Government ePublishing System

ePublishing System, Government of India

Tender Details

Date : 04-Jan-2024 06:04 PM

Print

Basic Details

Organisation Chain	Employees Provident Fund Organisation||Head Quarters, New Delhi||Information Services Division (ISD) HQ,New Delhi		
Tender Reference Number	40280/2187		
Tender ID	2024_EPFO_740527_1		
Tender Type	EOI	**Form of contract**	EOI
Tender Category	Services	**No. of Covers**	1
Payment Mode	Not Applicable	**Is Multi Currency Allowed For BOQ**	No
Is Multi Currency Allowed For Fee	No		

Cover Details, No. Of Covers - 1

Cover No	Cover	Document Type	Description
1	Fee/PreQual/Technical/Finance	.pdf	EOI Document

Tender Fee Details, [Total Fee in ₹ * - 0.00]

Tender Fee in ₹	0.00		
Fee Payable To	NA	**Fee Payable At**	NA
Tender Fee Exemption Allowed	NA		

EMD Fee Details

EMD Amount in ₹	0.00	**EMD Exemption Allowed**	NA
EMD Fee Type	NA	**EMD Percentage**	NA
EMD Payable To	NA	**EMD Payable At**	NA

Work /Item(s)

Title	Expression of Interest (EOI) Setting up Next Gen Security Operations Centre (Next Gen SOC)				
Work Description	Expression of Interest (EOI) Setting up Next Gen Security Operations Centre (Next Gen SOC)				
Pre Qualification Details	Please refer Tender documents.				
Tender Value in ₹		**Product Category**	Consultancy Services	**Sub category**	NA
Contract Type	Empanelment	**Bid Validity(Days)**	180	**Period Of Work(Days)**	45
Location	New Delhi	**Pincode**	110077	**Pre Bid Meeting Place**	New Delhi
Pre Bid Meeting Address	National Data Centre, EPFO, First Floor, Sector 23, Dwarka, New Delhi -110077	**Pre Bid Meeting Date**	11-Jan-2024 03:00 PM	**Bid Opening Place**	New Delhi

Critical Dates

Publish Date	05-Jan-2024 09:00 AM	**Bid Opening Date**	29-Jan-2024 03:00 PM
Document Download / Sale Start Date	05-Jan-2024 09:00 AM	**Document Download / Sale End Date**	25-Jan-2024 03:00 PM
Clarification Start Date	NA	**Clarification End Date**	NA
Bid Submission Start Date	05-Jan-2024 09:00 AM	**Bid Submission End Date**	25-Jan-2024 03:00 PM

Tender Documents

NIT Document

S.No	Document Name	Description	Document Size (in KB)
1	Tendernotice_1.pdf	Expression of Interest (EOI) Setting up Next Gen Security Operations Centre (Next Gen SOC)	440.93

Work Item Documents

S.No	Document Type	Document Name	Description	Document Size (in KB)
1	Tender Documents	EOI.pdf	Expression of Interest (EOI) Setting up Next Gen Security Operations Centre (Next Gen SOC)	440.93

Tender Inviting Authority	
Name	RPFC NDC
Address	National Data Centre, EPFO, First Floor, Sector 23, Dwarka, New Delhi -110077

Tender Creator Details	
Created By	Rahul Tanwar
Designation	Deputy Director
Created Date	04-Jan-2024 05:59 PM

EPFO

Expression of Interest (EOI)
Setting up Next Gen Security Operations Centre
(Next Gen SOC)

EOI No.: 40280/2187

Dated: 04.01.2024

National Data Centre,
EPFO,
First Floor,
Sector 23, Dwarka,
New Delhi -110077
INDIA

Notice inviting Expression of Interest for Managed Services of Next Gen Security Operation Centre for EPFO

1.1 The EPFO invites sealed Expression of Interest(EOI) from Firms of repute having expertise in Security Operation Centre implementation and commission for implementing, commissioning and managing the Next Generation Security Operation Centre for EPFO as managed Services.

1.2 Entities which satisfy the eligibility and pre-qualification criteria are required to communicate their interest in writing to the EPFO at the following address.

The Regional Provident Fund Commissioner
National Data Center, EPFO Complex, Sector 23, Dwarka
New Delhi – 110077

1.3 The EPFO reserves the right to reject any or all EOIs or cancel/withdraw the request inviting proposal without assigning any reason whatsoever and in such case no intending bidder shall have any claim arising out of such action.

1.4 This document does not constitute nor should it be interpreted as an offer or invitation for the selection of Managed Service provider of SOC for EPFO described herein. This document does not purport to be all inclusive or contain all the information or be the basis of any contract. No representation or warranty, expressed or implied, is or will be made as to the reliability, accuracy or the completeness of any of the information contained herein.

