NATIONAL INFORMATICS CENTRE

Request for Proposal

for

Selection of Managed Service Provider for Setting up, Operating and Managing the Government Cyber Security Operations Centre (GSOC) for NIC

Tender Reference Number: ----------

Address: National Informatics Centre, A-Block, CGO Complex, Lodhi Road, New Delhi-110003

Table of Contents

1. Summary Sheet

Tender number	
Name of the Purchaser	National Informatics Centre (NIC)
Tender type	Open tender
Tender category	Services
Contract Period	Three years of operational phase + implementation phase, from the date of Contract, extendable by a period of up to two years of operational phase.
Earnest Money Deposit	INR **6.5** Crore
Period of validity of the Bid	180 days from the last date for Bid submission
Submission of pre-Bid queries	Only queries submitted on the GeM Portal https://GeM.gov.in/) will be responded to in the pre-Bid meeting. However, the formal response to any query would be that published on the said portal.
Parts of Bid	Two-Stage online Bid, as under: (a) **Stage-1:** Technical Bid (b) **Stage-2:** Financial Bid
Resubmission of Bid	Bid may be resubmitted before the last date and time for submission of the Bid.

2. Definitions & Abbreviations

2.1. Definitions

2.1.1 In this RFP, the expressions in column (2) in Table 1 shall have the meanings respectively assigned to them in the corresponding entry in column (3).

TABLE 1: DEFINITIONS

S. No.	Expression	Definitions
(1)	(2)	(3)
1.	Asset	In relation to an Organisation, the Assets (including but not limited to: servers, virtual machines, containers and Endpoints), network components, peripheral devices (printers, scanners etc.), security devices and applications— (a) owned by it or any of its agencies; and (b) used by it but owned by the Purchaser or any of its agencies, or by any other entity in respect of whose ICT Resources there is no Work Order in force, and which is under the control of such Organisation Reference to— (1) "computer resource" means computer resource as defined in the Information Technology Act, 2000; and "entity" means any entity as referred to in the definition of "Organisation" in this RFP
2.	Audit	A systematic, independent review and examination of records, system configurations, processes, controls, and activities—whether manual, automated, or hybrid—conducted to: • Assess the adequacy, effectiveness, and resilience of technical, procedural, and administrative controls; • Verify compliance with applicable laws, regulations, security policies, contractual obligations, and operational procedures; • Detect deviations, vulnerabilities, misconfigurations, and control weaknesses; and • Recommend corrective and preventive measures to ensure continuous improvement and risk mitigation.
3.	Authorised Representative	For the doing of any act or thing, for the purposes of the RFP or identification of the Selected Bidder or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected Bidder, MSP or Purchaser, as the case may be, may specify as its Authorised Representative in this behalf

4.	Authorised Signatory	For the affixation of signature or Electronic Signature Certificate on any document or electronic record, for the purposes of the RFP or identification of the Selected Bidder or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected Bidder, MSP or Purchaser, as the case may be, may specify as its Authorised Signatory in this behalf
5.	Bid	The bidding process and the proposal submitted by the selected Bidder for this RFP, including any clarifications, responses and amendments submitted by the Bidder in response to any request made by the Purchaser in this connection
6.	Bidder	The person participating in the Bid process pursuant to this RFP and that has submitted or intends to submit a Bid in accordance with the terms and conditions set forth herein.
7.	Component	An item listed under BoQ (Refer paragraph 14.1), Service or Manpower under the scope of this RFP.
8.	Contract Period	The period of subsistence of the Contract
9.	Contract Value	Shall be equal to the GTV of the successful bidder, accepted by the Purchaser
10.	Contract/Agreement	The contract or agreement entered into between the Selected Bidder and the Purchaser
11.	Financial Year	The period commencing on the 1st day of April of a given calendar year and ending on the 31st day of March of the immediately succeeding calendar year, both days inclusive.
12.	Go-Live	The formal commencement of full-scale operations of the Government Security Operations Centre (GSOC) after the successful completion of implementation, configuration, and integration of all supplied components; execution and acceptance of User Acceptance Testing (UAT); and completion of all required internal and external security audits with closure of identified non-conformities, as certified in writing by the Purchaser.
13.	Implementation phase	The phase of the project before Go-Live
14.	Operational phase	The phase of the project after Go-Live
15.	Managed Service Provider	The Selected Bidder with whom the Purchaser enters into the Contract
16.	Organisation	One or more entities, including Ministries, Departments, Organisations, agencies, bodies, or other institutions etc. to which NIC provides information and communication technology (ICT) services or support
17.	Party	Either the Managed Service Provider (MSP) or the Purchaser, as the context requires; and **Parties** shall be construed as a

