National Institute of Electronics and Information Technology, Delhi
Centre 2nd Floor, Parsvnath Metro Mall,
Inderlok Metro Station, Inderlok, Delhi-110052

Eligibility Criteria against the Advertisement vide no. 07/280/2022/NDL/FM for empanelment of IT Resource Persons to be deployed in specific Govt. Department in Delhi/NCR on contract basis

S. No.	Name of The Post/ No. of Positions	Essential Qualification	Consolidated Monthly Salary (Rs.)	Experience (after availing essential qualification) as on -06-07-2022	Job Profile/ Skill Set/ Locations (probably)
01	**Sr. Consultant – CE (4)**	Bachelor's Degree in Technology or Engineering or equivalent in the field of Computer Science / Information Technology / Cyber Security / Electronics and Communications with atleast 60% marks in aggregate. OR M.Tech. in the field of Computer Science / Information Technology / Cyber Security / Electronics and Communications / MCA Degree, with at least 60% marks in aggregate	Rs. 90,000/- to 1,25,000/-	Minimum 10 years experience in the required domain field in areasof Cyber Security as per detailed responsibilities and tasks defined **in para-2 (below)** Desirable: Any certificate related to Cyber security: CEH/CISSP/CISA/ OSCP or Diploma in Cyber security	Age Limit: upto 40 years **For : Delhi/NCR**
02	**Jr. Consultant – CE (2)**	Bachelor's Degree in Technology or Engineering or equivalent in the field of Computer Science / Information Technology / Cyber Security / Electronics and Communications with atleast 60% marks in aggregate. OR M.Tech. in the field of Computer Science / Information Technology / Cyber Security / Electronics and Communications / MCA Degree, with at least 60% marks in aggregate	Upto 60,000/-	6 months experience in the required domain field in areas of Cyber Security as per detailed responsibilities and tasks defined in **in para-2 (below)** OR Any Certification related to Cyber security : CEH/CISSP/CISA/OSCP or Diploma in Cyber Security	Age Limit: upto 40 years **For : Delhi/NCR**

Note: The number of vacancies are tentative and can vary at any point of time as per office requirement.

Para 2- Detailed Responsibilities and Tasks

1. Sr. Consultant (CE)

(a) Senior Analyst

- Acting as resource persons for handling critical incidents and performing analytical tasks in the area of malware/artifact analysis, cyber forensics, threat hunting, breach investigation, operationalization of decoy systems, log analysis, correlation of incidents, analytics
- Data Scientists including operationalization of big data analytics
- Identification of new scientific techniques in incident analysis
- Tracking cyber threats, vulnerabilities reported in various systems/platforms/devices and preparation of vulnerabilities notes and advisories for publishing on website of CERT-In
- Tracking of malware threats and preparation of virus alerts for publishing on website of CERT-In
- Tracking of emerging threats, wider exploitation of vulnerabilities and new cyber-attacks and preparation of current activity for publishing on website of CERT-In
- Finding new vulnerabilities in s/w widely used in constituency , Coordination for vulnerability remediation with stakeholders
- Analysis and taking actions of reported vulnerabilities in systems/websites/networks and processes of organisations in various sectors
- Exploit writing and testing, finding and evaluating new tools/solutions in open source for using and commercial domain for procurement, creating testbeds
- Coordination for tracking of incidents such as website intrusions/defacements, Spam, vulnerable and open services such as open DNS, open NTP, exposed databases etc and coordinating incident response with shift teams
- Scientific ways of log analysis, attacker attribution, trends in IP masquerading (proxy, vpn etc.) , Review of analysis reports, preparing trends reports
- Preparation of guidelines and best practices to prevent recurrence of incidents and enhancing security posture of organisations in various sectors
- To make repository of publicly released incident information in specific sectors such as finance, telecom, power, transport, defence etc for keeping abreast of the current threats and achieve readiness to study and implement early responses
- Collection and analysis of relevant information, reports and data and maintain to help respond to inquiries received from stakeholders and to assist with reviews of documentation such as security architecture designs and security operation procedures
- Providing training to constituency on various areas of cyber security
- Participating in International cyber drills
- Conducting cyber drills/exercises at national level, sectoral /state level and organization level
- Handling of activities related to bilateral / multilateral agreements (MoUs) on cooperation in the area of cyber security and other coordination related tasks.