1.5 For further clarification, please contact:

Chief Information Security Officer
IT Security Vertical, IS Division, EPFO
(Email id: ciso.epfo@epfindia.gov.in and infosecurity@epfindia.gov.in with CC to: rc.ndc@epfindia.gov.in)
National Data Center, EPFO Complex, Sector 23, Dwarka
New Delhi-110076

Table of Contents

1. **EOI Schedule and Address**

S No	Event	Date
a.	Issuance of Expression of Interest (EOI) Document	**04.01.2024**
b.	Date for Pre EOI discussion	**11.01.2024**
c.	Last Date and Time for completed EOI document submission	**25.01.2024**
d.	Opening of EOI	**29.01.2024**
e.	Address for EOI submission and all communication on the subject	**National Data Centre, EPFO, First Floor, Sector 23, Dwarka, New Delhi -110077**

2. **Introduction**

a. EPFO is one of the world's largest Social Security Organizations in terms of clientele and the volume of financial transactions undertaken. At present, it maintains 24.77 crore accounts (Annual Report 2019-20) pertaining to its members. The Employees' Provident Fund came into existence with the promulgation of the Employees' Provident Funds Ordinance on the 15th November, 1951. It was replaced by the Employees' Provident Funds Act, 1952. The Employees' Provident Funds Bill was introduced in the Parliament as Bill Number 15 of the year 1952 as a Bill to provide for the institution of provident funds for employees in factories and other establishments. The Act is now referred as the Employees' Provident Funds & Miscellaneous Provisions Act, 1952 which extends to the whole of India. The Act and Schemes framed there under are administered by a tri-partite Board known as the Central Board of Trustees, Employees' Provident Fund, consisting of representatives of Government (Both Central and State), Employers, and Employees.

b. The Central Board of Trustees administers a contributory provident fund, pension scheme and an insurance scheme for the workforce engaged in the organized sector in India. The Board is assisted by the Employees' PF Organization (EPFO), consisting of offices at 138 locations across the country. The Organization has a well-equipped training set up where officers and employees of the Organization as well as Representatives of the Employers and Employees attend sessions for trainings and seminars. The EPFO is under the administrative control of Ministry of Labour and Employment, Government of India (Annual Report 2019-20). The Board operates three schemes - EPF Scheme 1952, Pension Scheme 1995 (EPS) and Insurance Scheme 1976 (EDLI).

c. Considering the ever-growing cyber threats and regulatory mandates (like of Cert-IN, MeitY, NCIIPC); EPFO has decided to go for an in-house Next Generation Security Operations Centre (SOC), which would be a command

centre facility at NDC Dwarka premise operated by enthusiastic team of security professionals. This team would be solely responsible for monitoring, analyzing, responding, and protecting the organization IT assets and services like Servers, Network Traffic (WAN, LAN, Local, Internet), Endpoints, Databases, Web Apps, User Identities etc. for the signs of potential security incident. In brief the objectives can be distinguished as below:

i. Complying with the 'Log Management', 'Security Incident Management' compliances mandated by the statutory bodies like Cert-In, NCIIPC etc.
ii. Prevention of cyber security incidents through various measures as establishing security policy, continuous threat analysis, deployment of preventive and detective security devices.
iii. Monitoring a EPFO IT ecosystem via standardized security tools to proactively identify potential cybersecurity threats 24/7/365, prioritizing the severity and thus closure of the incident.
iv. Analyzing identified anomalies for their severity and potential impact and prioritizing them for remediation. Isolating security incidents and implementing controls to prevent future events.
v. Improving the overall security posture of the EPFO by establishing centralized Security Operations Center.

3. **Broad Objective.** Keeping in view the regulatory requirements in India (CERT-In, NCIIPC etc.) and increasing innovative cyber threats and malwares, threats emanating from emerging technologies like AI/ML, block chain, bots, dark webs, social engineering, cloud etc., it has been decided to setup a 24x7x365 basis operating state-of-the-art Next Gen Security Operations Centre (SOC) for proactive monitoring as also predicting cyber-attacks (internal and external) on the EPFO's IT environment.

a. Bidder may propose SOC solution as of single or combination of multiple OEM. But there should not be any issue during the deep analysis of the incidents while handling with multiple OEM products/ solutions.
b. Bidder must implement the similar setup at both DC (Gurgaon) and DR (Secunderabad) locations. DR site should be envisaged considering minimal recovery time & points objectives.
c. Below services should be offered as part of SOC offering, but not limited to:
    i. Security Intelligence Feeds and Services
    ii. Threat Hunting Services
    iii. Dark Web Threats
    iv. Open-Source Intelligence
    v. Zero Day Attacks
d. The bidder shall supply skilled manpower for Security Operations Centre (SOC) operations over a period of five (5) years (three years extendable to two more years) at NDC location i.e., Dwarka, New Delhi, as detailed in this document.
e. Implementation Agency shall ensure uptime & availability of SOC related Infrastructure. Service provider resources are expected to deliver SOC services including but not limited to performance monitoring, performance tuning, optimization, and maintenance of SOC security tools, SIEM log backup, troubleshooting, security monitoring, security product management, vulnerability assessment and penetration testing and application security

testing. The detailed SOC reports formats will be discussed and finalized with bidder.

f. The scope is applicable for managing security operations within EPFO, including the following locations/ facilities:
    i. National Data Centre (NDC) at Dwarka, New Delhi
    ii. Data Center (DC) at Gurgaon
    iii. Disaster Recovery (DR) at Secunderabad
    iv. Network Operations Center (G-NOC) at Dwarka, New Delhi
    v. ADC (Additional NOC) at Secunderabad
g. On reaching stability and maturity of SOC system, additional scope could be added to the project and the scope of work for the bidder could be curtailed/ expanded, basis mutual understanding of EPFO & MSI both.

