ODISHA COMPUTER APPLICATION CENTRE
EXPRESSION OF INTEREST(EOI)
Enq.No.:- OCAC-SEGP-INFRA-0007-2022-23002

Odisha Computer Application Centre (OCAC) invites Expression of Interest (EoI) from industry leaders in cyber crime investigation, forensics & cyber intelligence for setting up of Cybercrime Centre of Excellence facility at Bhubaneswar, Odisha.

Details of EoI document is available in the website www.ocac.in & www.odisha.gov.in which may be downloaded by the interested bidders.

The last date of submission of EoI is 02-02-2023, 2 P.M.

General Manager(Admin), OCAC, Plot No.-N-1/7-D, Acharya Vihar, P.O.-RRL, Bhubaneswar-751013, Ph.-2567280/ 2567064/ 2567295

Expression of Interest (EoI)
for
Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility

EOI Ref No- OCAC-SEGP-INFRA-0007-2022/23002

Odisha**C**omputer **A**pplication **C**entre
(TechnicalDirectorateof E&I.T. Department, Government of Odisha) N-1/7-D, AcharyaVihar, P.O. - RRL,
Bhubaneswar- 751013
EPBX: 674-2567280/ 2567064/2567295/
2567283
Fax: +91-674-2567842
E-mailID: contact@ocac.in
Website: www.ocac.in

1. Invitation for EOI/ First stage of two-stage bidding

OCAC invites prospective bidders to setup the “Cybercrime Centre of Excellence” in the Government of Odisha. Proposals received by OCAC shall be evaluated by the Evaluation Committee. A Tender process among the successful bidders qualified during EOI process shall be initiated to select the bidder to execute the work.

Schedule of Events:

SL#	Event	Schedule
1	Last date for submission of queries seeking clarification	17/01/2023, 5PM
2	Date and Time of Pre-bid meeting	19/01/2023, 12Noon (VC Mode (through Microsoft Team))
3	Last date and time for submission of EOI	02/02/2023, 2PM
4	Opening of EOI	02/02/2023, 4PM
5	Presentation/POC	Will be intimated
6	Proposals, in its complete form in all respects as specified in the EoI, must be submitted to OCAC at the address specified below: General Manager (Admin) Odisha Computer Application Center N-1/7-D, Acharya Vihar Square P.O.- RRL, Bhubaneswar - 751013 Tel: 0674-2567280/ 2567064/ 2567295 Fax: +91-674-2567842 Email: gm_ocac@ocac.in	

2. Introduction:

Cybercrime is becoming a global phenomenon and a worldwide concern. As cybercriminals face no boundaries, the traditional law enforcement approach is becoming superseded. A vital aspect to fight against cybercrime is that, the State Law Enforcement Agency is to have Centre of Excellence for Cyber Security. Also to establish cyber intelligence, investigation and forensic units those are fully prepared both from the equipment and the knowledge point of view to face cybercriminals and their destructive actions.

As an initiative, Odisha Computer Application Centre (OCAC) and Government of Odisha is intended to setup Centre of Excellence (COE) for Cyber Security enabled with tools, technologies, process, and trained manpower to combat the Cybercriminals. The COE will be the nodal point of contact and advisory agency for the State in cybercrime investigation and enablement.

To efficiently handle the cybercrime investigations and analytics, it is pertinent to have skilled manpower in these core areas. One of the important aspects of this project is to have an effective cyber security workforce.

3. Objective and Overview:

The key objectives and functional requirement of the Centre of Excellence are -

- To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.
- Planning, designing, and analyzing cyber security capacity building program for the Government of Odisha (GoO).
- To organize Awareness, Training and Education program, as depicted in (but not limited to) the standards like National Institute of Standards and Technology (NIST) Special Publication 800-50, Advisories from NCIIPC and CERT-In.
- To create awareness, train and educate the citizens of Odisha, Police officials of cyber crime department and create a cybersecurity workforce with necessary capacity and capability for cyber resilience.
- To develop necessary workforce within government and law enforcement agencies/public prosecutors, pleaders/judicial officials in digital forensics and technology assisted investigation techniques.
- To develop tools, technologies, Standard Operating Procedures (SOPs) and establish Best Practices.
- To study and develop policies and advisories regarding various domains of Cyber Security and its allied domains, etc.
- To create and facilitate various services regarding Cyber Security and its allied domains.

4. Pre-bid Meeting

- OCAC shall hold a pre-bid meeting (on line) with the prospective bidders on **19.01.2023** at 12 Noon at Odisha Computer Application Centre through Microsoft Team.

    a. The prospective bidder willing to participate in the pre-bid meeting, will have to ensure that their queries for Pre-Bid meeting should reach to the General Manager(Admin), OCAC only through email (**gm_ocac@ocac.in**) with a copy to tushar.mohapatra@ocac.in, debaraj.behera@ocac.in on or before **17.01.2023** by 5 PM.

    b. If any bidder wants to participate the pre-bid meeting, they should submit a request (by mentioning the firm name, contact person name, WhatsApp number and e-Mail id) by email to the General Manager(Admin), OCAC through email (**gm_ocac@ocac.in**) with a copy to

"tushar.mohapatra@ocac.in, debaraj.behera@ocac.in" on or before **17.01.2023** by 5:00 PM. Only one person will be allowed to participate against one firm. The link for participation will be shared to the authorised persons one hour before pre-bid meeting.

c. The queries should necessarily be submitted in the following forma (Soft copy in .doc or .xls file to be attached):

Sl#	*RFP Document Reference(s) (Section & Page Number(s))*	*Content of RFP requiring Clarification(s)*	*Points of clarification*

d. OCAC shall not be responsible for ensuring receipt of the bidders' queries. Any requests for clarifications post the indicated date and time may not be entertained by OCAC.