		collective reference to both the MSP and the Purchaser together.
18.	Purchaser	National Informatics Centre (NIC), including any— (a) of its successors; (b) representative authorised by it; and (c) assignee permitted by it
19.	Quarter	A continuous period of three Months, reckoned from the date of Go-Live and, in respect of any period constituting less than a period of three Months in the period preceding the expiry of the Contract Period, such lesser period; and the expression "Quarterly" shall be construed accordingly
20.	Reputational Risk	Any event, incident, or circumstance that has the potential to cause negative publicity, negative public opinion/perception, or diminished trust and confidence in the Purchaser, whether justified or not, thereby impacting its public image, credibility, or stakeholder relationships.
21.	RFP/Tender	This RFP/Tender document, including all documents, amendments and clarifications issued by the Purchaser to invite Bids from Bidders for "Selection of Managed Service Provider for Setting up, Operating and Managing the Government Cyber Security Operation Centre for NIC". The terms "RFP" and "Tender" are used interchangeably in this document.
22.	Disaster Recovery Site	NDC Hyderabad
23.	Selected Bidder	The Bidder identified by the Purchaser for entering into the Contract
24.	Service(s)	Services to be provided by the MSP for the discharge of its obligations under the RFP and the Contract, in a manner consistent with— (a) Applicable Law; and (b) extant policies and guidelines for— (i) cybersecurity, information security and data protection procedures and practices; and (ii) prevention, response and reporting of cyber incidents, issued by the Government of India, the Purchaser, the Indian Computer Emergency Response Team (CERT-In) in the performance of functions entrusted to it by law, or the National Critical Information Infrastructure Protection Centre (NCIIPC) in respect of such Critical Information Infrastructure as may be declared as a protected system by law, including such amendments, revisions or modifications thereto as may be made from time to time during the contract period.

25.	System/ICT components	Includes, but is not limited to, applications, portals, cybersecurity devices, active network components, endpoints, and any other hardware, software, or technology infrastructure elements forming part of the Information and Communication Technology (ICT) environment. For the purposes of this RFP, the terms “System” and “ICT Components” shall be used interchangeably.
26.	Total Quarterly payment	The total payment to be made to the MSP against invoices submitted on a quarterly basis, calculated in accordance with criteria set forth in the Contract.
27.	Users	The administrators, application owners, or other authorised personnel of an Organisation who are responsible for managing, operating, or utilising specific systems, applications, or services within the scope of this RFP.
28.	UAT	The process of end-to-end testing of the complete SOC setup implemented by the MSP, conducted to verify that all functionalities, integrations, configurations, and performance requirements meet the specifications, service levels, and acceptance criteria, terms and conditions defined in this RFP, culminating in the Purchaser’s final acceptance prior to Go-Live.
29.	Work Order	An order placed by the Purchaser on the MSP for Setting up, Operating and Managing the Government Cyber Security Operation Centre for NIC under the Contract
30.	Working Day	“Working Day” means any day of the week and does not exclude Sunday, or a Holiday declared by Purchaser and/or Government of India.

