TELECOMMUNICATIONS CONSULTANTS INDIA LIMITED
(a Government of India Enterprise)

Advt. No : TCIL/ITTII/47/2023   **Date:02.11.2023**

Advertisement for Hiring of services of 15 contractual manpower in the field of IT and Telecom on Contract basis.

Telecommunications Consultants India Ltd. (TCIL) is a multinational Public Sector Organization under the administrative control of Department of Telecommunications, Ministry of Communications, Government of India. TCIL is operating globally to provide world-class technology and Indian expertise in all fields of Information Communication and Technology.

TCIL requires qualified and experienced Officers for the following post in the field of Cyber Security on Contract basis for deputation on MHA project.

Sl.No.	Post Description	No of Posts	Mini. Experience	Salary per month
1	Senior Technical Program Manager (TOR – 1)	3	7	₹ 250,000
2	Vulnerability and Threat Management Professional (TOR 8)	1	5	₹ 160,000
3	Executive Assistant (Office Expert)	1	3	₹ 65,000
4	Technical Assistant – (CFCFRMS)	1	3	₹ 65,000
5	Malware Researcher (TOR 14)	1	5	₹ 160,000
6	Data Analytics Professional (TOR 15)	4	5	₹ 160,000
7	Cyber Crime Researcher – BFSI (TOR 16)	1	5	₹ 160,000
8	Cyber Crime Researcher – Telecom & IoT (TOR 23)	2	5	₹ 160,000
9	Cyber Threat Analyst (TOR 22)	1	3	₹ 65,000

1. **Contract Period**
   a) The initial period of engagement shall be for 1(one) year and extendable to another one year with annual increment of 6% per year provided project gets extended by MHA.
   b) Upon selection candidate shall sign an agreement with TCIL and MHA (with detailed terms and conditions) to bring the recruitment into effect.
   c) The contractual employee shall not claim any appointment in TCIL during or after the contract period.
   d) The contract may be terminated by giving **one month's** notice.

2. **Entitlements**
   a) **Leave:** 12 days casual leave in a calendar year**,** on proportionate basis.

   b) **Holiday:** Hired Professionals shall be entitled for Gazetted Central Government

holidays.

c) **TA/DA:** No TA/DA shall be admissible for joining the assignment or on its completion. However, TA/DA shall be paid in case the HIRED EMPLOYEE is deputed by MHA for official work and the same shall be governed by provisions contained in Department of Expenditure O.M. No:19047/1/2016-E.IV dated 14.09.2017.

d) **Accommodation:** No accommodation or HRA will be provided by MHA or TCIL.

e) **Powers:** HIRED EMPLOYEE shall not exercise any statutory, legal or financial powers.

f) **Medical insurance:** No medical coverage will be given by MHA or TCIL.

3. **Working hours**
   a) The HIRED EMPLOYEE shall have to work as per the working hours of MHA. However, depending on the exigency of work, one may be required to come early or sit late to complete the time bound work. No overtime would be paid by MHA or TCIL.

   b) HIRED EMPLOYEE shall comply with the oral and written instructions given to them on day to day basis, by the officer(s) authorized by MHA from time to time. They will be bound by office timings, duty, placement, locations, etc., as decided by MHA.

4. **Conduct**

   a) Their conduct should be those becoming of at par with Government servant.

5. **Performance Evaluation**

   a) Performance will be evaluated on quarterly basis by TCIL/MHA.

6. **Termination of engagement**

   a) TCIL may terminate the engagement of HIRED EMPLOYEE if:
   - The person is unable to accomplish the assigned works.
   - The quality of the assigned work is not to the satisfaction.
   - The person fails in timely achievement of the milestones as decided by MHA.
   - The person is found lacking in honesty and integrity.

7. **Necessary Instructions**

   a) Before applying, the candidate should ensure he/she fulfills the eligibility criteria and other norms mentioned in the advertisement.

   b) Experience in the relevant field shall be calculated from the date of attaining the minimum essential qualification(s).

   c) Mode of selection will be Preliminary Skill Test .TCIL/MHA reserves the right to modify the selection procedure, if deemed fit.

   d) TCIL reserves the right to increase /decrease the number of vacancies and cancel the recruitment process at any stage.

   e) TCIL reserves the right to shortlist applicants for interview and not bound to call all

candidates meeting eligibility criteria.

f) The decision of TCIL in all matters would be final and binding, and no correspondence in this regard would be entertained.

g) Last date of receipt of application is **12/11/2023**.

8. Qualification and Work experience

8.1 Senior Technical Program Manager (TOR - 1)

Key Responsibility

Role of the professional is to lead and coordinate with vertical heads, officials of I4C, cybercrime research team etc. to implement creative ideas, engaging with multiple stakeholders, intermediaries and making data-driven decisions for following verticals each.

	Qualification	Work Experience
Essential	B.E/ B.Tech (Computer Science/Computer Engineering/Information Technology/Electronics / Electronics & Communication/Electronics & Telecommunication) / MCA with First Division or with minimum 60% marks in aggregate from a recognized University/Institution	Relevant Experience in domain Cyber Security/ Cyber Crime in execution and management Hands-On experience in Cyber Security Audits, Vulnerability Management, Penetration Testing, ISMS Implementations, Cyber Forensics, Cyber Threat Intelligence.
Desirable	Relevant Certification in Cyber Security / Information Security/ Program Management	Experience of working in Cyber Security/ Information security, strategy, planning & policy formulation

8.2 Vulnerability and Threat Management Professional (TOR 8)

Vulnerability Assessment and Penetration Testing Professional will be responsible to perform task of vulnerability management of organization's infrastructure and perform VAPT on application / network infrastructure on need basis. Professional will also be responsible for Information Security Audits as and when required.