4.1. Responses to pre-bid queries and issue of corrigendum

a. OCAC will issue timely responses to all queries.
b. At any time prior to the last date for receipt of bids, OCAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the EOI document by issuing a corrigendum.
c. The corrigendum (if any) & clarifications to the queries from all Bidders will be posted on the www.ocac.in and www.odisha.gov.in
d. Any such corrigendum shall be deemed to be incorporated into this EOI.
e. In order to afford prospective bidders reasonable time in which to take the corrigendum into account in preparation of their bids, Purchaser may, at its discretion, extend the last date for the receipt of EOI Bids.

4.2. Right to terminate the EOI process

a. Purchaser may terminate the EOI process at any time without assigning any reason. Purchaser makes no commitments, expression or implied that this process will result in a business transaction with anyone.

b. This EOI does not constitute an offer by the Purchaser. The Bidder's participation in this process may result in Purchaser short listing the Bidder to submit a complete technical and financial response at a later date in form of tender.

4.3. Submission of responses

a. Bids shall be submitted in a single sealed envelope and superscripted “Selection of System Integrator for Setting up of Cybercrime Centre of Excellence” – EoI Reference No- OCAC-SEGP-INFRA-0007-2022/23002.This envelope should contain hard copy of EOI proposal and one soft copy in CD media or in USB drive.
b. Bids shall consist of supporting proofs and documents as defined in the Prequalification and technical evaluation section.
c. Bidder shall submit all the required documents as mentioned in the Appendix including various templates (Form 1 to Form 4). It should be ensured that various formats mentioned in this EOI should be adhered to and no changes in the format should be done.
d. Envelope should indicate clearly the name, address, telephone number, Email ID and fax number of the Bidder.
e. The EOI response should be a complete document and should be bound as a volume. The document should be page numbered, must contain the list of contents with page numbers, and shall be initialed by an authorized representative of the Bidder.
f. Bidder must ensure that the information furnished by him / her in respective CDs/USB drive is identical to that submitted by him in the original paper bid document. In case any discrepancy is observed by the Purchaser in the contents of the CDs/USB drive and original paper bid documents, the information furnished on original paper bid document will prevail over the soft copy.
g. EOI document submitted by the Bidder should be concise and contain only relevant information as required under this EOI.

h. The bidder must submit EoI document fee amounting to *₹ 5600/-* (Inclusive of GST) in shape of DD from a schedule bank in favour of *Odisha Computer Application Centre*, payable at Bhubaneswar.

i. EoI document fee may optionally be furnished through NEFT/RTGS to OCAC in following account & furnish the UTR or any documentary evidence during evaluation of pre-qualification criteria.

Bank A/c No. : 149311100000195

Payee Name: Odisha Computer Application Center
Bank Name & Branch: Union Bank of India, Acharya Vihar, Bhubaneswar

Account Type: Savings

IFSC: UBIN0814938

5. Evaluation Criteria

5.1. Pre-Qualification Criteria:

The Bidder must meet the minimum conditions of eligibility provided herein. Proposals of only those Bidders who satisfy the Conditions of Eligibility will be considered for evaluation and eligible for the "Technical Stage" evaluation.

S. No	Pre-Qualification Criteria	Supporting Documents
1	Bidder should be the Company registered under the Indian Companies Act, 1956 or 2013 and shall have its registered office with legal presence in India.	Copy of Certificate of Incorporation &GST Registration Certificate
2	The Bidder must have a positive net worth as on 31st March 2022 or as per the last financial year audit report	Copy of the audited balance sheet of the company and Certificate from the Chartered Accountant clearly stating the net worth
3	Average annual sales turnover for the last three audited financial years (FY 2019-20, 2020-21 and 2021-22) should be minimum 100 crore	Copy of the audited balance sheet & Profit and Loss statements of the company for the concerned years
4	The Bidder's company must have average annual financial turnover of Rs.30 crore from IT Security services during last three financial years (FY 2019-20, 2020-21 and 2021-22).	Auditor/CA's certificate regarding company's last 3 years turnover from IT Security services and audited balance sheets to be submitted.
5	The bidder/ joint venture should have experience of at least 7 years in providing Cyber Forensic services/Cyber Security services/ Information security services/ IT Audit/ IT consultation/ Cyber Content	Declaration on letterhead signed by authorized signatory along with relevant PO Copies.