2.2. Abbreviations

TABLE 2: ABBREVIATIONS

Sr. No.	Abbreviation	Full Form/Definitions
1.	AI/ML	Artificial Intelligence/Machine Learning
2.	AMC	Annual Maintenance Cost
3.	BOM	Bill of Material
4.	BOQ	Bill of Quantity
5.	BOT	Build-Operate-Transfer
6.	CCN	Change Control Note
7.	CoC	Chain of Custody
8.	CPP	Central Procurement Portal
9.	DAST	Dynamic Application Security Testing
10.	DB	Data Base
11.	DCO	Device Configuration Overlay
12.	DLP	Data Leakage Protection
13.	DRM	Digital Rights Management
14.	EMD	Ernest Money Deposit
15.	EPS	Event Per Second
16.	FEC	Financial Evaluation Committee
17.	GeM	Government e-Marketplace
18.	GFR	General Financial Rules
19.	GOI	Government of India
20.	GTV	Gross Total Value
21.	HLD/LLD	High Level Design/Low Level Design
22.	HPA	Host Protected Area
23.	ICADR	International Centre for Alternative Dispute Resolution
24.	ICT	Information and Communication Technology
25.	IPR	Intellectual Property Rights
26.	ISO	International Organisation for Standardization
27.	ITAM	Information Technology Asset Management
28.	ITIL	Information Technology Infrastructure Library
29.	ITSM	Information Technology Service Management
30.	KT	Knowledge Transfer
31.	MAF	Manufacturer's Authorization Form
32.	MeiTY	Ministry of Electronics & Information Technology
33.	MIS	Managed Information System
34.	MSE	Micro and Small Enterprises
35.	MSME	Micro, Small & Medium Enterprises
36.	MSP	Managed Service Provider
37.	NAC	Network Access Control
38.	NDA	Non-Disclosure Agreement
39.	NIC	National Informatics Centre
40.	NIC-CSG	NIC Cybersecurity Group

41.	NOC	Network Operations Centre
42.	NVME	Non-Volatile Memory Express
43.	OEM	Original Equipment Manufacturer
44.	OS	Operating System
45.	PB	Peta Byte
46.	PBG	Performance Bank Guarantee
47.	PQ	Pre-Qualification
48.	QCBS	Quality and Cost Based Selection
49.	RBI	Reserve Bank of India
50.	RCA	Root Cause Analysis
51.	RFP	Request for Proposal
52.	SAS	Serial-Attached SCSI
53.	SAST	Static Application Security Testing
54.	SCA	Software Composition Analysis
55.	SIEM	Security Information and Event Management
56.	SLA	Service Level Agreement
57.	SOAR	Security Orchestration, Automation and Response
58.	SOC/GSOC	Security Operations Centre / Government Security Operations Centre (used interchangeably in this document)
59.	SOP	Standard Operating Procedures
60.	SSD	Solid State Drive
61.	SSO	Single Sign-On
62.	TDS	Tax Deduction at Source
63.	TEC	Technical Evaluation Committee
64.	TIP	Threat Intelligence Platform
65.	TQ	Technical Qualification
66.	UAT	User Acceptance Testing
67.	WO	Work Order
68.	ZTNA	Zero Trust Network Access

3. Introduction

3.1 NIC is a vital Information Technology entity of the Government of India, functioning as its premier IT arm. Operating under the Ministry of Electronics and Information Technology (MeitY). NIC plays a pivotal role in the advancement and execution of e-governance projects and initiatives in India. It offers a comprehensive range of ICT services, including software development, managing countrywide Government network infrastructure, data centre and cloud services, as well as web applications development and hosting. NIC is entrusted with the responsibility of developing and maintaining various government websites and portals, facilitating online services and transactions for citizens and businesses.

3.2 National informatics Centre has a vast network of offices and centres spread across the country upto District level, providing technical support and expertise to various government entities. It collaborates with various stakeholders, including government agencies, public sector organisations, and industry partners, to promote innovation, efficiency, and transparency in the delivery of government services.

3.3 Overall, the National Informatics Centre plays a crucial role in the digital transformation of the Indian government, enabling efficient and accessible online services, data management, and IT solutions for the benefit of citizens and the administration. Security and sustained availability of such services being provided by NIC are critical for the performance of public duties and acts in which the public are interested. Establishment of Government Security Operations Centres (GSOC) is envisaged for 24X7X365 monitoring and protection of the Government ICT infrastructure.

3.4 The GSOCs will be established at:

- **Primary GSOC:** New Delhi;
- **Disaster Recovery (DR) Site:** Hyderabad; and
- **Extended Remote Operations Location:** Chennai.

