, liquidity and risk management/measurement practices in this market along with added benefits like reduced settlement and operational risk, savings on settlement costs, etc. CCIL also provides non-guaranteed settlement for Rupee interest rate derivatives and cross currency transactions through the CLS Bank. CCIL's adherence to the stringent principles governing its operations as a Financial Market Infrastructure has resulted in its recognition as a Qualified Central Counterparty (QCCP) by the Reserve Bank of India in 2014. It has also set up a Trade Repository to enable financial institutions to report their transactions in OTC derivatives.

   For more details, please visit the website at www.ccilindia.com

b. CCIL has continuously evolved over the years with the shifting paradigms of the financial arena to take on various roles in the financial market. Through its fully owned subsidiary, Clearcorp Dealing Systems Limited (CDSL), CCIL has introduced various platforms for electronic execution of deals in various market segment. Further, CDSL has developed, implemented and manages the NDS-OM - the RBI owned anonymous electronic trading system for dealing in G-Secs and also for reporting of OTC deals as well as the NDS-CALL platform which facilitates electronic dealing in the Call, Notice & Term Money market.

c. Legal Entity Identifier India Limited (LEIL) - A Wholly Owned Subsidiary of The Clearing Corporation of India Ltd. acts as a Local Operating Unit (LOU) for issuing globally compatible Legal Entity Identifiers (LEIs) in India. The Legal Entity Identifier (LEI) is a global reference number that uniquely identifies every legal entity or structure that is party to a financial transaction, in any jurisdiction. LEIL assigns LEIs to any legal identity including but not limited to all intermediary institutions, banks, mutual funds, partnership companies, trusts, holdings, special purpose vehicles, asset management companies and all other institutions being parties to financial transactions.

d. CCIL and its subsidiaries are ISO/IEC 27001 certified since 2006 for securing its information assets and in July 2018 CCIL has been recertified for conforming to the new standard ISO 27001:2022

***Definitions***

a. RFP shall mean Request for Proposal. Bid, Tender and RFP are used to mean the same.

b. "Bid" means the written reply or submission of response to this RFP.

c. Bidder/Service Provider means an entity/company/firm who meets the eligibility criteria given in Annexure-III of this RFP and willing to provide the service as required in this bidding document.

d. "Services" means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and other obligation of the Vendor covered under the RFP.

## 2. Purpose of RFP

*a)* This Request for Proposal document ("RFP") has been prepared solely to enable The Clearing Corporation of India Ltd. ("CCIL") for obtaining proposals to appoint a competent agency/company to provide "**Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed service" for three years**.

b) Service Providers are requested to submit proposal in accordance with the enclosed Request for Proposal (RFP) terms. Information provided here should be used for its intended scope and purpose only. Retention of this RFP documents signify your agreement to treat the information as confidential.

## 3. RFP Schedule

Information on important dates and time related to this RFP is as follows

| Sr. | Description | Details |
|---|---|---|
| 1 | Name of RFP | Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed |
| 3 | Release Date of RFP | 04/08/2026 |
| 4 | RFP clarifications contact details | Mr. Surendra Gupta<br>E-mail: surendrag@ccilindia.co.in<br>Phone: +91-22-61546419<br>Mob - 9821764724 |

| | | |
|---|---|---|
| 5 | Last date and time of receiving Service Provider s' Pre-Bid clarifications by email | 10/08/2026 up to 18.00 Hrs |
| 6 | Last date of Proposal submission | 13/08 /2026 up to 18.00 Hrs |
| 7 | Address for RFP Response | Mr. Surendra Gupta<br>AVP – Risk Management Department<br>The Clearing Corporation of India Ltd.<br>CCIL Bhavan,<br>S. K. Bole Road,<br>Dadar (West),<br>Mumbai - 400 028<br>Tel. No. 61546419 |

*Table 1 RFP Schedule*

Proposals received after the due date and time specified will not be accepted.

## 4. Instructions for submitting proposal

Service Providers are advised to go through the entire document before submission of Bids to avoid any chance of elimination.

**The RFP response document should have following format:**

| S/N | Envelope | Contents |
|---|---|---|
| 1 | Sealed Envelope 'A' | **Technical Bid**<br>• Envelope should be titled as "Bidder Name - Technical bid for Darkweb_Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed"<br>• The following documents shall be inserted inside Envelope A<br>1. Technical Proposal<br>2. Covering Letter Format - (as per Annexure-I)<br>3. Contractor Profile Form (as per Annexure II)<br>• All relevant supporting documents as per the requirements of the above Annexures and eligibility criteria. |
| 2 | Sealed Envelope 'B' | **Financial Bid**<br>• Envelope Should be titled as "Bidder Name - Financial bid for Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed"<br>• Commercial Proposal (as per Annexure III) and Commercial |

| | | |
|---|---|---|
| | | Proposal Format Annexure -IV in one sealed cover. |
| 3 | Sealed Envelope 'C' | Envelope A and B altogether to be put in a single envelope super-scribed "Bidder Name" "RFP Submission for Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed". |

- Bids sealed in accordance with the Instructions to Bidders should be delivered at the address as mentioned at RFP Schedule table.

- The service provider is expected to examine all instructions, terms & conditions in the RFP document and furnish all requisite information as stipulated herein.

- The RFP response document should be page numbered and appropriately flagged and must contain the list of contents with page numbers.

- Any deficiency in the documentation may result in the rejection of the Proposal.

- The bid should be signed by the bidder or any person duly authorized to bind the bidder to the contract. The signatory should give a declaration and through authenticated.

- Submitted Proposals shall remain valid for 30 days from the last date of submission. A proposal valid for a shorter period may be rejected as non-responsive.

- CCIL reserves the right to request the Service Provider to extend the validity of the proposal through official correspondences.

- All commercials shall be expressed in Indian Rupees only.

- The response shall be in English Language.

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

- Any clarification of the RFP Documents may notify CCIL through email any time prior to the deadline of query.

- Bidders should submit the queries giving reference to document number, clause number, documentary evidence, establish that he/she is empowered to sign the bid documents and bind the bidder.

## *5.* Prequalification/Eligibility Criteria

The Service Provider must be an Indian firm/LLPs/ organization/company registered under Companies Act and should have been in existence for minimum of Three years as on the date of RFP.

- The bidder/OEM must have experience of proposed AntiPhishing, Brand Abuse

monitoring, Darkweb services and Cyber Threat Intelligence must have been successfully provided or currently being provided in at least 2 Banks/ BFSI Organizations in India, during last 3 years as on bid submission date. The period for which the services have been availed or are being availed by the client organization should be at least one year. (Two references should be provided from BFSI

- The date of incorporation of the bidder should be older than three years (less than 1st April 2023. (Certificate of registration /incorporation should be provided)
- Neither the OEM nor the Service Provider should have been currently blacklisted by any financial institution/ regulator in India or abroad. (Declaration on Letter should be provided)
- The Service Provider should have office in Mumbai and should provide list of office location(s) in Mumbai with address and contact numbers.
- The Service Provider must possess the requisite experience and capabilities/ competence to meet the requirements as described in this RFP.
- The Service Provider should have at least 5 deployments in similar technology (references should be given)
- Joint bids/ consortium arrangements are not permitted.

## 6. Scope of Work/Coverage

CCIL intends to procure a Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed which has the features including but not limited to the following.

### 6.1 Dark Web Monitoring

- ❖ The services provided by Bidder should include (but not be limited to): Intellectual Information assets exposed or leaked
- ❖ Monitoring activity and content search related to cyber threats that are of interest to the CCIL and its subsidiaries like “listed under cyber-attack”
- ❖ Monitoring of the Cyber threat trends to financial Services, financial Infrastructure, and Central counterparty clearing houses (CCPs) world-wide. Monitoring Industry Threats (if any)
- ❖ Credential Leak found
- ❖ IT Infrastructure Information which is Targeted or Leaked

- Mentions e-mail addresses and credentials
- Mentions of IP Addresses and Infrastructure
- Monitor Malicious or Typosquat Domains registrations
- Monitor Malicious Domain Certificate registrations (if any)
- Should provide Who-is information for Typosquat Domains
- Continuous monitoring of Fake/Threat domains for different stages of threats like hosting on C2 or Phishing host IP (if any)
- Continuous monitoring of Typosquats domains for any registration of MX records (if any)
- Monitor for Passive DNS records for typosquat domains (if any)
- Information on (alleged) data breaches pertaining to CCIL's sensitive information such as (customer or member bank data, exposed in the public domain or other forums)
- The proposed solution should monitor the Dark Web looking for compromised sensitive data to proactively mitigate impact after breaches.
- The Bidder should monitor online forums on Darkweb, Deepweb and Surface web for the Data Leak (information and Documents related to the CCIL and its Customers).
- The solution must have capability in tracking Threat actor groups as well as various ransomware operations targeting BFSI sector or financial institutions.
- The solution must provide data/information/intelligence related to threat actor, attack campaign, analysis report, tactics, techniques and protocols (TTPs) and profile the Threat Actors.
- The service must provide Intelligence in near real- time as new information or context is gathered from various sources.
- Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy without organization actually going onto Dark web to look for evidence.
- The solution / service should incorporate a range of multi- layered monitoring services and analysis techniques and correlates data across a range of resources including:
    - Tor, onion and alternative networks.
    - Dark Net blogs, forums, chat rooms.
    - Logs and Cookies -IRC conversations.