	Development & Simulation	
6	Bidder must have successfully executed and completed in the last 5 financial years, at least 5 major projects in the field of Cyber Security/ Cyber Forensics/ Information Security/ IT audit/ IT Consulting/ Digital Security etc. around the globe (Out of the above stated 5 projects, at least two projects should be in the field of IT/Digital/Cyber Security)	Copy of client citations / Work Orders OR client letter / testimonial stating the completion of the project and working satisfactorily in operations phase. Reference for each of the projects has to be given and should contain the following information – Name of organization, individual/s to contact, email-id, phone number and address, contract valueproject detail in brief
7	The Bidder must have a proven track record of implementing at least three 'IT Turnkey projects' of minimum value of Rs. 100 Cr each, in the last 5 years as on the date of release of this EoI. An 'IT turnkey project' should have the following deliverables as part of scope of project: > Supply, installation and configuration of hardware and system software for Security solutions. > Establishment of Security Operations Center (SOC), Forensics Investigation, Data Centre, LAN / WAN including firewalls, IPS, etc.	Work orders (in the name of Bidder) confirming year, scope of work and value of services to be delivered. AND Completion Certificate from client confirming year of completion / Self Certification by the Authorized Signatory.
8	The Bidder must have undertaken at least 1 project pertaining to data analytics with minimum project value of Rs. 50 crores in the last 5 years, as on the date of release of this EoI.	Work orders (in the name of Bidder) confirming year, scope of work and value of services to be delivered. AND Completion Certificate from client confirming year of completion / Self Certification by the Authorized Signatory.
9	The Bidder must have undertaken at least 2 projects pertaining to cyber security with minimum project value of Rs. 10 crores OR at least 1 project pertaining to cyber security with minimum project value of Rs. 20 crores in the last 5 years, as on the date of release of this EoI.	Work orders (in the name of Bidder) confirming year, scope of work and value of services to be delivered. AND Completion Certificate from client confirming year of completion / Self Certification by the Authorised Signatory.
10	The Bidder should not have been blacklisted by Central / State Government in India at the time of submission of the Bid	Self-declaration letter by Bidder as per format given in this Tender Document

11	The Bidder must have valid Goods & Service Tax registration in India & PAN card	Proof of valid Goods & Service Tax Registration in India & Copy of PAN Card
12	The Bidder must have at least 100 computer professionals, out of which minimum five (5) professionals having any of the certifications like CISA/ CISM/ EH/ CHFI/ GCIH/ CISSP/ CEH/ OSCP/ ISO 27001/ CISSP/ GCFA/ master's in cyber/Digital forensics working continuously full time for the past 1 year at the time of submission of bids.	Certificate from the HR head stating list of Employees with exposure to Projects and Technologies
13	The bidder must have a valid ISO 27001, ISO 9001 as on date of issue of this RFP.	Valid copy of certificate.
14	EOI Document Fee-Bidder must submit EOI document fee amounting to ₹ *5600/- (inclusive of 12% of GST)*	Tender Fees in shape of Bank Draft/NEFT

OCAC reserves the right to accept or reject any or all responses without assigning any reason.

6.2. Technical Evaluation Criteria:

SL#	Criteria	Documentary Evidence	Marks	Max. Marks
1	Implemented Security Operation Center (SOC) in Central Government/State Government/PSU in India.	Copy of work order and work completion certificate	Each implementation carries 10 marks	20
2	Implemented Cyber Forensic Lab in Central Government/State Government/PSU in India.	Copy of work order and work completion certificate	Each implementation carries 5 marks	15
3	Successfully completed cybercrime investigation	Copy of work order/work completion/document proof	Each successfulcompletion carries 5 marks	15
4	Establishment of COE in Central Government/State Government/PSU in India.	Copy of work order and work completion certificate	Each successful completion carries 5 marks	10

5	Proof of Concept of Solution	Online Demonstration		20
6	Technical Presentation- Methodology, Procedures, Tools to be used and Timeline			20

Bidder must score minimum 80% marks to be eligible for shortlisting.

6. Evaluation Process and Way Forward

6.1. This EOI is an endeavor to generate competition and receive an expression of interest from interested vendors by following an openly advertised competitive shortlisting process, thereby giving equal opportunity to all interested vendors to be considered for shortlisting. The interested vendors will be shortlisted based on the evaluation criteria given in this document.

6.2. In the second stage, a Request for Proposals (RFP) containing Technical and Financial Bids will be invited from such shortlisted bidders.

6.3. OCAC will constitute an Evaluation Committee to evaluate the proposal of the firms. The committee may seek additional documents as it deems necessary.

6.4. The decision of the Evaluation Committee in the evaluation of proposals to the Expression of Interest shall be final. No correspondence will be entertained outside the evaluation process of the Committee.

6.5. Those bidders who secure 80% mark in technical evaluation shall be shortlisted. After evaluation of expression of interest, an RFP containing scope of work along with technology to be adopted (Technical bid) as well as financial bid shall be prepared and invited from such shortlisted vendors in order to select the successful vendor.

6.6. The shortlisted eligible vendors will be required to demonstrate technology and its use before they can be allowed to participate in subsequent stages of bidding process.