4. **Invitation**

Expression of Interest (EOI) is invited in a sealed envelope superscripted with "Expression of Interest (EOI) for Next Gen SOC"

a. From the applicants / bidders who meet the eligibility criteria as set out in Annexure –A
b. Who have solution strictly in line with the Broad Scope of Work as set out in this EOI
c. Agree to abide by the terms and conditions contained in this document.

Please note that the EOI is not a qualification criterion. EPFO will float an Open/Closed RFP at its own discretion. By participating in this EOI process, applicant / bidder confirms that they are in complete agreement with EPFO as per all the Terms and Conditions of this EOI. A Sealed envelope containing complete set of signed hard copy of EOI document should be submitted by post or be delivered in person at the undernoted office (on any working day) on or before the date and time mentioned in "EOI Schedule and Address" section of this document.

5. **Applicant's / Bidder's Eligibility Criteria**

a. This EOI is open to all applicants / bidders who fulfil the eligibility criteria as set out in **Annexure-'A'** of this document and is in agreement with EPFO terms and conditions of this EOI document. The applicant should furnish documentary evidence supporting the information provided by them as per the EOI process. Bidder could be System Integrator (SI) partnering with OEMs of SOC technologies and front ending for the project or OEM who is also a system integrator, partnering with other SOC technologies OEMs and front ending for the entire project. The bidder needs to share the choice of OEM for each SOC technology proposed in response to this EOI. The bidder should restrict to only one OEM option for each SOC technology and describe relationship between bidder & respective OEM.

6. **Broad Scope of Work:** The minimum specified scope of work to be undertaken by the bidder for Establishing, Operations, and Maintenance of the proposed EPFO SoC at Datacenter facility, Gurgaon, as per the scope mentioned below. The selected bidder shall ensure an uptime as per the agreed SLA every quarter for five years (three plus two) after Go-Live.

a. The minimum specified work to be undertaken by the bidder for Supply, Installation and Commissioning of proposed solutions and devices including operation and maintenance for 05 years (three plus two) from the date of Go-Live.
    i. Schedule I: Delivery of product/appliances/solution or hardware as per the timeline.
    ii. Schedule II: Installation, commission, and integration of the complete solution within NDC, DR & DC.
    iii. Schedule III: Acceptance Tests i.e., FAT
    iv. Scheduled IV: Operations and Maintenance Services for the complete Infrastructure under EPFO SoC which includes Active and passive (IT & Non-IT) and Human resources at the project for 05(three plus two) years from the Go-Live.

b. To fulfill the objectives of the proposed SoC, It is expected that a shortlisted bidder should come up with architecture (including NG-SIEM, NBA, SOAR, Threat Feeds, Log Collectors, etc.) based on their experience and suitable for Project.

c. The Bidder will provide the following services for Site Preparation & Supply, Installation, Integration, and Maintenance of Infrastructure for the establishment of the EPFO SOC at the EPFO. The exact scope and boundaries of services provided as part of this Contract are detailed in the Detail Scope of Work in the EPFO SOC RFP.
    i. Site Preparation for Video wall, desktop/laptop/terminals as per the requirement.
    ii. Supply, installation, and setting up of the necessary IT Infrastructure including required Cabling.
    iii. AMC & FMS of all the devices/equipment/solutions, procure/comprised in EPFO SoC during the complete tenure of this project i.e., five Years (three plus two) from the day of Go-Live.
    iv. Onsite support for solution and Infrastructure Operations on a 24x7x365 basis by skilled human resource/personnel for five years (three plus two) to ensure the availability as per the agreed SLA.

d. The scope of the project will be divided into phases,
    i. SOC Establishment.
    ii. Integration with the Legacy Infrastructure.
    iii. Phase-wise enhancement of the SoC.
    iv. Incorporation with Cert-IN.

e. Initially, the implementation of the EPFO SoC will be done for NDC, DR, DC locations, post stability and maturity of the EPFO SoC additional stakeholder or additional services to the state may be added to the project and the under the scope of the successful bidder. A successful bidder or System Integrator needs to manage the entire infrastructure and services. For additional

services and scope, the bidder may get extra costs with the mutual agreement with the EPFO.