In the event of any service failures at Primary SOC in New Delhi, operations shall automatically transition to the DR site at Hyderabad for hardware/software failover, and to the extended SOC at Chennai in case of manpower/operational failures, to ensure uninterrupted service delivery

3.5 The DR for SOC operations shall incorporate, at a minimum, the following critical components:

(a) IT Service Management (**ITSM**);
(b) Security Information and Event Management (SIEM);
(c) Security Orchestration, Automation, and Response (SOAR); and
(d) Threat Intelligence Platform (TIP).
(e) Governance, Risk management and Compliance (**GRC**)

These components shall be deployed at both the Primary SOC and the DR site in **High Availability (HA)** configuration (at least N+1 redundancy at each site). The solution must ensure:

- **Automatic failover** from the Primary SOC to the DR site in the event of a failure, without any manual intervention;
- **Continuous data synchronisation** between the Primary SOC and DR site at all times through automated tools;

- Provision by the MSP of all hardware, software, and ancillary components necessary for DR operations, including synchronisation, failover, and operational continuity;

Retention of a complete **log archive** (As per log retention policy of the Purchaser) at the DR site to ensure full forensic and compliance coverage.

4. Purpose of this RFP

4.1. This Request for Proposal (RFP) is issued for the selection of a Managed Service Provider (MSP) to design, supply, implement, operate, and manage a comprehensive Government Cyber Security Operations Centre (GSOC) for National Informatics Centre (NIC).

4.2 The objective of this engagement is to ensure that the SOC provides:

- Proactive monitoring, detection, and response to cybersecurity threats and incidents;
- High availability and disaster recovery capabilities to maintain uninterrupted SOC operations; and
- Compliance with applicable cyber security policies, and guidelines issued by the Government from time to time.

5. Scope of Work

5.1 Overview

5.1.1 The Government Security Operations Centre (GSOC) serves as the core component in managing the overall cybersecurity of the Government. The SOC must possess comprehensive visibility into the prevailing cyber threats within the Government's cyberspace and undertake necessary measures to address and prevent these threats. The scope of this RFP is to design, supply, install, configure, integrate, implement, operate and provide comprehensive services for Government Security Operations Centre (GSOC) including DR and extended location(s). The MSP shall possess the necessary expertise to efficiently operate the SOC at the anticipated scale required by the Government, ensuring uninterrupted services.

The selected **Managed Service Provider (MSP)** shall:

a) Design, supply, install, configure, integrate, implement, operate, and maintain a **fully functional, multi-location SOC**;
b) Provide **24x7x365 operations** with real-time monitoring, Threat hunting, Threat detection, and incident handling capabilities.

The scope of work includes but not limited to is given below:

5.1.2 The MSP shall automate the incident detection, triaging, mitigation. Identification of such incidents/service-requests/problems must be automated as far as possible by requiring minimal manual intervention. Proactive threat detection, threat hunting and mitigation shall also be responsibility of the MSP. Service tickets are to be created and closed successfully for each incidents/service-requests/problems detected automatically or logged in manually. The incidents must be categorised in different priorities as defined under paragraph 6.2 (Priority types for Service SLA). The MSP shall also carry out detailed investigations, forensic analysis, reverse engineering etc. to identify the root cause of such incidents and

prepare detailed incident reports as per need. Detailed Forensics and/or RCA may be required for Approx. 30% or more of the reported/detected incidents.

The tickets/service requests can also be logged through manual tickets by various users from Government Ministries/Departments/Organisations etc. which shall be closed through an automated mechanism or through manual intervention. Automated tickets logged through various platforms like SIEM which shall be automatically resolved through tools like SOAR etc.
The overall ticket handling capacity can be enhanced during the contract period, which shall be handled through the change management process as given at paragraph 13.4.