- Black market and criminal auction sites
- Ransomware leak

❖ Other communication channels where cyber-criminals congregate to sell/ buy services and tools and exchange knowledge for CCILs brand.

### 6.2 Brand Abuse Monitoring

Brand abuse monitoring service to perform proactive cybersecurity and reputational risk management that detects and mitigates misuse, impersonation, or attacks targeting an CCIL's brand, digital assets, and key leadership (KMP) across online and underground spaces including the surface web, deep web and dark web.

❖ 24x7 anti-phishing services to scan critical websites and Mobile Apps for Anti-Phishing, Anti-Malware, Anti- Pharming, Anti- Defacement, Anti- Rogue, Anti-Trojan and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown.

❖ The Bidder should be able to provide anti-phishing domain monitoring, brand abuse support services-for CCIL's public websites, Internet facing websites and social media accounts.

❖ Continuous monitoring of Typosquats domains for any registration of MX records.

❖ Fake Apps on AppStore like Google Play, Apple Store etc. (if any)

❖ Monitor for Passive DNS records for typosquat domains. (if any)

❖ Monitoring social network profile related to CCIL's account.

❖ Anti-phishing and domain monitoring services

❖ Compliance with regulatory advisory on phishing attacks

❖ Social media threat protection services

❖ The Bidder should review CCIL's websites on a periodic basis and suggest anti-phishing measures to be taken.

❖ The Bidder should have the capability for 24x7x365 detection and monitoring for phishing, pharming and brand abuse attacks targeting the CCIL (logo, URL Domain, digital watermark etc.) & CCIL IFSC.

❖ Monitoring potential logo abuse for organization logo (if any)

- The Service should support 100 takedowns of phishing sites and brand abuse within 24 hours during contract period. The Bidder should be capable of blocking of the phishing sites in web browsers.
- Block / takedown / shutdown of the Brand Abuse (Social media violations), including fast flux attacks on CCIL, anywhere in the world within five days of creation of such sites.
- It would be great if the bidder has tie-ups with Browser providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites through built-in Phishing and Malware Protection.
- Bring down the reactivated phishing site at earliest which was earlier detected as phishing site.
- Monitor spam traps to detect phishing mails.
- The Bidder should track new domain name registrations to detect any spoofed site being registered.
- Identify fake news about the organization, any fake sites / scam / misinformation in the name of Company.
- Identification of account impersonation activity
- The solution must provide the monitoring of Exposed Top Managements credentials and Executive mentions / Discussion on Top Management on Dark Web
- The Bidder/OEM should be member of Anti-Phishing Working Group (APWG).
- The Bidder should have global partnership with domain name registrars, application distribution platforms and ISPs for easier take downs of phishing sites anywhere in the world.
- The Bidder should monitor networks known to be source of attacks and/or points of collection of compromised data, compromised devices, Malicious URL's, malicious command and control sites.
- The Bidder should be able to support shutting down/blocking of Trojans, malware, phishing sites irrespective of region of origin or browsers or ISPs.
- The Bidder should monitor similar domain name registrations.

- ❖ The Bidder should provide weekly, monthly & quarterly reports to the CCIL via email. Additionally, whenever incidents are reported/ resolved, CCIL is to be notified via email.
- ❖ The service provider should provide access to Dashboard for CCIL which will be utilized for activities like logging of incidents, ascertaining status of current/closed incident, generating reports of the reported incidents etc. as per requirement.
- ❖ Perform brand monitoring and protection including a variety of sources, feeds, locations, and repositories, but not limited to:
  - o Messaging Suite – Spam, IM, SMS
  - o Malicious Website/URL Scanning
  - o DNS Suite (Domain Name Service) Brand Suite
  - o Social Suite – Social media platforms, Blogs, Forums
  - o Fake domains similar to CCIL's domain
  - o Defacement Monitoring
- ❖ Data sources monitored by the Bidder should include (but not be limited to): Domain Names Databases, Monitor Hacker Forums, Junk E-mail Messages, Abuse Mailbox, Internet Relay Chat, Compromised credentials and Brand specific intel
- ❖ The Bidder should not face obstruction in their activity regardless of international border & language.
- ❖ The Bidder should get into meetings and calls on demand.
- ❖ The Bidder should support investigation for phishing incidents.

### 6.3 Cyber Threat Intelligence Feed

The Threat Intelligence Feed is required by CCIL to help stay ahead of cyber threats by keeping an eye on what hackers are doing and looking for signs of trouble before it causes damage. Threat Intelligence Feeds is required to collect up-to-date information from around the internet—like known hacker techniques, malware, and risky websites and share that with security teams so they know what to watch out for.

- ❖ Intelligence must be gathered from various sources, ranging from public sources, technical sources, dark & deep web, Underground forums, special access sites, Code Repositories, Paste bin and human analyst.

- Collection of intelligence from the various sources should be automated, using technologies such as machine learning, temporal analysis and Deep Language Processing, which allows mass collection of intelligence with low false positives, in real time.
- The threat intelligence solution used by the bidder must allow users to request data review or validation of threat intelligence.
- The feed should provide but not limited to:
- Risk lists of vulnerabilities with a configurable update frequency within 24 hours
- Risk lists of Malicious IP, Malicious Domain, URL, Hash, Vulnerability probers, Malware propagation sources with an update frequency in very short TAT.
- Threat actor grouping along with TTP attribution
- Threat Intelligence feed and Advisory must provide basic attributes as part of data feeds based on availability like IP, Domain, Reputation, Confidence, Behavior, Listing over a 90-day window, Geo-location Attributes, Industry Attributes, IP/Domain Ownership Attributes, Attack Behavior Details, Modus of operandi, Malware Behavior Details, Bot Behavior Details, CnC Behavior Details, DNS Exfiltration Details etc.
- Threat feed should be refreshed immediately on any new threat identification or any new attack observed around globe.
- TI feeds should be sourced from actual attacks including inspection of decrypted TLS network traffic (as opposed to synthetic environments or honeypots) happening on Threat Intelligence Feed Provider's sensor network.
- The CCIL shall have access to Bidders/OEM portal for Threat Intelligence.
- The threat intelligence should preferably be able to provide insights into the attackers, campaigns, the targets being attacked and provide guidance on how to protect the CCIL from attacks.
- Bidder must provide intelligence feeds in open standard formats like OpenlOc, Yara, STIX, TAXII etc. and there should not be any vendor proprietary format.
- Integrate with CCIL’s existing SOC tools, vulnerability management tools such as SIEM, SOAR and other devices to integrate the feeds.

- ❖ Intelligence of IOCs must be delivered with full context of related entities, such as related hashes, IPs, CVEs and Threat Actors, Threat Vectors, Malwares, Product impacted etc.
- ❖ Threat Intelligence solution must include vulnerability advisories covering software products, hardware, platforms, and services, enabling timely identification and remediation of security risks.

## 7. Expected Deliverables / Outcomes

Monitor the CCIL's confidential data on the dark web and notifies if found on the dark web. Help CCIL to reduce the time between a data breach occurring and finding out that it occurred

Increase the chances of identifying and reducing the impact of data breaches.

Brand abuse monitoring sites take down as per the RFP scope.

The service provider needs to provide free trainings/ conduct an online workshop to CCIL technical staff.

### Technical Specifications

Proposed product should meet the features / specifications mentioned below:

| | **Dark Web Monitoring** | |
|---|---|---|
| 1 | Create monitor, automate alert and report for threat on Clear/Deep/Dark Web. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 2 | Intellectual property exposed or leaked | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 3 | Monitoring activity and content related to mentions and cyber threats that are of interest to CCIL such as listed as targeted attack | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 4 | Monitoring of the cyber threat trends to CCIL, Payment and Clearing corporation sector of India or another region. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |

| | | |
|---|---|---|
| 5 | Platform should monitor Employee Credential Leaks on Darkweb | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 6 | Brand Mentions on Sensitive Sources | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 7 | Infrastructure Targeted or Leaked | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 8 | Mentions of IP Addresses and Infrastructure | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 9 | Monitoring social network profile related to CCIL or VIP account example twitter | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 10 | Monitor Malicious or Typosquat Domains registrations | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 11 | Should provide Who-IS information for Typosquat Domain | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 12 | Monitor for Brand mentions in sources Messaging platforms like Telegram, Discord etc. (if any) | Good to have feature and bidder to elaborate how this is being achieved using their proposed solution |
| 13 | Monitoring potential logo abuse for organization logo (if any) | Good to have feature and bidder to elaborate how this is being achieved using their proposed solution |
| 14 | Platform should be able to identify any data leak | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 15 | Platform should support Business Email compromise attack monitoring | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 16 | Platform should be able to identify account impersonation | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |

| | | |
|---|---|---|
| 17 | The platform should provide a link to the actual source of data leak | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 18 | Bidder should provide a sample/complete data or database of leaked data/information to the CCIL to confirm the veracity of leaked data/information (as per availability). | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 19 | Bidder should be ready to buy leaked data/information of the CCIL from dark web/ other sources on case to case/ mutual agreement basis. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 20 | Monitor Cybercrime forums on normal web as well as dark web/deep web. The vendor should monitor underground forums, IRC chat rooms, the open web (OSINT), other communication channels etc. where cyber criminals congregate to sell/buy services and tools and exchange knowledge about CCIL data/information. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 21 | The solution/service should have the capability for real-time monitoring of suspected servers used by cybercriminals to identify CCIL sensitive information stored in that server. Such details should be immediately alerted to CCIL so that CCIL can take necessary precautions before such details are available for sale in dark web | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 22 | The solution should have real time search facilities on dark web as per the search criteria given by the CCIL. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| | **Brand Abuse Monitoring** | |

| | | |
|---|---|---|
| 1 | The platform should be able to identify defacements. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 2 | The Bidder should review CCIL's websites on a periodic basis and suggest anti-phishing measures to be taken. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 3 | Monitoring potential logo abuse for organization logo (if any)<br>The Service should support unlimited takedowns of phishing sites and brand abuse during contract period. The Bidder should be capable of blocking of the phishing sites in web browsers. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 4 | The bidder needs to have tie-ups with Browser providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 5 | Bring down the reactivated phishing site at earliest which was earlier detected as phishing site. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 6 | The Bidder should track new domain name registrations to detect any spoofed site being Registered. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 7 | Identify fake news about the organization, any fake sites / scam / misinformation in the name of Company. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 8 | Identification of account impersonation activity | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 9 | Top executive monitoring / VIP account monitoring | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 10 | The Bidder/OEM should be member of Anti-Phishing Working Group (APWG). | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |

| | | |
|---|---|---|
| 11 | The Bidder should have global partnership with domain name registrars, application distribution platforms and ISPs for easier take downs of phishing sites anywhere in the world. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 12 | The Bidder should be able to support shutting down/blocking of Trojans, malware, phishing sites irrespective of region of origin or browsers or ISPs. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 13 | The Bidder should monitor similar domain name registrations. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 14 | The Bidder should provide weekly, monthly & quarterly reports to the CCIL via email. Additionally, whenever incidents are reported/ resolved, CCIL is to be notified via email. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| | **General** | |
| 1 | The WebGUI / console of the solution should be encrypted with SSL (https) and access to it should available 24/7 from anywhere | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 2 | The bid should include on-boarding training for CCIL analyst. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution. |
| 3 | Predictive analysis of social engineering tactics likely to be used | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 4 | Bidder should have the ability to report incidents through all modes of communication (E-Mail, SMS, Phone call, Dashboard etc). The reporting basis should be immediate on detection. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |

| | | |
|---|---|---|
| 5 | Bidder should have the ability to provide advisory / whitepaper of online threats | Good to have feature and bidder to elaborate how this is being achieved using their proposed solution |
| | **Reports** | |
| 1 | The web interface/portal provided to the bank should have provision for the following: CCIL should able to download reports on its own without vendor's support. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 2 | The web interface dashboard should provide threat data, takedown status etc. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 3 | The reporting basis should be immediate on detection | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |

| | | |
|---|---|---|
| | **Cyber Threat Intelligence** | |
| 1 | Global cyber threat intelligence from multiple trusted sources. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 2 | Intelligence on nation-state, cybercrime, hacktivist, insider, and ransomware threats. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 3 | Coverage of:<br>a. Indicators of Compromise (IOCs)<br>b. Indicators of Attack (IOAs)<br>c. Tactics, Techniques and Procedures (TTPs)<br>d. Malware<br>e. Vulnerabilities<br>f. Exploits<br>g. Command and Control (C2) infrastructure<br>h. Botnets<br>i. Phishing campaigns | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 4 | Real-time and scheduled intelligence updates<br>Machine-readable threat feeds. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |

| | | |
|---|---|---|
| 5 | Structured intelligence formats including:<br>STIX 2.x<br>TAXII 2.x<br>OpenIOC<br>JSON<br>CSV<br>XML. | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 6 | Threat Analysis:<br>a. Threat actor profiling<br>b. Malware family analysis<br>c. Campaign tracking<br>d. Attack chain visualization<br>e. MITRE ATT&CK framework mapping<br>f. Kill Chain mapping<br>g. IOC enrichment<br>h. Contextual intelligence | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 7 | Vulnerability Intelligence:<br>CVE monitoring<br>CVSS scoring<br>Exploit availability<br>Exploitation trends<br>Zero-day intelligence<br>Patch prioritization recommendations | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |
| 8 | **Integration:**<br>SIEM platforms<br>SOAR platforms<br>XDR/EDR solutions<br><br>**Integration shall be available through:**<br>REST APIs<br>TAXII<br>Syslog | Must to have and Bidder to elaborate how this is being achieved using their proposed solution |

## 8. **Roles and Responsibility Matrix**

The roles and responsibility matrix between M/s CCIL and selected bidder is as give below

| **Roles and Responsibility Matrix** | **CCIL** | **Selected Bidder** |
|---|---|---|
| **Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed** | | |

| | | | |
|---|---|---|---|
| 1 | Implement and maintain all the necessary services for CCIL, which comprise the complete solution as per the requirements specified. | | √ |
| 3 | Configuration of the Web Management Console for the services. | | √ |
| 4 | The vendor should ensure that services should be available on a 24*7 basis and maintain the uptime as specified. | | √ |
| 5 | Prioritizing the alerts | √ | √ |
| 6 | Identification of Dashboard, Reports and Schedule | √ | |
| 7 | Dashboard, Reports Implementation and analysis | | √ |
| 8 | Creation & Submission of Daily, Weekly, Monthly and ad-hoc report | | √ |
| 9 | Providing on demand report | | √ |
| 10 | Acknowledgment of Daily, Weekly, Monthly and ad-hoc report | √ | |
| 11 | Service review Daily/Weekly/Monthly Basis | √ | √ |
| 12 | Create monitor, automate alert and report for threat on Clear/Deep/Dark Web. | | √ |
| 13 | To buy leaked data/information of the CCIL from dark web/ other sources on case to case/ mutual agreement basis. | √ | √ |
| 14 | Review CCIL's websites on a periodic basis and suggest anti-phishing measures to be taken. | | √ |

## 9. Proposal Evaluation and right to negotiate

CCIL reserves the right to modify/ amend evaluation criteria, re-issue/ re-commence/ cancel the Bid/ RFP process at any time during the RFP process, without assigning any reason for such action. Any decision in this regard by CCIL shall be final, conclusive and binding on the Bidders.

The Bidder shall submit their offers strictly in accordance with the terms and conditions of the RFP Document. Any Bid, which is incomplete or stipulates conditions contrary to the

terms and conditions given in the RFP Document, is liable for rejection. Any decision of CCIL in this regard shall be final, conclusive and binding on the Bidder.

CCIL reserves the right to accept or reject any or all the Bids without assigning any reason whatsoever and without any liability whatsoever and/or any obligation including intimation to the Bidder(s). Any decision of CCIL in this regard shall be final, conclusive and binding on every Bidder and shall not be questioned/ challenged by the Bidder.

CCIL reserves right to negotiate prices submitted with bidders who qualify eligibility and technical evaluation criteria.

**10. Commercial Proposal**

The Commercial Proposal, besides the other requirements of the RFP, shall comprise of the following:

a. Prices quoted in the proposal must be firm and final and shall not be subject to any upward revisions. CCIL reserves the right to negotiate the prices quoted in the proposal to effect downward revision.

b. The price should be in INR and applicable taxes being mentioned separately.

c. Annual Price quoted should be separate for each item as per the format given below:

| Item | Price (Rs.) | Applicable* Tax (Rs.) | Total Price (including taxes) (Rs.) |
|---|---|---|---|
| Annual Subscription and support for Dark Web monitoring, Brand Abuse Monitoring and Cyber Threat Intelligence Feed | | | |
| Total of 1 year | | | |
| Total for 3 years | | | |

(*Subject to applicable taxes)

d. Deployment of Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed Platform solution will be done within 3 weeks from the date of release of PO.

e. The subscription cost of the Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed Platform should be valid for 3 years.

**Payment Terms**

- The 90% of the annual Payment towards license/subscription will be released on activation of subscription license as per the PO and on successful on-boarding to Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed Platform and the remaining 10% on completion the annual subscription for each year.
- Any tax deductible at source shall be deducted by us at the applicable rates.
- No incidental expenses or out of pocket expenses shall be paid.
- Invoice should be serially numbered, duly stamped and signed
- Invoice should contain CCIL's future PO reference number.
- Invoice should contain the Name, Address, CIN, PAN Number, GST ID and all relevant statutory information.
- Invoice should also contain the Name, Address and GST ID of The Clearing Corporation of India Ltd. (GST ID: 27AABCT4143P2ZY)
- If the company is Micro, Small and Medium Enterprises (MSME) compliant, it should be informed to CCIL accordingly during invoicing itself.
- Invoice should contain description of the service, and applicable taxes payable on the same.
- The amount in figures should match the amount in words with the number of transactions.