6.1 Design, Supply, Installation, Commissioning of the Infrastructure

a. Supply, Install, Test, Commission and Manage Next Gen SOC technologies together at EPFO premises for the contract period of 5 years (three years extendable to two years).

b. Following are the list of components to be implemented:

i. Security Operations Center (SoC): Define and implement baseline Cyber Security Operations Policy at the enterprise level. Procure and deploy the necessary infrastructure to run a NextGen SOC 24*7*365. Extend SOC operations including AI/ML-based analytics tools. SOC should have following major technologies and related services with deep learning, analytics, automation of routine SOC activities to improve threat detection and response capabilities leveraging AI/ML
ii. NextGen Security Incident & Event Management (SIEM)
iii. NextGen Security Orchestration, Automation and Response (SOAR)
iv. SOC Infrastructure Setup (HCI)
v. Security Data Lake(SDL)
vi. Application & API Security
vii. Ticketing Tool
viii. Vulnerability Assessment and Penetration Testing(VAPT)
ix. Network-Based Anomaly Detection (NBAD)
x. Database Activity Monitoring (DAM)
xi. Privileged Access Management (PAM)
xii. Endpoint Protection Solution(EPP)
xiii. End-point Detection and Response (EDR)
xiv. Security Trainings and Awareness
xv. Integration with the existing IT Infrastructure

c. Successful bidder shall submit stage-wise reports and it should be done strictly in accordance with the scope of work in the document.
d. Successful bidder is expected to adhere to all criteria as mentioned in the **Annexure A**.
e. Any additional design guidelines as provided in the tender document / proposed solution document has to be achieved as per established delivery timelines.
f. The successful bidder would be required to submit detailed design documents and would be approved by EPFO before actual execution of work.
g. A supply schedule for all materials with make and model is to be prepared and submitted in line with the work break down structure of the project plan.
h. All materials are to be delivered at the designated location(s) as per expected delivery timelines with no additional dispatch or delivery costs.
i. Any deviation from the expected timelines of delivery is to be intimated in advance for appropriate actions and reason.
j. Bidder should take care of Insurance against the material loss.
k. Delivery Challans and Installation Reports shall be validated by the EPFO personnel.

l. OEMs are expected to perform the following:
    i. Respective OEMs shall certify the installation of the applicable solutions and components.
    ii. Respective OEMs shall provide premium support and minimum 50 hours of professional services per annum for the project tenure.
    iii. Respective OEMs shall provide free-of-cost certification/ training for any 5 personnel identified by the EPFO, with a coverage of solution/ component configuration, administration & management.
m. Successful bidder shall submit stage-wise reports and it should be done strictly in accordance with the scope of work in the document.
n. The successful bidders would be required to submit detailed design documents and would be approved by EPFO before actual execution of work.

6.2 Integration with the existing IT landscape

a. All SOC Infrastructure must support scalability with adequate licensing, accessories, and modules to provide continuous growth to meet the requirements and demand of EPFO.
b. Bidder accordingly shall implement the solution provided for integration of all applications and hardware.
c. Bidder is expected to successfully deploy and integrate additional security solutions / tools in the existing datacenter environment, which has some legacy components in its inventory.
d. Implementation of above-mentioned solutions should be done in a phased manner.
e. Bidder must regularly monitor and analyze the Network and Application performance metrics and raise an alert/ intimation to the EPFO. To achieve this, bidder could utilize existing tools (NMS, APM) and real-time dashboards/ feeds available with the EPFO.
f. Bidder must ensure that the deployment of the above security components (including SIEM & SOAR) should not significantly impact the Network and IT Infrastructure performance, especially during the prime business hours i.e., 09:00 am to 6:00 pm.
g. Bidder must support older versions of the existing hardware/ software/ operating system / middleware etc. in case the EPFO chooses not to upgrade to latest version.

6.3 Manpower Supply

a. For Design & Implementation Phase: Bidder should ensure that key personnel with relevant skill sets are available to the EPFO at the designated location(s) for installation and commissioning of the solutions/ products mentioned in above sections.
b. For Operations & Management Phase: Bidder must provide OEM certified manpower & relevant technical experience to proactively manage and administer the solutions/ tools mentioned in the above sections.
c. For Process & Procedure Documentation: Deployed manpower should be capable enough to clearly document ‘process’ and ‘procedures’ for the operational areas like Incident Monitoring & Management, Logging &

Monitoring, Storage & Backup Management, privacy management. *Refer ISO 27001:2013/2022 , ISO/IEC 27002 standard.*

d. Subject Matter Experts: SME's responsible to manage additional security components like DAM, WAF etc; should not only have tool/solution management experience but also should have practical knowledge of the respective security domain (that particular tool/ solution caters).

6.4The Next-Gen SOC should have the following capabilities:

a. Ability to sustain the size, complexity and geographic spread of EPFO's IT infrastructure and its growth YoY. Presently, 25000 desktops with agents like AV, 1000+ IT systems including Servers, Network and Security systems, and 50+ applications etc. are deployed in the EPFO. Please refer "Logs Source systems for SOC" section below for log sources.
b. Architecture should have multi-tier, distributed, high availability (DC and DR) deployment having flexibility to deploy on premise as well as on private cloud.
c. Self-learning, proactive, predictive & cognitive by completely leveraging AI/ML and deep analytics.
d. Structured and unstructured data i.e. all the events to be stored in data lake like environment
e. SIEM should have robust, scalable architecture to consume and withstand 10 Thousand EPS (scalable up to 25k EPS) or equivalent per day of data whichever is higher without compromising system functionality or performance each at DC & DR locations.
f. SIEM including Deep Packet Inspection, UEBA capabilities, and Big Data Lake platform must be single point of collation / convergence of logs from SOC technologies, Security, Operational and Emerging technologies for correlation, analytics and must provide 360- degree real-time analysis and incident reporting.
g. Logs collated by SOC technologies from all log sources as enumerated below must be correlated on real-time basis within SIEM for depicting conclusive complete kill chain of incident and report the same to stakeholders on real-time basis.
h. SOC must be able to detect attacks emanating from emerging technologies.
i. Configuration and Customization of the tools as per EPFO requirements on ongoing basis.
j. Uptime of the solutions at minimum 99.99%.
k. Capable to correlate events, network activity data, alerts, and vulnerability data to provide complete view of security threats and generate real- time security alerts.
l. Capable to provide real time security alerts based on strong correlation of including but not limited to:
    i. Vulnerabilities data, Application Security data, External penetration testing, Configuration / hardening assessment data, etc.
    ii. Alert from SIEM, DAM, PAM, NBAD, EDR, Threat Intelligence etc.
    iii. Cross-IT Infrastructure IT Correlation like Firewall + IPS + WAF, IPS + VA+ web, logs + WAF etc.
m. Capable to detect slow attacks, Advance Persistent Threats, file less attacks, advance malwares, zero-day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI / ML.

n. Capable to detect, prevent & predict attacks including but not limited to bots, zombies, autonomous systems etc.
o. Provide visual depiction of attack for incident investigation & forensic requirements w.r.t complete attack kill chain life cycle.
p. Capable of retrieving the archived logs for reporting, analysis, correlation, investigation and forensics.
q. The solution should ensure that the overall load on the network bandwidth at DC, DR, WAN level would be minimal.
r. Be configured to serve as end-to-end incident management, Incident response, investigation platform and single evidence repository.
s. Capable to provide automated detailed post incident documentation about all the actions taken, root cause, controls implemented etc.
t. System should have capability to integrate with ITSM and ITAM platforms for ticketing and auto vulnerability management etc.
u. Solution should have machine learning capabilities to execute the playbook tasks appropriately, connect inputs and outputs of multiple automated tasks, recommendations for next steps etc.
v. Capability to modify, customize, delete/deactivate out of the box workflows as per EPFO's environment and needs.
w. Digital forensic investigation with complete replay of attack including the ingress and egress of payload.
x. Continuous collaboration with global threat intelligence stakeholders.
y. Anti-phishing, Antimalware, anti-rogue mobile application, brand abuse across EPFO environment.

6.5 Logs source systems for Next Gen SOC

a. The solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service.
b. Security technologies such as Firewall, IPS, WAF/WAAP (LB & SSL Off loader), AV, EPP, EDR, NBAD, PAM, DAM etc. These are feeder technologies / source system of logs provided to the SOC.
c. Operational technologies include OS, databases (traditional and big data), webservers, applications, networking technologies, middleware, virtualization and cloud technologies (private/hybrid/public) i.e. entire IT infrastructure and business applications. These are feeder technologies / source system of logs provided to the SOC.
d. The Emerging technologies include Chabot's, voice bots, block chain, cryptocurrency, augmented & virtual reality, IOT. These are feeder technologies / source system of logs provided to the SOC.

Note: The technologies cited above at Para 'b' as log source systems (apart from firewall and IPS) are part of the solution to be proposed by bidder in Next Gen SOC.

7. Format and Signing of EOI

a. The applicant should prepare EOI strictly as desired in this Request for EOI Document.
b. All pages of the EOI should be signed only by the authorized person(s) of the company/firm/bidder. Any interlineations, erases or overwriting shall be valid only if the person(s) signing the EOI authenticates them. The EOI should bear

the rubber stamp of the applicant on each page except for the un-amendable printed literature.

c. The applicants / bidder should demonstrate that they meet eligibility criteria given in Annexure – 'A' of this EOI.
d. As a part of this EOI, the applicant has to submit detailed approach paper on how they propose setting up of Next Gen Security Operations Centre (SOC) along with the requirements, Annexure-'B' and Annexure-'C' to setup the same.
e. Contact detail of the authorized signatory and an authorized contact person on behalf of the applicant is to be provided.

8. **Process after submission of EOI**

a. All EOIs received by the designated date and time will be examined by the EPFO to determine if they meet criteria/terms and conditions mentioned in this document including its subsequent amendment(s), if any, and whether EOI is are complete in all respects.
b. On scrutiny, if the EOI is found NOT in desired format /illegible /incomplete /not containing clear information, in view of EPFO, to permit thorough analysis or failing to fulfil the relevant requirement will be rejected for further evaluation process.
c. EPFO reserves the right, at any time, to waive any of the requirements of this Request for EOI document if it is deemed in the interest of EPFO.
d. If deemed necessary, EPFO may seek clarifications on any aspect of EOI from the applicant. If a written response is requested, it must be provided within 5 working days. Beyond the response received, if any, will not be considered. However, that would not entitle the applicant to change or cause any change in the substances of their EOI document already submitted. EPFO may also make enquiries to establish the past performance of the applicants in respect of similar work. All information submitted in the application or obtained subsequently will be treated as confidential.
e. After examining the EOI, some or all eligible applicants may be asked to make presentation of the solution and demonstrate proof of concept.
f. EPFO may shortlist the applicants who fulfil the eligibility criteria, have solution as per the requirement of the EPFO and are agreeing to abide by the terms and conditions of the EPFO. EPFO's judgment in this regard will be final.
g. EPFO may issue an Open/Closed Request for Proposal (RFP) to shortlisted applicants for inviting technical and indicative commercial bids for next process of procurement. However, please note that short listing of applicants should not be treated as a contract for the proposed work.
h. Applicants will be advised about shortlisting of their EOIs or otherwise. However, applicants will not be provided with information about comparative position of their EOIs with that of others.
i. Nothing contained in this EOI shall impair the EPFO's Right to issue 'Open Tender' on the proposed solution.
j. The bidders, whose proposed solution is finally selected, shall have to provide the sizing of the solution implementable within the EPFO and achieve the stated objectives.