6.7. The Evaluation Committee reserves the right to reject any or all proposals.

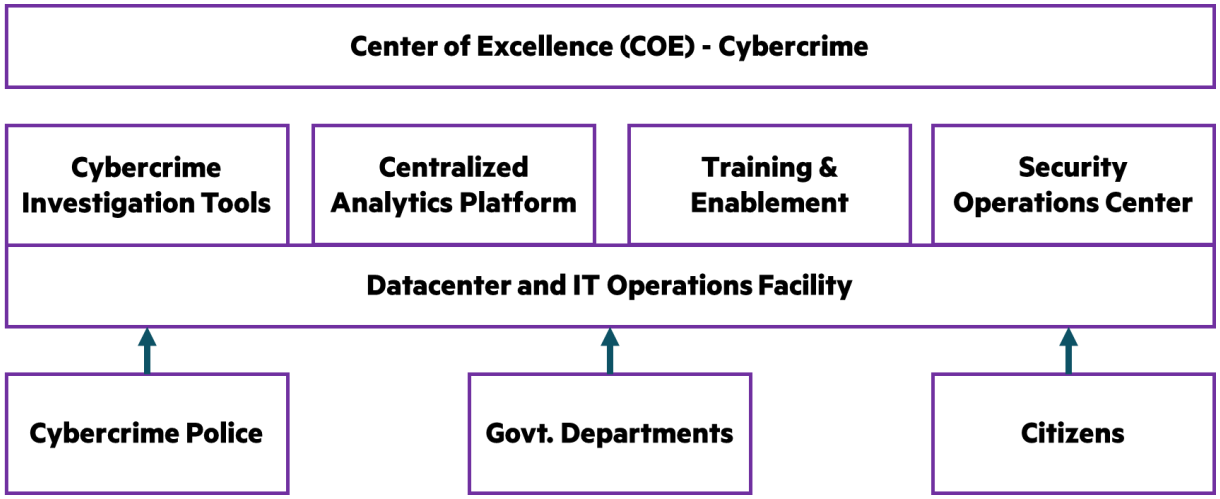
7. Scope of Work

This section details out the broad scope of work. Please note that the indicative lists of activities mentioned in this section are envisaged to meet the broad scope of work. However, the detailed scope of work / list of activities would be finalized at the time of issue of RFP. The period of engagement of the system integrator shall be for a duration of 5 years.

7.1. Centre of Excellence (CoE) - Cybercrime

The proposed COE needs to be established in Bhubaneswar, Odisha and will have advanced forensics tools, in addition to those installed at Forensic Lab, to handle cases that require advanced digital investigative capabilities beyond those available at Forensic Lab. The COE will address advanced functional requirements using tools & technology procured through this EOI. This digital forensic capability at COE will help in empowering the Investigative Officer, reducing investigation timelines, and improving operational efficiency of overall criminal investigation process.

The COE and Forensic Lab will be connected over secured MPLS connectivity for multiple purposes including but not limited to sharing data between COE and Forensic Lab, accessing enterprise applications & file server hosted at COE, securely configuring the end user devices at Forensic Lab, enforcing a uniform security policy, remote administration & management, provisioning of connectivity to implement future tools and technology to enable the district labs & agencies, etc.



Envisaged Cybercrime COE framework

Centre of Excellence (COE) - Cybercrime:

Operating these core areas will require skilled manpower, hence, Capacity Building becomes one of the important aspects of this project to have an effective cyber security workforce.

The key objectives of Centre of Excellence (CoE) are:

- To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace
- Planning, designing and analyzing cybersecurity capability building program for the state of Odisha

- To organize Awareness, Training and Education program, as depicted in (but not limited to) the National Institute of Standards and Technology (NIST) Special Publication 800-50
- To create awareness, train and educate the residents of Odisha and create a cybersecurity workforce with necessary capacity and capability for cyber resilience
- To develop necessary workforce within government and law enforcement agencies/public prosecutors, pleaders/judicial officials in digital forensics and technology assisted investigation techniques
- To develop tools, technologies and Standard Operating Procedures (SOPs)
- To study and develop policies and advisories regarding various domains of Cyber security and its allied domains, etc.
- To provide various services regarding cyber security and its allied domains

Cybercrime Investigation Tools:

The objective is to establish the capability to provide real-time digital media analytics to police for investigating crimes. In view of increased cyber-crimes and the need to fast track investigation and provide specialized skill set and manpower to handle cyber-crime. In continuation to its efforts, OCAC intends to set up a Centre of Excellence (COE) equipped with advanced forensic equipment comprising software and hardware along with required infrastructure.

Indicative list of tools to be procured for forensics investigation and reporting shall be –

- Write Blocker Set for SATA, IDE, USB, Fireware and SAS
- ADF Triage
- Encase Portable
- E-Fence
- Forensic Falcon
- UFED Touch Ultimate Ruggedized with Chinex PC Model along with connecting chord
- XRY mobile extraction tool
- Oxygen Forensic @Detective Software
- Phone Image carver
- CDAMS academic license
- C5 CDR Analyzer – Academic license version
- FTK latest version
- Navigation data recovery tool
- Stego Suite
- MAC acquire and analysis tool Black Bag
- Elcomsoft Password Recovery Suite
- Internet analysis and social media linkage tool X1 Forensics
- Net Force Suite

The above list of tools is only indicative to mention the wide variety of technology areas for forensics and cybercrime investigation. The final tools shall be finalized at the time of RFP.