**11. Time to deliver**

The bidder should deploy Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed Platform solution within 3 weeks from the date of release of PO.

**12. General Terms & Conditions**

Unless otherwise agreed to in writing by CCIL, the following terms and conditions apply to this RFP, in addition to any terms set forth on the face of or attached to or incorporated by reference into this RFP. The response to RFP is subject to an evaluation process. Therefore, it is important that the contractors carefully prepare the proposal. Contractor is

required to respond to the RFP only in the prescribed format. Under no circumstances, the format can be changed, altered and modified.

- Contractor should abide by all the terms and conditions contained in the RFP. Submission of responses will be construed as acceptance to all clauses of the RFP. If the responses contain any extraneous conditions, such responses may be disqualified and may not be considered for the selection process.
- All pages in the proposal should be signed by authorized signatory under seal.
- CCIL reserves the right to accept the whole proposal or such parts thereof as CCIL may in its absolute discretion to decide. CCIL decisions in this respect will be final. CCIL reserves the right to award the contract to the contractor as it deems fit.
- CCIL may, at its discretion, extend the timeline for submission of proposals by amending the RFP Document, without any change to all rights and obligations either party.
- Contractor will propose only those items which are not reaching end of support within 5 years from the date of release of RFP.

**13. Due Diligence**

The contractor is expected to examine all instructions, terms and specifications in this RFP document. Proposal shall be deemed to have been prepared and submitted after careful study and examination of this RFP document with full understanding of its implications. The proposal should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information required by this RFP or submission of a proposal not responsive to this RFP in every respect will be at the contractor's risk and may result in rejection of the proposal.

Contractor should note that CCIL does not make any warranty, express or implied, with respect to the information provided in this RFP or on which the RFP is based.

**14. Cost of RFP Document**

There is no cost for the RFP document. The contractor shall bear all costs associated with the preparation and submission of its proposal and CCIL will, in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the process.

**15. Language of Proposal**

The proposal prepared by contractor, as well as all correspondence and documents relating to the proposal exchanged by the contractor and CCIL shall be in English only.

**16. Proposal Currency**

Prices shall be quoted in Indian Rupee (INR). The quoted Rate/Cost should be inclusive of all costs like Customs/Excise duty etc., if any. Taxes such as Goods & Service Tax shall be indicated separately.

**17. Proposal Evaluation**

Pursuant to the pre-qualification criteria, contractors will be short-listed for technical proposal. Technical proposals will be considered only for the contractors who succeed the prequalification criteria.

CCIL will review the technical proposal of the short-listed contractors to determine whether the technical proposals are substantially responsive. Proposals that are not substantially responsive are liable to be disqualified at the discretion of CCIL. CCIL will first evaluate the technical proposal followed by commercial proposals.

**18. Proposal rejection**

- CCIL reserves the rights to reject the Proposals which are incomplete and / or received after the due date.
- Proposals received through FAX will be rejected.
- CCIL shall not be responsible for non-receipt of proposals by the specified date and time for any reason, including postal holidays or delays.
- CCIL reserve the right to accept or reject any proposal in full or part.
- CCIL reserves rights to choose/select the Unit/Qty, and to suspend this process and reject all quotations or part at any time prior to the award of contract, without thereby incurring any liability to the affected Contractors on the grounds of the purchaser's inaction without assigning any reason. CCIL's decision in this respect will be final.
- CCIL reserves the right to reject the proposals if it finds that any unfair business practices being resorted to by the contractors.

## 19. Proposal Terms & Submission Instructions

Before submitting the proposal, the Contractors are requested to carefully examine the Proposal Documents and the terms and conditions of the contract thereof, and if there appears to be any ambiguity, gap(s) and/or discrepancy between any of the proposal documents they should forthwith refer the matter to CCIL for necessary clarifications and / or confirmation.

## 20. Price negotiation

Prices quoted in the proposal must be firm and final and shall not be subject to any upward revisions. CCIL reserves the right to negotiate the prices quoted in the proposal to effect downward modification. The Proposal Prices shall be indicated in Indian Rupees (INR) only. Negotiation for the said procurement will be conducted either in person by calling qualified contractor OR via e-Auction with Reverse Auction option between the qualified contractors. CCIL reserves the right to further deliberate and discuss the commercials with the lowest or all the participants if the e-Auction results are found to be unreasonable/illogical/unjustifiable or erroneous.

## 21. PAYMENT TO MSME

In case selected bidder is a MSME company and submitted the requisite registration details, the payment will be made within 45 days from the date of acceptance of the report & receipt of proper invoice. The date of acceptance shall be based on the date of acceptance by respective Committees/ Board of the Company. In case of any deficiency in the report or services received by the Company, the payment will be made within 45 days from the date of rectification of the deficiency.

## 22. LIABILITY

Selected bidder is not liable under any circumstances, for losses or damages to CCIL including those claimed by third parties against CCIL, for loss of, or damage to, any records of data, or for any economic, indirect or consequential damages including, but not limited to, loss of business profits, revenues or savings, actual or anticipated, or incidental damages. CCIL shall have no liability whatsoever for any injury to selected bidder

personnel, agents or representatives suffered while on CCIL premises or anywhere else including, without limitation, liability for any damages suffered which results from the malfunction of any equipment. In no event the total liability of both parties shall exceed the total order value.

## 23. LIQUIDATED DAMAGES FOR DELAY IN DELIVERABLES

a) In case the Contractor is not able to complete the delivery of the licenses /solution as per terms of delivery as stipulated, the Contractor shall pay, at CCIL's discretion, liquidated damages at the rate of 0.1% of the order value per day. The levy of liquidated damages shall not relieve the Contractor from their obligation to deliver software license under this RFP. In case the delay exceeds 2 weeks over and above the agreed terms of delivery, CCIL reserves the right to cancel the order unconditionally.

b) Any tax applicable on the liquidated damages amount will be deducted by CCIL at applicable rates, if any.

## 24. SERVICE LEVEL EXPECTATIONS

a) The Bidder shall ensure an uptime of the platform as 99% and in case of failures, penalty to the tune of proportionate amount shall be deducted from the invoice with maximum of 7.5% of yearly subscription value. CCIL would measure the Service Levels on monthly basis however penalty amount, if any, will be adjusted during subsequent payments.

b) Uptime: The percentage uptime shall be calculated on monthly basis as follows: Availability = (Total no of Hours in month – Total Outage Hours in month) x 100% / (Total No of Hours in month).

Bidder should give uptime guarantee of 99% on monthly basis. No payment would be made for a month, if uptime found to be below 94%.

c) "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime during non-business hours with prior intimation to the CCIL. The Scheduled Maintenance Time of one day per month shall not be considered for SLA calculation.

## 25. TERMINATION OF CONTRACT

Either Party shall have the right to terminate the future PO at any time before the expiry of the Term, in writing, in the event of any violation of the terms & conditions upon thirty days prior written notice.

The future PO may be terminated upon the following:

1. In case of a material breach of any of the terms of the future PO by the breaching Party, the non-breaching Party shall notify the breaching Party of the breach so committed. Such breach shall be rectified by the breaching Party within 15 calendar days from the date of receipt of the notice issued by non-breaching Party. If, the breaching Party fails to rectify the breach within such cure period, the non-breaching Party shall have the right to terminate the future PO by giving 30 calendar days' notice in writing to the breaching Party and the future PO shall accordingly stand terminated at the end of the 30th calendar day.
2. This Agreement may be terminated immediately by notice in writing by either Party if the other Party is likely to become or becomes insolvent or makes or attempts to make an assignment for the benefit of creditors or ceases or attempts to cease to do business or institutes or has instituted against it or allows any third party to institute against it, any proceedings for bankruptcy, reorganization, insolvency, or liquidation or other proceedings under any bankruptcy or other law for the relief of debtors; and does not terminate such proceedings within thirty (30) days.
3. Any termination of the future PO howsoever caused, shall not affect any accrued rights or liabilities of other Party nor shall it affect the coming into force or the continuance in force of any provision hereof which is expressly or by implication intended to come into force on or after such termination. The Parties agree that the clause "Confidentiality" shall survive and continue to remain in force in accordance with the terms of the non-disclosure agreement in notwithstanding the termination of the future PO
4. Upon termination of the future PO (a) the right of access granted to the employees/agents/representatives of the contractor to enter the premise of CCIL under the future PO shall cease immediately; (b) shall hand over possession of all

infrastructures, documentation, information or any item provided by CCIL under the future PO; and (c) CCIL will be liable to pay the contract amount for the running month or up to the last date of notice period on prorate basis, whichever is later.