	Qualification	Work Experience
Essential	B.E/ B.Tech (Computer Science/Computer Engineering/Information Technology/Electronics / Electronics & Communication/Electronics & Telecommunication) / MCA with First Division or with minimum 60% marks in aggregate from a recognized University/Institution	Minimum 3 years hands-on experience in domain of Vulnerability Management, Application Security Assessment, Information Security Audits.

Desirable	Relevant Certification in Cyber Security / Information Security	Experience in Red Teaming, Securing critical / sensitive IT infrastructure (Banks, Government etc.)

8.3 Executive Assistant (Office Expert)

Key Responsibilities

Executive Assistant will be responsible for creating presentations, documentations, data entry operations for officers of all verticals. Professional will also be responsible to work on advanced excel, macro programing as and when required.

	Qualification	Work Experience
Essential	Graduate Degree in any field with minimum 60% marks in aggregate from a recognized University / Institution	Minimum 2 years of experience in data entry and making presentations. Must be conversant with Excel Programming, Word, Professional Power Point Presentation.
Desirable	Certification in advanced excel, Microsoft office.	Experience in Macro Programming, Excel Automation etc.

8.4 Technical Assistant - (CFCFRMS)

Professional will be responsible for managing CFCFRMS platform related operational work like user creation/deletion, query resolution, email replies, onboarding intermediaries, troubleshooting law enforcement issues etc.

	Qualification	Work Experience
Essential	Graduate Degree in any field with minimum 60% marks in aggregate from a recognized University / Institution	Minimum 2 years of experience in general support, ticket management, customer support executive etc.
Desirable	Certification related to basic computing concepts.	Experience in financial / Government sector.

8.5 Malware Researcher (TOR 14)

Key Responsibilities

As a member of the Malware Research Team, the candidate would be responsible for setting up malware lab, malware analysis on various platforms (mobile, windows and linux etc.). to create actionable report and coordinate with the concerned agencies.

	Qualification	Work Experience

Essential	B.E/ B.Tech (Computer Science/Computer Engineering/Information Technology/Electronics / Electronics & Communication/Electronics & Telecommunication) / MCA with First Division or with minimum 60% marks in aggregate from a recognized University/Institution	Minimum 3 Year of experience in malware analysis and reverse engineering domain.
Desirable	Relevant certification related to Malware Analysis/Cyber Security.	Experience in incident response (phishing campaigns detection, malware attack, APT etc.)

8.6 Data Analytics Professional (TOR 15)

Key Responsibilities

Data Analyst would be responsible for analyzing the data generated out of NCRP, CFCFRMS, JMIS, Social Media Handles etc. and provide visualization, dashboard creation, trend analysis on periodic basis.

	Qualification	Work Experience
Essential	B.E/ B.Tech (Computer Science/Computer Engineering/Information Technology/Electronics / Electronics & Communication/Electronics & Telecommunication) / MCA with First Division or with minimum 60% marks in aggregate from a recognized University/Institution	3 Year's experience in the field of Data Analytics and Data Science including (not limited to) data correlation, data cleanup, dashboard creation / visualization, OCR etc.
Desirable	Relevant Certification in Data Analytics / Data Science.	Experience with MS-SQL, MongoDB, Power BI, Tableau, Web Scrapping etc. and Perform data profiling, linkage analysis, attribution to identify and abilities to understand anomalies.

8.7 Cyber Crime Researcher - BFSI (TOR 16)

Key Responsibilities

Professional will work on research on in loopholes exploited by cyber criminals using various modus operandi, provide technical and policy level suggestions to counter the same in the field of Banking and Financial Services sector. Professional will overlook operation of CFCFRMS and develop investigation approach as and when required.

	Qualification	Work Experience

Essential	B.E/ B.Tech (Computer Science/Computer Engineering/Information Technology/Electronics / Electronics & Communication/Electronics & Telecommunication) / MCA / MBA with First Division or with minimum 60% marks in aggregate from a recognized University/Institution	Minimum 3 years of experience in the field of banking and financial services domain for cyber security/cyber forensics.
Desirable	Relevant Certification in Cyber Security / Security Operations Center / Incident Response.	Understanding of Payment Technologies like UPI, IMPS, AePS etc; relevant RBI - NPCI regulations.

8.8 Cyber Crime Researcher - Telecom & IoT (TOR 23)

Key Responsibilities

Professional will work on research on in loopholes exploited by cyber criminals in telecom and using various modus operandi, provide technical and policy level suggestions to counter the same in Telecom & IoT sector.

	Qualification	Work Experience
Essential	B.E/ B.Tech (Computer Science/Computer Engineering/Information Technology/Electronics / Electronics & Communication/Electronics & Telecommunication) / MCA / MBA with First Division or with minimum 60% marks in aggregate from a recognized University/Institution	Minimum 3 years of experience in Telecom Security and IoT security.
Desirable	Relevant Certification in Cyber Security / Security Operations Center / Incident Response.	Understanding of telecom infrastructure (4G, 5G), Internet of Things, SIM Box, VoIP etc.

8.9 Cyber Threat Analyst (TOR 22)

Key Responsibilities

Professional will be responsible to prepare Cyber Digest, create actionable report through OSINT, inputs from National Cyber Crime Reporting Portal, Social Media Handles etc., manage in-house information sharing platform.

	Qualification	Work Experience
Essential	Graduate Degree in any field with minimum 60% marks in aggregate from a recognized University / Institution	Minimum 1 years of experience in OSINT, Social Media Analysis, Report Creation, Crime Research
Desirable	Certification related to basic computing concepts, language, cyber security / information security, OSINT.	Experience in financial / Government sector.