9**. Terms & Conditions:**

a. Lodgment of an EOI is evidence of an applicant's consent to comply with the terms and condition of Request for EOI process and subsequent bidding process. If an applicant fails to comply with any of the terms, its EOI may be summarily rejected.
b. Wilful misrepresentation of any fact in the EOI will lead to the disqualification of the applicant without prejudice to other actions that the EPFO may take.
c. The EOI and the accompanying documents will become property of EPFO. The applicants shall be deemed to license, and grant all rights to EPFO, to reproduce the whole or any portion of their product/solution for the purpose of evaluation, to disclose the contents of submission to other applicants and to disclose and/ or use the contents of submission as the basis for EOI process.
d. EPFO reserves the right to accept or reject any or all EOI s received without assigning any reason therefore whatsoever and the EPFO's decision in this regard will be final.
e. No contractual obligation whatsoever shall arise from the EOI process.
f. Any effort on the part of applicant to influence evaluation process may result in rejection of the EOI.
g. EPFO is not responsible for non-receipt of EOIs within the specified date and time due to any reason including postal delays or holidays in between.
h. EPFO reserves the right to verify the validity of information provided in the EOIs and to reject any bid where the contents appear to be incorrect, inaccurate or inappropriate at any time during the process of EOI or even after award of contract.
i. Applicants shall be deemed to have:
    i. examined the Request for EOI document and its subsequent changes, if any for the purpose of responding to it.
    ii. examined all circumstances and contingencies, having an effect on their EOI application and which is obtainable by the making of reasonable enquiries.
    iii. satisfied themselves as to the correctness and sufficiency of their EOI applications and if any discrepancy, error or omission is noticed in the EOI, the applicant shall notify the EPFO in writing on or before the end date/time.
j. The applicant shall bear all costs associated with submission of EOI, presentation/POC desired by the EPFO. EPFO will not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.
k. Applicants must advise the EPFO immediately in writing of any material change to the information contained in the EOI application, including any substantial change in their ownership or their financial or technical capacity. Copies of relevant documents must be submitted with their advices. For successful applicants, this requirement applies until a contract is awarded as a result of subsequent bidding process.
l. Applicant shortlisted must not advertise or publish about the result of process / engagement with EPFO on the subject in any form without prior written permission from EPFO.
m. The detail scope of work will be included in the Request for Proposal (RFP document.
n. Subcontracting is not permitted.
o. EPFO may review eligibility criteria, Terms & Conditions and other evaluation criteria as per requirements of EPFO at the time of publishing RFP for setting up of Next Gen Security Operations Centre (SOC).

p. EPFO shall have the right to cancel the EOI process itself at any time, without thereby incurring any liabilities to the affected Applicants. Reasons for cancellation, as determined by EPFO in its sole discretion include but are not limited to, the following:
    i. Services contemplated are no longer required.
    ii. Scope of work not adequately or clearly defined due to unforeseen circumstance and/or factors and/or new developments.
    iii. The project is not in the best interest of EPFO.
    iv. Any other reason.

10. **Disclaimer**

EPFO is not committed either contractually or in any other way to the applicants whose applications are accepted. The issue of this Request for EOI does not commit or otherwise oblige EPFO to proceed with any part or steps of the process. Subject to any law to the contrary, and to the maximum extent permitted by law, EPFO and its directors/officers/employees/contractors/agents and advisors disclaim all liabilities (including liability by reason of negligence) from any loss or damage, cost or expense incurred or arising by reasons of any person using the information and whether caused by reasons of any error, omission or misrepresentation in the information contained in this document or suffered by any person acting or refraining from acting because of any information contained in this Request for EOI document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, default, lack of care or misrepresentation on the part of EPFO or any of its officers, employees, contractors, agents or advisors.