**26. NOTICES**

All notices and other communications required or permitted under this Agreement will be in writing and will be deemed effectively delivered upon receipt by personal delivery, overnight courier service, or facsimile as confirmed by delivery and/ or transmission receipt or to a dedicated e-mail ID as set out herein. Any Party may change its particulars for such communications by giving a 15 business days' prior written notice to the other Party.

Contact person name
For **The Clearing Corporation of India Ltd.**
CCIL Bhavan, College Lane,
S.K.Bole Road
Dadar (W), Mumbai 400 028
Attn: CRO/ CISO

For Contractor: (To be provided by the Contractor)
_____
_____
Attn: _____

**27. Matters for Consultation**

If any matter which is not provided in the future PO or if any question arises concerning the interpretation of the future PO, CCIL and Contractor will confer in good faith and try to resolve the matter.

**28. Headings**

The headings to the clauses of the future PO are for ease of reference only and shall not affect the interpretation or construction of the future PO.

**29. Publicity**

The Contractor agrees not to use, without the express permission of CCIL the name of CCIL to directly promote its business.

Except as otherwise expressly agreed to by CCIL in writing, the Contractor shall not use in advertising, news release, marketing materials, trade publication, publicity or otherwise any trademark, service mark, symbol or logo thereof of CCIL or its affiliates.

**30. APPLICABLE LAW**

The Contractor shall comply with all the applicable laws including but not limited to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and/ or any other data protection laws, as may be made applicable from time to time. Further, Contractor shall be solely responsible for compliance with the provisions of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 by its employees and for educating its employees about prevention of sexual harassment at work place and related issues and in case of any complaint of sexual harassment against the employees of the Contractor or CCIL, the Parties shall take appropriate actions according to the provisions of the aforesaid Act.

**31. INSOLVENCY**

CCIL may terminate the contract by giving written notice to without compensation, if the Contractors become bankrupt, goes in liquidation or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue to CCIL.

**32. Unfair means**

Contractors are advised not to resort to any unfair means /practices directly or indirectly during and after the RFP process. Any such attempt may lead to disqualification from the

process.

**33. Copyrights, Patents and Other Proprietary Rights**

It is hereby acknowledged and agreed by the Contractor that CCIL shall be entitled to all intellectual property and other proprietary rights including but not limited to patents, copyrights, trademarks and design (if any) with regard to products, processes, inventions ideas, know-how or documents and other materials which the contractor has developed for CCIL under the contract and which bear a direct relation to or are produced or prepared or collected in consequence of or during the course of the performance of the contract. The Contractor shall ensure that any provisions of this type necessary to protect the Intellectual Property Rights of the Employer are included in all its contracts with Sub-Contractors

**34. Confidential Nature of Documents and Information**

Information and data that is considered proprietary by either Party or that is delivered or disclosed by one Party ("Discloser") to the other Party ("Recipient") during the course of performance of the Contract, and that is designated as confidential ("Information"), shall be held in confidence by that Party and shall be handled as follows:

The recipient ("Recipient") of such Information shall:

(a) use the same care and discretion to avoid disclosure, publication or dissemination of the Discloser's Information as it uses with its own similar Information that it does not wish to disclose, publish or disseminate; and,

(b) use the Discloser's Information solely for the purpose for which it was disclosed.

Confidentiality of all data and information shall be maintained as aforesaid, not only during the term of this Contract but also thereafter. Confidential information shall also include such oral and written information which should reasonably be deemed confidential by the Contractor whether or not such information is designated as confidential.

The Contractor agrees that prior to assigning any employee or agent or hiring any Sub Contractor or consultant to discharge any of its obligations under this Contract, such employee, agent, Sub-Contractor or consultant shall be required to execute a document containing in substance and form, a confidentiality provision similar to this provision.

The Contractor agrees to release confidential information only to employees, consultants requiring such information on need-to-know basis, and not to release or disclose it to any third party.

Further, Contractor undertakes that it shall be solely liable for any breach of confidentiality by its officers, employees, agents and /or persons who have discontinued to be its employee, officer, agent. Nothing contained herein shall preclude CCIL with other remedies available to it under the applicable laws.

**35. Compliance with rules and regulations**

The Contractor shall at all times during the currency of contract conform to and comply with all the regulations and by the laws of the State or Central Government or of CCIL and of all other local authorities.

**36. Environment, Social and Governance principles**

The Contractor shall comply with the applicable laws and regulations relating to environmental, social and governance ("ESG") principles, such as:

a) promoting and respecting human rights, as provided under various international conventions, treaties, etc. (including the fundamental rights enumerated under Part III of the Constitution of India) and providing a work environment, which respects and upholds individual dignity;

b) abiding by the "National Guidelines on Responsible Business Conduct" released by the Ministry of Corporate Affairs (MCA), to the extent applicable;

c) furnishing the applicable disclosures such as business responsibility & sustainability reporting (BRSR) and BRSR core, etc. (if applicable); and

d) adhering to the anti-bribery and anti-corruption requirements in terms of the clauses titled "Anti-Bribery Clause" and "Anti-Corruption Clause" respectively.

(Collectively referred as "ESG Laws").

The Contractor shall ensure continued adherence to the ESG Laws, including any amendments made therein, from time to time and take all necessary actions to ensure compliance. The Contractor shall respond diligently to CCIL's requests for information on ESG related matters or Contractor's compliance with the ESG Laws. In case any

incident pertaining to the ESG Laws or this clause occurs, the Contractor shall proactively inform CCIL as soon as practicable and shall take all necessary steps to contain and remedy the same. Any breach of this clause shall be deemed to be a material breach of this Agreement.

**37. Variations**

No variations or modifications to any of the terms of future PO shall be valid unless they are reduced in writing signed by or on behalf of the Parties hereto or by mutual consent and subsequent exchange of letter/ email by the authorised representative of either Party.

**38. IS SECURITY**

Personnel from the Contractor working at CCIL's site shall be provided with only the necessary limited physical and logical access to the IT resources like hardware, software, network, e-mail, Internet, etc. for the purpose of installation/configuration of hardware/software if it part of contract. The contractor shall ensure that all its personnel are made aware of and necessary undertaking is obtained to strictly comply with CCIL's Information System (IS) Security policies/ procedures in force. In the event of any lapse/ violation in the above and any breach of IS Security by the personnel from the Contractor, CCIL shall have right to take appropriate action including but not limited to termination of Agreement/contract, termination of induction of concerned personnel and claim the direct, indirect/ consequential damages, arising out of breach of the IS Security policies of CCIL, from the contractor. Further, the Contractor shall ensure that the hardware/software/network/application etc. provided as part of the Contract is free from embedded malicious code and malwares.

During the execution of work under this contract, the Contractor shall ensure that all relevant aspect of Confidentiality, Integrity and Availability shall be maintained during the entire life cycle of the project from initiation to signoff.

The Contractor shall implement and maintain information security policies, procedures, data protection safeguards and ensure compliance by its employees, agents, representatives, and subcontractors. Contractor shall be solely liable for non-compliance by any of its employees, agents, representatives, and subcontractors.

**39. Entire RFP**

CCIL, if necessary, may submit document as required by the Contractor for their internal use. However, in the event of any conflict between the two, CCIL's RFP Terms and Conditions shall prevail over the document submitted. The RFP supersedes all prior purchase order, arrangements and understandings between the Parties and constitutes the entire RFP between the Parties relating to the subject matter hereof. No addition to or modification of any provision of the RFP shall be binding upon the Parties unless made by a written instrument (signed) or by exchange of letter/email by the duly authorised representative of each of the Parties. The Annexures enclosed form part of the RFP and to the extent that they do not conflict with the terms and conditions set out herein.

**40. No Agency**

Nothing herein contained shall be construed as constituting or evidencing any partnership or agency between the Parties

**41. CONTRACT AMENDMENTS**

No variation in, or modification of, the terms of the contract shall be accepted unless a written amendment is exchanged between the parties, duly endorsed by their authorized signatories.

**42. Quality Assurance and Commitments**

The service provided as part of the future PO shall be of the highest grade and quality. The Contractor will make sure that the supplied service has gone through rigorous testing at the Contractor's end. In case CCIL experiences failure of any of the components or software incompatibility during the implementation, CCIL reserves the right to return the delivered software/ licenses at NO cost to CCIL or demand replacement which needs to be supplied within 1 week of reporting of failure.

**43. Remedies**

In the event of termination of future PO for any reason whatsoever, Contractors shall perform their obligations due to CCIL up to the date of termination.
In the event of default by the Contractor, Contractor shall reimburse CCIL for all reasonable expenses incurred by the latter in the enforcement of its rights but neither Party would be liable for any consequential losses to the other.

**44. Waiver of remedies**

No forbearance, delay or indulgence by either Party in enforcing the provisions of the future PO shall prejudice or restrict the rights of that Party nor shall any waiver of its rights operate as a waiver of any subsequent breach and no right, power or remedy herein conferred upon or reserved for either Party is exclusive of any other right, power or remedy available to that Party and each such right, power or remedy shall be cumulative.