(b) Cyber security audit and VAPT

- Web Application and mobile application auditing (including Android, and iOS) vulnerability assessments, Compliance audits, Code Reviews
- Source Code Security Audit; inspect the source code for security weaknesses.
- Remote Vulnerability assessment and Security Testing of Web applications.
- Static Source code Vulnerability Audit and Security Testing of websites code.
- Review of authentication, authorization, session and communication mechanisms
- Research and Development of solution to mitigate Application level attacks.
- Review of third-party libraries
- Security validation of cryptographic functions and routines
- Evaluation of tools/solutions for Vulnerability Assessment and Penetration Testing

(c) Analyst /developer/auditor (expert areas)

- Tracking of cyber threat and vulnerabilities and analysis
- Vulnerability analysis, Support for Exploit testing, writing scripts, Advisory preparation
- Preparation of guidelines, case studies and white papers
- Providing assistance to senior analysists for tracking of incidents such as website intrusions/defacements, Spam, vulnerable and open services such as open DNS, open NTP, exposed databases etc and coordinating incident response with shift teams
- Determination of operational and implementation feasibility by evaluating problem definition, requirement analysis, solution design development of the proposed solutions.
- Preparation of specifications, designs, flowcharts, layouts, diagrams of the required application/software.
- Preparation and installation of solutions by determining and designing system specifications, standards, and programming.
- Providing information by collecting, analyzing, and summarizing development and service issues.
- Providing expert guidance to external/internal developers/programmers
- Improving overall development efforts by conducting systems analysis, recommending changes in policies and procedures, recommending platforms and products, testing and approving products.
- Development of scripts/programs according to the specific requirement different internal teams such as Operations/malware analysis/ Infrastructure management
- Leading teams for development of Scripts for aiding in Malware analysis and forensics.
- Web application and mobile application auditing
- Source code review
- Evaluation of tools/solutions for VAPT
- ISMS audits
- Auditing of Industrial Control Systems

2. Jr. Consultant (CE)

Incident Response Team Members

- Support for Incident handling, log analysis ,IT operations
- Collection of evidences from websites, portals, cloud environments, computers, mobile devices including assistance in onsite operations
- Participation in fly-away teams and performing Forensic imaging of systems/devices and log collection
- preliminary analysis of evidences and logs to aid in incident handling
- Maintaining repository of data, indexing, maintenance of files, artifacts including online storage and removal media
- Tracking vulnerabilities, Advisory preparation, maintaining vulnerability database, Inventory of systems and software widely used in constituency
- Tracking of cyber threats and cyber-attacks, sending alerts, maintaining database
- Maintenance of computer systems, networks, devices and databases
- Maintaining of data, data entry and generating reports
- Development and coding for relevant applications tools, portals and writing scripts to aid in incident response
    - Determination of operational and implementation feasibility by evaluating problem definition, requirement analysis, solution design development of the proposed solutions.
    - Preparation of specifications, designs, flowcharts, layouts, diagrams of the required application/software.
    - Preparation and installation of solutions by determining and designing system specifications, standards, and programming.
    - Providing information by collecting, analyzing, and summarizing development and service issues.

    - Identification and study of emerging programming languages and related utilities
    - Implementing secure coding practices
    - Source code audit, unit testing and SDLC for internal applications
- Technical support in the activities of International Cooperation, APCERT Working Groups (IoT Security, Secure Digital Payments, Drills, malware mitigation, information sharing, capacity building),
- Tasks related to meetings and presentations, calls for support and implementation of State/Sectoral CSIRTs
- Operations and maintenance of networks including wireless networks
- Maintenance labs for malware analysis, mobile devices, IoT, Cloud/virtualization solutions
- Deployment and configuration of log collectors, SIEM, Analytics platforms
- Virtualization solution implementation and maintenance
- implementation and maintenance of Advanced Threat Detection solutions within the Centre and in remote locations
- Performing various project management and maintenance tasks relating to the networking infrastructure
- Performing regular security monitoring to identify any possible intrusions, attempts etc.
  Assisting Network Engineers and others in determining the source of a problem
- Rack/server management, server room management, cooling, power consumption monitoring etc. and maintaining relevant records
- Assist in creating system design models, specifications, diagrams and charts to aid Network Administrator.