Centralized Analytics Platform:

It has been envisaged to capture data from various data sources and analyze the ingested data to provide actionable intelligence to Law Enforcement Agencies (LEA). Data obtained from various sources can be utilized to determine the relationships that exist in the data through various analytical engines, finding correlation between events, detection of crime/fraud, perpetrators, etc. Analytics platform can help in meeting broad level objectives such as –

- Reducing the time required for investigation by providing collated information from various data sources at one place through data synthesis.
- Generating timely, relevant, actionable insights and alerts to mitigate a broad range of threats
- Mining large sets of data from various data sources simultaneously for discovery of threats and actionable insights. The required data feeds also must be provisioned
- Use analytical tools such as, but not limited to, Link Analysis, Timeline analysis, Location analysis, metadata analysis, trends, sentiment analysis, Facial Recognition & matching, Image analysis, pattern matching, predictive analysis, Language identification, entity extraction, etc.
- Monitoring of habitual offenders in order to determine their involvement in the crime
- Determination of the hidden or past relationships of the target, crime history
- Identifying new leads on crime and terrorism for monitoring
- Detection of potential violence, unrest etc. by analyzing hate speeches, posts and messages on social media that can trigger such kind of incidence
- Uncovering the modus operandi used to commit a particular crime
- Detecting and solving recurring problems such as robbery, chain snatching in a particular area
- Identification of illegal activities being carried out in deep and dark web such as drug / human trafficking, credit card frauds, fake passports etc.
- Assistance in maintaining law and order situation by identifying rumors and fake/provocative information

Training and Enablement:

The proposed COE should fulfill the competence gaps in the State due to lack of adequate expertise in cyber security, by building a three-tier program consisting of “Awareness”, “Training” and “Education” for the LEA staff and the citizens, broadly covering:

- Creation and maintenance of Awareness Portal, media campaigns on cyber security, and cyber security domain education – for the citizens of the state, and
- A Learning Management System (LMS) and Classroom Training – for all its constituents.

These services can be categorized into each tier as follows:

Awareness:

The Awareness tier consists of the Awareness Portal and Media Campaign, along with content preparation, as explained below.

- Content Preparation, development, and publishing
- Content for all channels of spreading awareness pertaining to cyber security
- Awareness portal
- Domain registration for awareness portal
- Awareness Portal development
- GIGW (Guidelines for Indian Govt. Websites) compliance
- Testing & Security Audit
- Hosting in a secured environment
- Content Management
- Maintenance of awareness portal for 5 yrs
- Media Campaign
- Social media page (FB, Twitter etc.) content designing
- Content management
- E-mail messages
- E-newsletters
- Advisories
- Posters, etc.

Training

The Training tier (continuous training program) aims to train Government and its constituents including LEA staff over a period of 5 years through two modes, the Learning Management System (LMS) and Classroom Training, as explained below:

Learning Management System

- Content Preparation, development, and publishing
- Development of LMS with features including (but not limited to):
- Device Agnostic access
- Mobile Application
- Modern, easy-to-use interface
- Personalized dashboard
- Collaborative tools & activities
- All-in-one calendar
- Convenient file management
- Simple & intuitive text editor
- Notifications
- Tracking progress
- Secure authentication & mass enrollment
- Multilingual capability
- Bulk course creation & easy backup
- Manage user roles & permissions
- High interoperability
- Regular security updates
- Detailed reporting & audit trail maintenance
- Marking workflow
- Peer & self-assessment
- Group management
- Embed external resources
- Automatic alerts,

- Online simulators, etc.
- Testing & Security Audit
- Hosting in a secured environment
- Content Management
- Maintenance of awareness portal for 5 years

Classroom Training

- Training-cum-Certification Course content preparation
- Provision of Trainers
- Training calendar preparation
- Organizing training programme
- Onsite/Offsite, instructor led training
- Training over Video Conference

Case Studies to be involved (Law Enforcement perspective)

Bidder is expected to prepare the knowledge repository in form of case studiesfor below mentioned modus operandi of cybercrime.

All the case studies will be the combination of videos, simulation, and gamification supported by the relevant documents containing elaborate details and techniques and procedure involved for solving the crime.

Case studies will be developed in a collaborative model. The vendor will be responsible for developing videos/simulation/gamification, documentation etc. on common cybercrime investigation related case studies by their own. However, OCACwill collect various case studies on cybercrime investigation from States/UTs andthese will be shared with the vendor for building the simulation on the same.