Annexure – "A''

Eligibility Criteria

Sr.	Pre-Qualification (PQ) Criteria	Document(s) to be submitted
1.	A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid.	Declaration by the bidder / OEM on their letter head that the bidder has proposed no such solutions in response to the EoI.
2.	The bidder should be an established Company registered under the Indian Companies Act, 1956/ 2013, or partnership firm register under LLP Act, 2008 since last 5 years as of December 2023.	Following certificates would be required: a. Certificate of the incorporation, provided by Ministry of Corporate Affairs, GoI. b. Certificate consequent to change of name, if applicable.
3.	The bidder should have a registered number of: a. GST Registration. b. Income Tax / PAN.	Following certificates would be required: a. Certificate of GST registration. b. Copy of PAN / Income tax number.
4.	The bidder should be an authorized partner of the OEM whose product bidder is proposing. (Solution proposed may be from a single or multiple OEMs).	In case of an OEM authorized partner, a letter of authorization (MAF) from original manufacturer for each solution / equipment must be furnished in original duly signed. Undertaking from the OEM mentioning a clause that OEM would provide support services during the complete period of the contract if the bidder authorized by them fails to perform.
5.	The bidder should have a minimum average annual turnover of at least Rs. 100 Crores in the last three audited financial years as on bid submission date.	Audited Balance Sheets for last 3 years, i.e., 2019-20, 2020-21 & 2021-22 where financial turnover from SOC business should be clearly mentioned. Every sheet should be duly certified by a chartered

Sr.	Pre-Qualification (PQ) Criteria	Document(s) to be submitted
	Note: Turnover should be applicable to bidder and not for its group companies/ subsidiary companies/ parent company.	accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years. **OR** A letter under the head of the chartered accountant / or firm certifying the financial turnover of the company is to be submitted with the bid.
6.	Bidder should be a net profit-making organization in each of the last three financial years as on bid submission date.	Audited Balance Sheets for last 3 years, i.e., 2018-19, 19-20 & 2021-22 where profit or loss from similar works is segregated. Every sheet should be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years. **OR** A letter under the head of the chartered accountant / or firm certifying the profit and loss of the company from similar line of service is to be submitted with the bid.
7.	At least three (3) Central Government / State Government/ PSU/ BFSI clients shall be served by bidder, with similar nature of work (On-	Relevant MSA copy/ Work order copy / Customer Satisfaction Letter regarding successful implementation or ongoing implementation of security operation

Sr.	Pre-Qualification (PQ) Criteria	Document(s) to be submitted
	Premises SOC, Managed SOC, Hybrid SOC) the recent past and all work orders / contracts should be in the name of the bidder for the SOC services. • Minimum value of any one project should be above 20 Crores or more. • One of the projects should be completed or under steady state of operations	center (SOC) in the name of the bidder is to be submitted. The PO / letter should be in the name of the bidder and clearly mention the scope of work.
8.	Bidder must have dedicated in-house SOC/ Captive SOC with minimum of 20-seater occupancy.	An undertaking in the company's letter head signed by authorized signatory to be submitted. In addition, pictures/ video footage of the established SOC facility (within the country), could be shared along with the technical bid.
9.	The bidder should have local office in New Delhi or National Capital Region(NCR)	Self-certification with office location addresses to be submitted / declaration for establishment of an office in case LoI has been awarded. The document should be on the bidder's letter head signed by the authorized signatory.
10.	The bidder or any of its group / sister concern company should not have been blacklisted by any Regulatory or Government Authority or Public-Sector Undertaking or any Law Enforcement Authority for breach of any Regulations or Laws as on date of submission of the tender.	An undertaking to this effect in the company's letter head signed by authorized signatory.
11.	The bidder should have at least 10 in-house certified resources on proposed SIEM & SOAR technology.	An undertaking in the company's letter head signed by authorized signatory to be submitted.

Sr.	Pre-Qualification (PQ) Criteria **Note**: All the manpower list should be on the payroll of the bidder.	Document(s) to be submitted
12.	The bidder should be certified to the following standards (preferably latest one): o ISO 9001: 2008/ 2015 o ISO 20000: 2018 o ISO 27001: 2013/ 2022	Copy of the certificate(s) to be submitted along with the bid.
13	OEM of each technology proposed for SOC must be a reputed global company registered in India under the Companies Act 1956 and have strong client support centres in India.	Certificate of incorporation in India from each OEM

Note

Bidder should submit detailed response along with documentary proof for all of the above eligibility criteria. The eligibility will be evaluated based on the bid and the supporting documents submitted. Bids not meeting the above eligibility criteria will be rejected.

Technical Evaluation will be done by EPFO's technical evaluation committee and the decision of the committee will be final.

Bidders to submit relevant documentary evidence for all parameters mentioned. Providing any wrong information by the bidder will result in disqualification of the bidder. EPFO may cross check above parameters by any means / during site visit.

For a particular Solution, only the OEM or its authorized representative can bid. If both the OEM and its authorized representative bid for the same Solution, both the bids will be rejected.

In case any purchase order has been issued to the bidder by EPFO in respect of any other project/product and the same has not been delivered/executed even after the prescribed time period and is pending for execution as on date of bid, the bid of the respective bidder is liable for rejection.

The bidder or any of its group / sister concern company should not be any of the following – a) Network Integrator for the EPFO. b) Application related service provider for the Applications of the EPFO. c) ISSPs empanelled with EPFO.

Please Note:

Since this is not a Request for Proposal (RFP), commercials are not required to be submitted at this stage.