**45. Return of Information**

If so requested by CCIL and subject to the provisions of this Agreement or in the event of termination of the future PO for any reason whatsoever, the Contractor shall promptly destroy or cause to be destroyed, or return or cause to be returned to CCIL, all Confidential Information received from or on behalf of CCIL, including all copies or duplicates of such Confidential Information, and all summaries, analyses, compilations, studies, notes, memos or other documents which contain or reflect any Confidential Information.

**46. Absence of Litigation**

The Contractor represents and warrants to CCIL that there are no pending or threatened lawsuits, actions or any other legal or administrative proceedings against the Contractor which, if adversely determined against the Contractor, would have a material adverse effect on the Contractor's ability to perform the obligations under this Agreement.

**47. Indemnity**

**a.** The Contractor will indemnify and keep indemnified and otherwise hold harmless, CCIL, its affiliates, directors, shareholders, officers, employees, authorised representatives, etc. from and against all direct losses, damages, claims, demands, costs and expenses (including legal fees and attorney charges) which CCIL may suffer or incur, as well as all actions, suits and proceedings which CCIL may face and all costs, charges and expenses relating thereto, arising out of:

i. any misrepresentation or inaccuracy of the representations and warranties of the Contractor or any of the representations and warranties as provided by the Contractor being untrue, misleading or incorrect.

ii. any breach, non-fulfilment or failure to perform (whether in whole or part) any obligation or covenant required to be performed by the Contractor pursuant to this Agreement.

iii. any negligence (including delay or deficiency to perform its obligations as per this Agreement), fraudulent act or concealment on the part of the Contractor, as determined by a court of competent jurisdiction.

iv. any loss, damage or liability suffered due to misappropriation, leakage, security breach, or misuse of the Confidential Information, Intellectual Property, User Data, or the Services or of the documents or any other instruments which are in possession of the Contractor or its personnel or any sub-contractor engaged by the Contractor.

v. infringement, misuse, or misappropriation of any Intellectual Property by the Contractor.

vi. any claim, suit, action or proceeding related to the Services provided hereunder.

vii. violation of any Applicable Law.

**b.** The Contractor shall indemnify, defend and hold harmless, CCIL and its officials, agents and employees, from and against all suits, proceedings, claims, demands, losses and liability of any kind of nature brought by any third party against CCIL, including but not limited to, all litigation costs and expenses, attorney's fees,

settlement payments and damages, based on, arising from, or relating to: (a)allegations or claims that the possession of or use by CCIL of any patented device, any copyrighted material, or any other goods, property or services provided or licensed to CCIL under the future PO, in whole or in part, separately or in a combination contemplated by the Contractor's published specifications, therefor, or otherwise specifically approved by the Contractor, constitutes an infringement of any patent, copyright, trademark, or other intellectual property right of any third party; or (b) any acts or omissions of the Contractor, or any one directly or indirectly employed by it in the performance of the Contract, which give rise to legal liability to anyone not a party to the Contract, including, without limitation, claims and liability in the nature of a claim for workers' compensation; (c) for failure to comply with the requirements of the section hereof titled Governing law and Jurisdiction.

**c.** If the Contractor's information or any part thereof or any use thereof is held to constitute infringement, the Contractor shall promptly and at its own expense either: (1) procure for CCIL the right to continue using the Contractor's Information; or (2) replace same with non-infringing Information or (3) modify such Information in a way so that it becomes non-infringing or (4) repay to CCIL, the fee relating to the whole or infringing part.

**d.** If any claim is commenced by a third-party with respect to which the CCIL is entitled to indemnification under this Clause, CCIL will provide notice thereof to the Contractor. CCIL will be entitled, if it so elects and in its sole discretion, to retain control of the defence, settlement, and investigation of any indemnification claim and to employ and engage attorneys to handle and defend the same, at Contractor's sole cost. In the event that CCIL does not elect to retain control of an indemnification claim, the Contractor will control the defence, settlement, and investigation of such indemnification claim, employ and engage attorneys reasonably acceptable to CCIL to handle and defend the same, at the Contractor's sole cost. CCIL will cooperate in all reasonable respects, at the Contractor's cost and request, in the investigation, trial, and defence of such indemnification claim and any appeal arising therefrom. The Contractor will not consent to the entry of

any judgment or enter into any settlement with respect to an indemnification claim without CCIL's prior written consent. CCIL may also, at its own cost, participate through its attorneys or otherwise in such investigation, trial, and defence of any indemnification claim and related appeals.

**e.** Notwithstanding anything contained in this Agreement, the rights granted to CCIL under this Clause will be in addition to and not in substitution for any other remedies, including a claim for damages or specific performance that may be available to CCIL in respect of an indemnification event under the Applicable Law. However, exercise of any alternative legal remedy will not be deemed to have relieved the Contractor of its liability under this Clause.

**48. Limitation of Liability**

CCIL shall have no liability whatsoever for any injury to Contractor personnel, agents or representatives suffered while on CCIL's premises or anywhere else including, without limitation, liability for any damages suffered which results from the malfunction of any equipment. CCIL will not be liable for any indirect, incidental, special or consequential damages, including the loss of profits, revenue, or use or cost of procurement of substitute goods, incurred by the Contractor or any third Party, whether in an action in contract, tort, based on a warranty or otherwise, even if the Contractor or any other person has been advised of the possibility of such damages.

**49. Counterparts**

This Agreement may be executed in any number of counterparts, each of which when so executed and delivered will be deemed an original, and all of which together shall constitute one and the same Agreement.

**50. ADMISSION AND WORKING AT THE SITE**

All the personnel deputed by contractor shall comply with the instructions and follow the required security norms in respect of the personnel, vehicles, materials etc.

## 51. INDEPENDENT CONTRACTOR

Contractor will perform its obligations under the future PO as an independent contractor and in no way will Contractor or its employees be considered employees, agents, partners, fiduciaries, or joint venturers of CCIL. Contractor and its employees will have no authority to represent CCIL or its Affiliates or bind CCIL or its affiliates in any way, and neither Contractor nor its employees will hold themselves out as having authority to act for CCIL or its affiliates.

The Contractor will (i) be solely responsible for payment of all compensation due to the Contractor's employees in connection with this Agreement, (ii) file on a timely basis all tax returns and payments required to be filed or made to any federal, state or local tax authority with respect to the Contractor's performance of Services and receipt of compensation by the Contractor and its employees hereunder and (iii) be responsible for providing, at its expense and in its name, disability, workers' compensation or other insurance as well as any and all licenses and permits necessary for rendering the Services.

## 52. Anti-Corruption Clause

The Contractor shall comply with all applicable laws, statutes, regulations and codes relating to anti-corruption including but not limited to the applicable legislations in India throughout the term of the future purchase order. Further, the Contractor shall maintain adequate policies and procedures at their end to ensure compliance with the said legislations. It is agreed that the Contractor shall not engage in any activity or practice which constitutes an offence under the said legislation including but not limited to offer, pay, consider or benefit, either directly or indirectly an inducement or reward of any kind for any services, or possible services in relation to the future purchase order. Breach of this clause shall be deemed a material breach of the future purchase order.

## 53. FORCE MAJEURE

a. Notwithstanding anything contained in the future PO, neither Party shall be liable for any delay in performing its obligations hereunder if and to the extent that such delay is the result of an event of Force Majeure. In the event of such delay,

the date of performance will be extended for a period equal to the effect of time lost by reason of the delay, as mutually agreed between the Parties.

**b.** For purposes of this clause, **"Force Majeure"** shall include without limitation the following acts or events: (i) natural phenomena, such as storms, hurricanes, floods, lightning, volcanic eruptions, avalanche, blizzard and earthquakes; (ii) explosions or fires arising from lightning or other causes unrelated to the acts or omissions of the Party seeking to be excused from performance; (iii)acts of war or public disorders, civil disturbances, riots, insurrection, sabotage, pandemic, epidemic, lockdowns, terrorist acts, or rebellion; (iv) strikes or labour disputes (v) action by a Governmental Authority, including a moratorium on any activities related to the Agreement; (vi) any loss of insolation that is caused by any natural phenomena and (vii) the inability for one of the Parties, despite its reasonable efforts, to obtain, in a timely manner, any Governmental Approval necessary to enable the affected Party to fulfil its obligations in accordance with the Agreement, provided that the delay or non-obtaining of such Governmental Approval is not attributable to the Party in question and that such Party has exercised its reasonable efforts to obtain such permit. However, it does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of CCIL or Contractor. The above is without prejudice to the rights already accrued by the Parties as a result of their performance or failure to perform either in full or in part, pursuant to their obligations in the future PO, prior to the occurrence of events of Force Majeure.

**54. Legal Binding:**

No Legal binding will exist between the contractor and CCIL until the issuing of the future Purchase Order by CCIL.