- Cyber bullying / stalking/sexting
- Fake/impersonating profile
- Profile hacking
- Impersonating email
- Email hacking
- Threatening email
- Online job fraud
- Online matrimonial fraud
- Provocative speech
- Debit/credit card fraud
- Internet banking relatedfraud
- Business frauds/emailtakeover
- Fraud call/vishing
- E-wallet related fraud
- Sim swap fraud
- Ransomware
- Unauthorized access/databreach
- Website related/defacement
- Cryptocurrency related fraud
- Online trafficking
- Online gambling
- Email spoofing
- Phishing/vishing
- Email bombing
- Spamming
- Spear phishing
- Illegal Online transaction
- Job Frauds
- Cyber defamation
- Copyright Violation

- Journal authentication
- IPR
- Patent practice crimes
- DNS Attack
- Bitcoin wallet
- Cyber warfare
- Android hacking
- Key Logger
- IRC (Internet relay chat)
- Author/researcher authorization
- Ponzi scheme
- Cyber stalking
- Cyber bullying
- Cyber pornography
- Denial-of-service attack
- SQL injection
- Man-in-the-middle attack
- Malware attack
- Cyber extortion
- Password trafficking
- Enterprise trade secret theft
- Software piracy
- Counterfeiting andtrademark infringement
- Domain name hijacking
- Salami slicing attack
- Data diddling
- Logic bombs

IT & Non-IT Infrastructure

Necessary IT and Non-IT infrastructure in a secured environment for providing aforementioned services.

Continuous research and development:

- Set up process for continuous research and development so as to cater to changing trends in cyber security domain
- Set up cyber range. The proposed cyber range will have features for accurate network simulation, real life threat scenarios, interactive learning and actionable feedback, etc.
- To develop tools, technologies and Standard Operating Procedures (SOPs) related to cyber security

As a part of the proposed CoE, the Bidder should also be able:

- To study and develop policies and advisories regarding various domains of Cyber security and its allied domains, etc.
- To provide various services regarding cyber security and its allied domains

Datacenter Setup:

The Data Centre Setup will be hosting all the core solutions in a centralized location, catering to the entire technical/logical and physical infrastructure. The data centre will be in OCAC, Bhubaneswar, with DR in future. The broad objectives are:

- Build data center setup, capable of hosting/delivering all the core areas (specified in detail in the above sections), on a turnkey basis.

- Design, procure, implement, commission, and operate all the data center IT (active and passive) as well as all the non-IT components. The design must incorporate all the latest data center design principles including machine-to-machine sensor-based alerts and controls.

- Monitor the performance of the data centre including usage and availability and analyze the future requirements (if any). Infrastructure management solution should be deployed to facilitate monitoring and management of data centre infrastructure on the integrated console.

Following are the indicative list of expectations, activities involved, and project deliverables (This list is just indicative, and the Bidder needs to come out with a comprehensive list of their own, covering all points mentioned below as well as those deemed fit to achieve the overall goal of this project):

- Supply of all the hardware as per the requirement and to be accommodated in DC location. This includes (but, is not limited to) Storage, Backup Devices, Database, Application Servers etc. Scope includes supply and implementation of all software/applications at DC, and their associated Data (able to handle any structured/unstructured data required for the project).
- Supply Communication/Collaboration tools/applications, Office Automation and Enterprise Management Applications etc. (Directory Services, Mail/Web Proxy, Indexing Server, Access Control, Proxy, Web Portal etc. as required). The Bidder must recommend the entire list required for this project. This also includes all end-point security options (for all the Hosts in core areas).
- Supply and implement all required OS & Virtual Platforms required to host the application and all the data processed and generated out of this project. All the deployment model must be on high performing, redundant and highly available storage & server infrastructure. The idea should be to build a virtualized & scalable internal private cloud environment, capable of expanding and provisioning seamlessly as required to accommodate various departments
- DC Built components including (but, not limited to) Fire & Security, Civil & Interior, Electrical & Data Cabling, Air Conditioning, Raised Floor, False Ceiling, Temperature/Humidity Controls, Rodent Control, Access Security, Surveillance, UPS Systems, Racks, Passive and UPS Cabling etc. The centre must build using new age sensor-based network (for alerts and quick response) & utilize smart cooling and proper thermal modeling & air flow controls.
- The Bidder should be able to plan to connect Forensic lab and other government departments to the COE (Data Centre), and adequate WAN / Security Equipment and connectivity must be recommended & provisioned as part of this project. A central staging (as required) can be carried out for any network devices/equipment and deployment at remote site.
- Provide all the on-going as well as one-time services for setting up of IT Infrastructure (& non-IT infrastructure) for DC. The services to also include One time & On-Going training envisaged for these equipment's & applications. Product Maintenance services for all supplied Hardware & Software must be planned for 5 years.
- Disk based backup solution must be planned for shorter duration to facilitate easy archival & thereafter long-term retention on low-cost medium. The Bidder should

propose a solution and suggest best practices for all categories of backup involved. The solution should also be capable of catering to even VM & Cloud environment.