Annexure – "B"

Contents of Technical Submission by the Bidder
Name of the Bidder: M/s

Sr.no	Contents of the EOI Response (w.r.t. EPFO Next Gen SOC proposed setup)
1	Detailed unified technology Next Gen SOC architecture for size, complexity and geographic spread and growth of EPFO vetted by all OEMs together.
2	Estimated EPS and per day data size in TB of the Next Gen SOC. Explain the rational how it is arrived at. Sizing guidelines for next five years
3	Detailed unified reference functional Next Gen SOC architecture with data flow diagrams vetted by all OEMs together.
4	Share out of the box support of Next Gen SOC tools with each log source as per “Logs Source systems for Next Gen SOC” section.
5	Share out of the box integration support / compatibility of Next Gen SOC tools with each other (e.g. name the SIEM OEM with compatible DAM, PAM, EDR, VM OEMs and vice-a-versa for each tool proposed)
6	Data and logs integration from source systems as per “Logs Source systems for Next Gen SOC” strategy cited above
7	Data, logs, rules, policies etc. migration strategy from current SOC (if applicable) to Next Gen SOC.
8	Provide resource deployment model (L1/L2/L3/L4) for Run operations. Clear description needs to be provided on how many resources (SI and OEM) per support level along with the experience, certifications and skills of the resources.
9	Confirmation on OEM of Next Gen SOC technologies must be ready to deploy their personnel resources onsite at EPFO for 24x7x365 days operations.
10	Technical and Operational support mechanism with SI and OEMs available in India with location and number of resources for each OEM.
11	Availability of Certified resources of the proposed Next Gen SOC tools in India (give appx number certified trained resources technology wise)
12	System Integrator relationship with OEM (i.e. platinum, gold etc). Bidder to submit certificate obtained from each SOC technology OEM on kind of relationship with them.
13	Plan to deploy the technologies and bring down the dependency on L1 & L2 resources by providing automation and reducing man power in three years’ timeframe.
14	Each OEM’s technology, innovation and functionality roadmap of their product for first 3 years and subsequent 2 years.
15	Clients wherein SI has implemented proposed Next Gen SOC technologies. Please provide technology-wise client list in the last 3 years.
16	Global clients wherein proposed Next Gen SOC technologies are operational by OEM or their partners. Please provide technology-wise client list in the last 3 years.
17	The project plan with high level description of project phases and estimated duration.
18	What is not deliverable in Next Gen SOC by SI & OEMs

Bidder should provide complete solution stack to be presented in a tabular form:

S.No	Name of GSOC Solution	Product Name proposed	OEM partnership (if yes, type)
1	<SIEM>		
2			
3			
4			

Note:
All relevant product information such as user manual, technical specifications sheet etc. should be submitted along with the offer.

Hard copy of supporting documents or documentary proof for all the above criteria should be submitted to **RPFC**, **National Data Centre, EPFO, First Floor, Sector 23, Dwarka, New Delhi -110077, INDIA**

Annexure – "C"

PROFILE OF THE BIDDER

S. No.	Particulars	Response
1.	Name of the bidder	
2.	Country of HQ (if other than India) and Date of Incorporation	
3.	Head Quarters Address	
4.	Address in India & Date of Incorporation in India	
5.	Communication Details of Contact Official(s) – Name, Designation, Phone & Fax Number (with STD code), Mobile No. & E-mail Address.	
6.	Ownership structure (e.g. Company, Partnership)	
7.	Details of Partners / Directors	
8.	In case of limited companies, names of major shareholders with percentage holding.	
9.	Total number of offices worldwide and list thereof	
10.	Experience in Security Operations Centre setup & management (No of years with details of significant work done including volumes, capacities etc.)	
11.	Experience in implementing Security products (No. of years with details of products and implementation locations)	
12.	a. Total Number of Employees.	
	b. Total Number of Technical employees	
	c. Number of employees having Qualifications / Certifications (GSOC technologies proposed, CISSP, CEH, ISACA CRISC, CVA, CCNA, CCNE, CCSP, CCIE-Network, CCIE-Security etc.). (breakup of each to be given)	
13	a. Tangible Net Worth, Total turnover, Sales & Profit for the last 3 Financial Years	
	b. Turnover relating to Security Operations Centre for the last three financial years.	
14.	Name of Primary Bankers/Financers & their address	
15.	Furnish information relating to the Clients where security operations have been undertaken.	
16.	Furnish details of pending/past litigations within the last 3 years, if any.	
17.	Independent analyst (Gartner, IDC etc) report about your firm / company (if any) related to products / services in the information security domain	
18.	Brief Bio-data of the key personnel to be associated with the proposed project	

S. No.	Particulars	Response
19.	Activities proposed to be covered under Next-Gen SOC along with names of products / appliances/ solutions proposed for each activity, name & details of Partner companies / Applicants (please attach details of the arrangements). As per table given in Annexure-B	
20.	Names of proprietary products, technologies for Security Operations Centre, used by you.	
21.	Details of empanelment / tie-ups / assignments with Government units and industry bodies	
22.	Details of the proposed Next Gen SOC framework / approach, architecture, Technical approach	

Note – The bidder must attach appropriate document attested by their Authorized Signatory in support of their claim in compliance of the above particulars.

---End---