**55. No Third-Party Beneficiary**

Save as expressly provided herein, this Agreement is made and entered into for the sole protection and benefit of the Parties to this Agreement and is not intended to convey any

rights or benefits to any third party, nor will this Agreement be interpreted to convey any rights or benefits to any person except the Parties to this Agreement.

**56. Disputes**

CCIL and the Contractor shall make every effort to resolve amicably by direct informal negotiations any disagreement or dispute arising between them under or in connection with the future PO. Failing such settlement, the same shall be referred to a panel of 3 Arbitrators, one to be appointed by the CCIL and the other by Contractor and the third by both the arbitrators. The arbitrator so appointed shall be the Presiding Officer. The procedure shall be in accordance of the provisions of the Arbitration and Conciliation Act, 1996 (as amended from time to time), or any re-enactment for the time being in force. The findings of the Arbitrator shall be final and binding on both the Parties. The venue and seat of Arbitration shall be Mumbai, India and only courts at Mumbai shall have exclusive jurisdiction in all such matters. The Arbitration proceedings shall be conducted in the English language.

**57. Contractor to inform itself**

The Contractor shall fully inform itself of all necessary obligations and statutes under Indian Law or any other applicable law and shall hold CCIL harmless for any such obligations. The Contractor shall also fully inform itself of all obligations and works necessary under the future PO. This shall include, but not be limited to, the knowledge and understanding of the physical, environmental and technical standards required for the provision and operation of the equipment, software and services within India

**58. Injunctive Relief**

The Contractor understands that in the event of a breach or threatened breach of this Agreement by the Contractor, CCIL may suffer irreparable harm and will therefore be entitled to seek injunctive relief to enforce the Agreement in addition to all other remedies available to it.

**59. Obligation to Disclose**

If the receiving Party is required to disclose the Confidential Information of the disclosing Party as part of a judicial process, government investigation, legal proceeding, or other similar process, the receiving Party, where legally permissible, will give prior written notice of such requirement to the disclosing Party. Reasonable efforts will be made to provide this notice in sufficient time to allow the disclosing Party to seek an appropriate confidentiality agreement, protective order, or modification of any disclosure, and the receiving Party will reasonably cooperate in such efforts

**60. Right To Audit**

Notwithstanding anything contained hereinabove, Contractor shall on notice of 03 business days facilitate the CCIL and/or RBI to audit the services being provided by Contractor, limited to and in connection with services as under the Agreement. Such audit shall be done during normal business hours. For avoidance of doubt, such audit will not cause Contractor to be in breach of its organizational confidentiality requirement.

**61. Assignment**

Neither Party shall assign or otherwise transfer, subcontract, pledge or make any other disposition of the future PO or any of its rights, claims and obligations thereunder whether in whole or in part without the prior written consent of the other. Any such unauthorized assignment, transfer, subcontract, pledge or other disposition, or any attempt to do so, shall not be binding on CCIL. However, such action shall not relieve the Contractor from fulfilling its responsibilities under this Contract.

**62. RELATED PARTY DISCLOSURE**

The Contractor shall make prior disclosure of the transactions falling under the 'Related Party Transactions' in terms of the provisions of the Companies Act, 2013, Accounting Standard AS-18 or any other law time being in force and in case the transaction is non-Related Party Transactions, the Contractor shall confirm the same in writing to CCIL.

## 63. FINAL PAYMENT

Acceptance by selected bidder of the final payment on this order/ contract price shall be and shall operate as a release of CCIL from all claims of selected bidder arising out of or in connection with the order.

## 64. ESCALATION MATRIX

Selected bidder shall provide CCIL with an escalation matrix. Details such as name, contact number, email id should be included in the escalation matrix. The escalation matrix should be provided within two weeks of acceptance of this order.

## 65. CONTRACTOR's REPRESENTATION

(Where labour/staff of selected bidder is appointed to perform at CCIL's premises or other locations as decided by CCIL) selected bidder shall take full and sole responsibility for the payment of all wages, benefits and monies (as per the Labour Laws and Rules and Regulations (as amended from time to time there under) due to all the persons and entities used by it in connection with the implementation and execution of the Contract, including but not limited to, the Selected bidder 's employees, permitted subcontractors and suppliers.

Selected bidder shall be subject to the inspection by CCIL for the compliance of various Labour Laws, Rules, Regulations, and Circulars thereunder. Selected bidder agrees to extend its full support at the time of inspection for production of various documents etc. regarding the necessary compliances.

Selected bidder shall obtain adequate insurance to cover losses, damages to its equipment/personnel before commencing the work under this Contract.

Selected bidder shall be solely responsible for any loss/damage to the equipment/personnel not attributable to CCIL's negligence.

Selected bidder shall comply with all laws, ordinances, rules and regulations bearing upon the performance of its obligations under the terms of this Contract.

Selected bidder shall at all times comply with and ensure that the policies and procedures of CCIL have been adhered to by its employees, representatives, agents etc. The Policies and Procedures may be with respect to (i) Occupational health and safety (ii) Security and

Administrative Requirements (iii) privacy and confidentiality (v) general business conduct and behavior etc. CCIL reserves the right to take action against the violation of any of its policies and procedures against selected bidder or its representatives.

Selected bidder shall ensure that their employees/representatives/agents/subcontractors shall adhere to the highest ethical standards and are physically/mentally fit to perform the duties under this Contract.

## 66. CONFIDENTIAL NATURE OF DOCUMENTS AND INFORMATION

Information and data that is considered proprietary by either Party or that is delivered or disclosed by one Party ("Discloser") to the other Party ("Recipient") during the course of performance of this Contract, and that is designated as confidential ("Information"), shall be held in confidence by that Party and shall be handled as follows:

The recipient ("Recipient") of such Information shall:

(a) use the same care and discretion to avoid disclosure, publication or dissemination of the Discloser's Information as it uses with its own similar Information that it does not wish to disclose, publish or disseminate; and,

(b) use the Discloser's Information solely for the purpose for which it was disclosed.

Confidentiality of all data and information shall be maintained as aforesaid, not only during the term of this Contract but also thereafter.

Selected bidder agrees that prior to assigning any employee or agent or hiring any Sub Contractor or consultant to discharge any of its obligations under this Contract, such employee, agent, Sub-Contractor or consultant shall be required to execute a document containing in substance and form, a confidentiality provision similar to this provision.

Further, selected bidder undertakes that it shall be solely liable for any breach of confidentiality by its officers, employees, agents and /or persons who have discontinued to be its employee, officer, agent. Nothing contained herein shall preclude Customer with other remedies available to it under the applicable laws. Information and data that is considered proprietary by either Party or that is delivered or disclosed by one Party ("Discloser") to the other Party ("Recipient") during the course of performance of the Contract, and that is designated as confidential ("Information"), shall be held in confidence by that Party and shall be handled as follows:

The recipient ("Recipient") of such Information shall:

(a) use the same care and discretion to avoid disclosure, publication or dissemination of the Discloser's Information as it uses with its own similar Information that it does not wish to disclose, publish or disseminate; and,

(b) use the Discloser's Information solely for the purpose for which it was disclosed.

Confidentiality of all data and information shall be maintained as aforesaid, not only during the term of this Contract but also thereafter. Confidential information shall also include such oral and written information which should reasonably be deemed confidential by the Contractor whether or not such information is designated as confidential.

The Contractor agrees that prior to assigning any employee or agent or hiring any Sub Contractor or consultant to discharge any of its obligations under this Contract, such employee, agent, Sub-Contractor or consultant shall be required to execute a document containing in substance and form, a confidentiality provision similar to this provision.

The Contractor agrees to release confidential information only to employees, consultants requiring such information on need-to-know basis, and not to release or disclose it to any third party.

Further, Contractor undertakes that it shall be solely liable for any breach of confidentiality by its officers, employees, agents and /or persons who have discontinued to be its employee, officer, agent. Nothing contained herein shall preclude CCIL with other remedies available to it under the applicable laws.

**67. Warranty**

In addition to its standard warranties, Contractor/Service Provider warrants to CCIL that each product furnished hereunder and any component part thereof shall be:

(a) in conformity with the specifications in all respects and fit for the purpose intended

(b) free from faulty workmanship, material or design,

(c) free and clear of all liens, claims, security interests or other encumbrances of any kind, with Contractor having good and marketable title thereto.

Services furnished hereunder shall be performed in a skilled, professional and workman like manner.

**68. No Infringement**

The Seller/ Party, hereby warrants that it is an authorised seller/ reseller of the products and the sale of the products to CCIL under this Agreement does not infringe on or constitute a misappropriation of the Intellectual Property or any other rights of any third party and the sale is in accordance with the provisions of applicable laws including but not limited to The Copyright Act, 1957, Information Technology Act, 2000 and Rules / Regulations framed thereunder as amended from time to time.

**69. ARBITRATION**

In the case of any dispute or any difference between the parties arising out of or in relation to this agreement including disputes or differences as to the validity of this agreement or interpretation of any of the provisions of this agreement, the same shall be resolved by mutual discussion.