- The space provided will be RAW Building (for DC/DR), and everything else must be built grounds-up. This includes (but, not limited to) - Facility design/architecture (using tier specific Best Practices), Internal modification, scalable Infrastructure (standard/modular), lighting layout, furniture/fixture etc. The flooring and ceiling design must be as per leading industry standards.
- Apart from the DC, SOC would need additionally video wall - a multi-monitor setup made up of LCD panels / LED arrays, blended projector screens etc., specifically designed for SOC/NOC kind of operations (e.g., min gap between active display areas). This should also support compressed internet streams of video and audio.
- The Bidder also needs to plan (design and supply) for the structured cabling and high available, high speed and redundant LAN switching (core/distribution/access) for entire operations (covering all core areas and floors)
- The centre must follow a comprehensive approach to power and cooling (including conservation of energy and thermal and energy efficiency). Green building rating and certification systems must be achieved and regularly audited for the entire duration of operations.
- Mechanical and Electrical planning must be done for 100% uninterrupted operations with adequate UPS sizing and backup planning. The site will be supplied with adequate input feeders for uninterrupted grid supply. The Bidder will be responsible for sizing & supply for alternative power as well as backup power for uninterrupted operations including power monitoring & management.
- The Fire detection & protection must be completely planned. This must take care in terms of standards used as per hazardous material and able to achieve the required approvals from authorities. The Bidder will be responsible for required certifications.
- Physical security system must be planned and adequate access control and surveillance has to be proposed. This also includes manpower required for internal security of the DC/DR Floors
- The Bidder must deploy skilled data centre specialists, Certified professional (with Data centre specific & adequate experience and expertise) and nominate SPOC for day-to-day activities. The DC must be taken up as Total Turnkey Solution for entire duration of project.

8. Operations & Maintenance Services

Training

- Classroom-based hands-on training for approximately 10-15 Odisha Cyber staff should be given by an Expert

- Functional Training – This training would focus on the usage of software/tool so that the users are aware of all the operations of the software/tool, ensuring smooth operations

- Administrative Training – This training would focus on the administration of software, backup and server infrastructure and would be imparted to 4-6 concerned persons nominated by Odisha Cybercrime department.

- The Bidder shall provide at least 2 sets of manuals which include technical, operational and maintenance information

Help Desk

- Design, procure, implement, operate and maintain the Help Desk components to resolve user department issues and incidents

- Provide Help Desk facility during agreed service period window for reporting user department incidents/issues/problems. The solution will include ticketing system and escalation matrix

- Help Desk operator should be fluent in local language Marathi (read/write)

Storage, Backup & Restore Services

- The Bidder is required to take backup of operating system, database, and application as per stipulated policies

- The Bidder shall be responsible for installation and configuration of the storage system and management of storage environment to maintain performance at desired optimum levels

- Back-up could be of various types: Full Backup / Cold Backup / Incremental Backup, etc. and would be taken as per the requirements of the departments

- The Bidder shall undertake monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies

- The Bidder shall provide ongoing support for file and volume restoration on requests.

Application Related Services

- The scope of application related services includes, but is not limited to, the following areas:
- Application, development, maintenance & enhancement

- Performance tuning and testing

- Configuration management and version control

- Release management

- Maintenance of development, testing and release (staging) environments

Acceptance Testing

The successful Bidder should cooperate with the third-party agency to ensure successful completion of Acceptance tests

- IT Infrastructure including Hardware equipment testing before commissioning
- Application, System and/or integration test on solution as a whole
- Audit of Network, Server and Application security mechanisms

Manpower Requirement

- The Bidder will provide the required manpower for the complete project for a period 5 years.

Project Documentation

- Weekly & Monthly status reports
- Upcoming milestones and releases
- Risk identification and mitigation plan

Appendix I: Bid submission forms

Proposal / pre-qualification bid shall comprise of following forms:

Form 1: Covering letter with correspondence details

Form 2: Particulars of Bidder

Form 3: Documents against Pre-qualification criteria

Form 4: Documents against technical criteria

Form 1: Covering letter with correspondence details

(Company letter head)

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of I.T. Dep't, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: EOI for Selection of System Integrator for setting up of Cybercrime Centre of Excellence (COE)

EoI Ref No : OCAC-SEGP-INFRA-0007-2022/23002

Dear Madam,

We, the undersigned, offer to provide the Centre of Excellence(COE) Implementation services for cybercrime.

Our correspondence details with regard to this EOI are:

SL#	Information	Details
1.	Name of the Contact Person	
2.	Address of the Contact Person	
3.	Name, designation and contact, address of the person to whom, all references shall be made, regarding this EOI.	
4.	Telephone number of the Contact Person.	
5.	Mobile number of the Contact Person	
6.	Fax number of the Contact Person	
7.	Email ID of the Contact Person	
8.	Corporate website URL	

We are hereby submitting our Expression of Interest (EOI) in both printed format and as a soft copy in a <<CD/USB drive>>. We understand you are not bound to accept any proposal you receive.

We understand and agree to comply that on verification, if any of the information provided here is found to be misleading the EOI process or unduly favours our company in the short listing process, we are liable to be dismissed from the selection process or termination of the resultant contract during the project.

We hereby declare that our proposal submitted in response to this EOI is made in good faith and the information contained is true and correct to the best of our knowledge and belief.

For and on behalf of <<Legal name of bidding entity>>

Signature Name:
Designation : Company Seal

Form – 2: Particulars of the Bidders

SlNo.	Information Sought	Details to be Furnished
1.	Name and address of the bidding Company	
2.	Incorporation status of the firm (public limited / private limited, etc.)	
3.	Year of Establishment	
4.	Date of registration	
5.	ROC Reference No.	
6.	Details of company registration	
7.	GST	
8.	PAN	
9.	Turnover FY 2019-20 FY 2020-21 FY 2021-22 (un-audited)	

Form-3: Documents against Pre-qualification Criteria

SL#	Pre-Qualification Criteria	Supporting Documents	Page Reference No.
1	Bidder should be the Company registered under the Indian Companies Act, 1956 or 2013 and shall have its registered office with legal presence in India.	Copy of Certificate of Incorporation & GST Registration Certificate	
2	The Bidder must have a positive net worth as on 31st March 2022 or as per the last financial year audit report	Copy of the audited balance sheet of the company and Certificate from the Chartered Accountant clearly stating the net worth	
3	Average annual sales turnover for the last three audited financial years (FY 2019-20, 2020-21 and 2021-22) should be minimum 100 crore	Copy of the audited balance sheet & Profit and Loss statements of the company for the concerned years	
4	The Bidder's company must have average annual financial turnover of Rs.30 crore from IT Security services during last three financial years (FY 2019-20, 2020-21 and 2021-22).	Auditor/CA's certificate regarding company's last 3 years turnover from IT Security services and audited balance sheets to be submitted.	
5	The bidder/ joint venture should have experience of at least 7 years in providing Cyber Forensic services/Cyber Security services/ Information security services/ IT Audit/ IT consultation/ Cyber Content Development & Simulation	Declaration on letterhead signed by authorized signatory along with relevant PO Copies.	
6	Bidder must have successfully executed and completed in the last 5 financial years, at least 5 major projects in the field of Cyber Security/ Cyber Forensics/ Information Security/ IT audit/ IT Consulting/ Digital Security etc. around the globe (Out of the above stated 5 projects, at least two projects should be in the field of IT/Digital/Cyber Security).	Copy of client citations / Work Orders OR client letter / testimonial stating the completion of the project and working satisfactorily in operations phase. Reference for each of the projects has to be given and should contain the following information – Name of organization, individual/s to contact, email-id, phone number and address, contract valueproject detail in brief.	

7	The Bidder must have a proven track record of implementing at least three 'IT Turnkey projects' of minimum value of Rs. 100 Cr each, in the last 5 years as on the date of release of this EoI. An 'IT turnkey project' should have the following deliverables as part of scope of project: > Supply, installation and configuration of hardware and system software for Security solutions. > Establishment of Security Operations Center (SOC), Forensics Investigation, Data Centre, LAN / WAN including firewalls, IPS, etc.	Work orders (in the name of Bidder) confirming year, scope of work and value of services to be delivered. AND Completion Certificate from client confirming year of completion / Self Certification by the Authorized Signatory.	
8	The Bidder must have undertaken at least 1 project pertaining to data analytics with minimum project value of Rs. 50 crores in the last 5 years, as on the date of release of this EoI.	Work orders (in the name of Bidder) confirming year, scope of work and value of services to be delivered. AND Completion Certificate from client confirming year of completion / Self Certification by the Authorized Signatory.	
9	The Bidder must have undertaken at least 2 projects pertaining to cyber security with minimum project value of Rs. 10 crores OR at least 1 project pertaining to cyber security with minimum project value of Rs. 20 crores in the last 5 years, as on the date of release of this EoI.	Work orders (in the name of Bidder) confirming year, scope of work and value of services to be delivered. AND Completion Certificate from client confirming year of completion / Self Certification by the Authorised Signatory.	
10	The Bidder should not have been blacklisted by Central / State Government in India at the time of submission of the Bid	Self-declaration letter by Bidder as per format given in this Tender Document	
11	The Bidder must have valid Goods & Service Tax registration in India & PAN card	Proof of valid Goods & Service Tax Registration in India & Copy of PAN Card	
12	The Bidder must have at least 100 computer professionals, out of which minimum five (5) professionals having any of the certifications like CISA/ CISM/ EH/ CHFI/ GCIH/	Certificate from the HR head stating list of Employees with exposure to Projects and Technologies	

	CISSP/ CEH/ OSCP/ ISO 27001/ CISSP/ GCFA/ master's in cyber/Digital forensics working continuously full time for the past 1 year at the time of submission of bids.		
13	The bidder must have a valid ISO 27001, ISO 9001 as on date of issue of this RFP.	Valid copy of certificate.	
14	EOI Document Fee-Bidder must submit EOI document fee amounting to *₹ 5600/- (inclusive of 12% of GST)*	Tender Fees in shape of Bank Draft/NEFT	

Form-4: Documents against Technical Criteria

SL#	Criteria	Documentary Evidence	Description	Page Ref. No
1	Implemented Security Operation Center (SOC) in Central Government/State Government/PSU in India.	Copy of work order and work completion certificate		
2	Implemented Cyber Forensic Lab in Central Government/State Government/PSU in India.	Copy of work order and work completion certificate		
3	Successfully completed cybercrime investigation	Copy of work order/work completion/document proof		
4	Establishment of COE in Central Government/State Government/PSU in India.	Copy of work order and work completion certificate		
5	Proof of Concept of Solution	Online Demonstration		
6	Technical Presentation- Methodology, Procedures, Tools to be used and Timeline			