Failing such resolution by mutual discussion, the same shall be referred to a panel of 3 arbitrators, one to be appointed by CCIL and the other by selected bidder and the third by both the arbitrators. The arbitrator so appointed shall be the Presiding Officer. The procedure shall be in accordance of the provisions of the Arbitration Act, 1996 (as amended from time to time), or any re-enactment for the time being in force. The venue and seat of Arbitration shall be Mumbai and only courts at Mumbai shall have exclusive jurisdiction in all such matters. The Arbitration proceedings shall be conducted in the English language.

**70. Governing law and Jurisdiction**

The Contractor shall be responsible for compliance with the provisions of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 by its employees and for educating its employees about prevention of sexual harassment at work place and related issues and in case of any complaint of sexual harassment against the employees of the Contractor or CCIL, the Parties shall take appropriate actions according to the provisions of the aforesaid Act.

The Contractor shall comply, at all times, with any and all applicable laws relating to personal data protection and any and all legal conditions that must be satisfied in relation to the collection, transfer, processing, storage, and destruction of personal data (i.e., data

that is capable of personally identifying any individual). including but not limited to Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, made and each of the Party hereby submits to the exclusive jurisdiction of the courts in Mumbai.

**71. BACKGROUND VERIFICATION**

Selected bidder shall conduct and be solely responsible for background checks of its employees, agents, representatives, and subcontractors.

**72. Mandatory disclosure of Cyber incidents/IS incidents**

In the event of a Cyber security/ Information Security incident at Vendor's office, affecting the confidentiality, integrity and availability of CCIL's data/services, directly or indirectly, the Vendor shall, within 24 hours of finding out the incident, report to CCIL details of the incident along with details such as root cause analysis, damage caused, data/ service compromised, action taken to contain the incident. CCIL will ensure that the information received in this regard shall be kept confidential for its use and will be disclosed only to regulators, if required.

**73. Implementation of Security Measures**

The vendor shall be responsible for the implementation of security measures for processing of Dark web forensics data. The vendor shall take the appropriate Technical and organizational measures to protect CCIL's Dark web data against misuse and loss, or against any other Data Protection Breach in accordance with the applicable Data Protection Laws.

**74. Contract Award**

CCIL will award the contract to the successful contractor where the proposal has been determined to be the best valued services through a purchase order. CCIL is entitled to vary the details of its requirement and the contractor shall implement such variations without undue delay, and or penalties, even if the effect of the variations on cost and delivery schedule have not been agreed. Such variations may include increase or

reduction of the hardware / software licenses /services provided that such variations are within what CCIL and the contractor should reasonably expect when entering into the contract. CCIL reserves the right to accept the whole proposal or such parts thereof as CCIL may in its absolute discretion to decide. CCIL's decisions in this respect will be final. CCIL reserves the right to award the contract to the contractor as it deems fit.

**75. Queries and Clarifications**

All Queries/Clarifications requested should be sent by email in the following format:

Format of Request for Clarification/Query

Sir,

Re: RFP No. CCIL/IT/RFP/SG/26/082 dated July 30, 2026 for Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed

Name of Respondent:

Date:

Name of Contact Person from respondent in case of need:

Tel No.:

| S/N | Reference from RFP Section | Query/Clarification |
|---|---|---|
| | | |
| | | |

I have carefully gone through the terms & conditions and qualifying criteria contained in the above referred RFP. I hereby declare that our company/ firm meets all the qualifying criteria as mentioned in the above RFP. I further certify that I am competent officer in my company/ firm to make the above queries.

For M/s (company/ firm name)

Name of Authorized Signatory

## Annexure I

**Covering Letter Format – (Envelope A)**

To,
Chief Risk officer (CRO),
Risk Management Department,
The Clearing Corporation of India Ltd.
CCIL Bhavan,
S K Bole Road, Dadar (West),
Mumbai-400028.

Dear Sir,

Ref: RFP No CCIL/IT/RFP/SG/26/082 Dated 04/08/2026

We, the **<name of the OEM/ vendor>**, having read and examined in detail the subject RFP documents do hereby submit our response.
We confirm that the information submitted has been carefully examined for correctness before submission to you.
In case you require any other information/ documentary proof in this regard during evaluation process, we agree to furnish the same in time to your satisfaction.
We understand that our proposal is binding on us and that you are not bound to accept the same.
We agree to abide by and fulfill all the terms and conditions of the RFP.
We hereby also confirm that our bid confirms to all the proposed terms, conditions of this RFP. We understand that any deviations mentioned elsewhere in the bid may not be considered and evaluated by the CCIL.
We also agree that the CCIL reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

The undersigned confirms that he/she has requisite powers to sign and submit this response.

Thanking you,
Yours faithfully,

(Signature of the respondent)
Printed Name,
Designation & Seal

## Annexure-II

## Contractor Profile Form

Contractors should be meeting all the requisite prequalification criteria as mentioned in RFP above and furnish the requisite details as per the following format:

| | | | |
|---|---|---|---|
| 1 | Name of the Company | | |
| 2 | Registered office (Address) | | |
| 3 | Registered under Micro Small and Medium Enterprises (MSME) Development Act 2006? | Yes / No | |
| | If Yes, Provide MSME Registration No & Certificate Copy | | |
| 4 | Year of incorporation | | |
| 5 | Brief company profile<br>a) Constitution<br>b) Promoters<br>c) Chairman/MD/CEO<br>d) No. of employees<br>e) No. of branches and their locations | | |
| 6 | Financial Details<br>(Last 3 years, in Rs Crores) | **Total Turnover for FY 2025-26** | |
| | | Total Net Profit | |
| | | **Total Turnover for FY 2024-25** | |
| | | Total Net Profit | |
| | | **Total Turnover for FY 2023-24** | |
| | | Total Net Profit | |
| 7 | Products / Services offered | | |
| 8 | Area of expertise | | |
| 9 | Skill sets & competencies | | |
| 10 | Technology Partners / Associates | | |
| 11 | Credentials / Major Clientele List | | |
| 12 | Certification, if any | | |
| 13 | Contact details | | |

| | | |
|---|---|---|
| 15 | Have you been black listed any time by any organization | |

Note: Submit all relevant documents as proof of the above declarations.

**Prequalification checklist:**

| S/N | Description | Submitted By | Document Attached (Yes/No) |
|---|---|---|---|
| 1 | Company Registration document | Email | |
| 2 | Year of Incorporation Certificate | Email | |
| 3 | Copy of Audited Annual Report for past three consecutive years | Email | |
| 4 | Contractor Profile Form | Email | |
| 5 | MSME Certificate | Email | |
| 6 | Company PAN Card | Email | |
| 7 | GST Certificate | Email | |

**Deviation from RFP Terms and Conditions**

| S/N | Section | Clause No | Page No | Deviation and Variation | Remark |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Note: If any deviations are warranted, reasons for such variation should be specified.

## Annexure -III

***Commercial Proposal – (to be physically delivered) - (Envelope B)***

Please note, this annexure is required to be submitted in a sealed Envelope.

To,

Chief Risk officer (CRO),
Risk Management Department,
The Clearing Corporation of India Limited
CCIL Bhavan,
S K Bole Road, Dadar (West),
Mumbai-400028.

Dear Sir,

Ref: RFP No CCIL/IT/RFP/SG/26/082 Dated 04/08/2026

- With reference to the above RFP, having examined and understood the instructions, Terms and conditions, we hereby enclose our Commercial offer for **"Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed",** as detailed in your above referred RFP.
- We confirm that the offer is in conformity with the terms and conditions as mentioned in your above referred RFP. We further confirm that the information furnished in the proposal, annexure, formats, is correct.
- CCIL may make its own inquiries for verification and we understand that the CCIL has the right to disqualify and reject the proposal, if any of the information furnished in the proposal is not correct.
- We also confirm that the prices offered shall remain fixed for a period of ninety (90) days from the date of submission of the offer.
- We also understand that the CCIL is not bound to accept the offer either in part or in full. If the CCIL rejects the offer in full or in part the CCIL may do so without assigning any reasons there for.

Yours faithfully,
Authorized Signatories
(Name, Designation and Seal of the Company)
Date:

## Annexure -IV

***Commercial Proposal Format***

**(To be submitted on company letterhead)**

***RFP for Darkweb Online Brand Abuse Monitoring Service and Cyber Threat Intelligence Feed***

| S/N | Product Description | Price (Rs.) | Applicable Tax (Rs.)* | Total Price (including taxes) (Rs.) |
|---|---|---|---|---|
| 1 | Annual Subscription and support for Dark Web, Online Brand Abuse Monitoring and Cyber Threat Intelligence Feed | | | |
| 2 | Total of 1 Year | | | |
| 3 | Total of 3 Years | | | |

**Note:**

- Contractors need to appropriately specify taxes and % of its applicability.
- Contractor is required to provide the latest available version of the specified software products at the time of license delivery. Accordingly, the contractor may notify CCIL of the revised part number corresponding to the latest version of the software
- All the prices quoted should be in Indian Rupees (INR) only.