5.1.3 The activities to be performed by the MSP as part of scope of work includes but not limited to the following:

(a) Design, supply, install, configure, integrate, implement, operationalize and maintain all the supplied components as part of the complete integrated solution.
(b) Integrate the supplied components with the existing ICT Infrastructure components (which shall include but not limited to hardware, software, databases, services required for operations of Central logging, Threat intelligence, SSO, endpoint solutions, email, SMS gateway and any other components/platforms of the Purchaser.)
(c) Maintain the logs in supplied SIEM and archive the logs as per policy of the purchaser (Indicative metrics shall be 6 Months Live Logs in the SIEM, 6 Months hot/ready to use Archive beyond 6 months live logs and 1 Year cold archive beyond hot/ready to use archive.)
(d) The ingestion of the Logs in the supplied SIEM tool shall be optimised to minimise the effective EPS while maintaining the Logs archives as per the policy of the Purchaser.
(e) The logs archive shall be retained at the DR site also.
(f) Creation of Rules and Logic for Playbooks under SIEM and SOAR and implement the playbooks.
(g) Monitor the playbooks and update the same as per requirement.
(h) Create Standard Operating Procedures for various cyber-attack scenarios and implement the same in day to day SOC operations.
(i) Create a SOC operations manual which shall be followed for day to day SOC operations during the contract period. The SOC operations manual shall be approved by the Purchaser and shall be reviewed at least biannually or as and when desired by the Purchaser, and shall be updated as per requirement.
(j) Develop and deploy a solution architecture that is secure and resilient, leveraging the supplied components for establishment of SOC.
(k) End-to-end security operations and management of the SOC.
(l) Maintain strong and robust cybersecurity practices and measures.
(m) Identify security breaches, incidents, compromises, anomalies, unauthorised accesses, and violations of Government security policies, guidelines, processes, and procedures.
(n) Respond to security tickets related to any incidents/ service requests/ problems and take necessary corrective and preventive measures.
(o) Conduct investigations of security incidents/ service requests/ problems including suspected breaches and provide comprehensive investigation reports with Root Cause Analysis (RCA).
(p) Prepare security monitoring reports, security alert reports, and any other requested reports and dashboards as per requirement of the Purchaser on an ongoing basis.

(q) Ensure baseline security hardening of all MSP supplied and deployed ICT infrastructure, applications, databases, services of SOC/extended location(s) as per Centre of Internet Security (CIS) benchmarking and identify, address and rectify any identified security gaps and vulnerabilities before Go-Live.

(r) Search for potential cyber security threats to the Government's ICT infrastructure, data and services etc. through proactive threat hunting, threat detection and to proactively mitigate these.

(s) Create, train, deploy, and manage Artificial Intelligence and Machine Learning models for various use cases as per the requirement of the Purchaser.

(t) Design and develop dashboard visualizations, alerts, correlation rules, reports etc.

(u) Perform end-to-end incident investigation, tracing all components of a suspected compromise, including initiation of the compromise, identification of compromised devices/systems, subsequent recovery process and RCA.

(v) Conduct investigation and forensic analysis on endpoints, VMs, operating systems, servers, computers, laptops, hard drives, mobile phones, and other digital devices. Additionally, perform tasks such as preserving digital evidence, recovering data, analysing electronic mail, extracting information from databases, and other related activities.

(w) Ensure the maintenance of a proper Chain of Custody (CoC) to preserve the integrity of evidence. All actions for evidence recovery and collection shall be conducted and managed in a manner that ensures the preservation and protection of data and evidence in its original form, making it admissible in a court of law.

(x) Ensure a continuous engagement of an Incident Response Retainer service from a security OEM which has global presence and is backed by security group conducting research in the area of threat telemetry. The open ended Incident Response Retainer service shall also be provided initially for 100 hours in the name of NIC and the decision to leverage the retainer service for specific incidents shall be taken by NIC on a case to case basis. The MSP shall continue to provide incident response services through the manpower deployed through this tender, without any dependence on the retainer service.

(y) The MSP may optionally set up a simulation test bed as per requirement of the MSP, replicating relevant security technologies to practice various threat scenarios in a virtual environment. The test bed shall include all the required hardware, software platforms, system software, networking equipment, storage etc. which shall be provided by the MSP.

(z) Perform data recovery from servers, applications, databases, computers, and damaged/corrupted hard disks/removable media when necessary.

(aa) Ensure compliance with and adherence to all government security policies and regulations.

(bb) To get the internal security audits done and take appropriate measures to address and resolve the audit findings.

(cc) To get the external security audit of the GSOC, done through Cert-In empanelled vendor, resolve the findings of such audit.

(dd) Ensure logs and audit trails of all supplied components are available in the solution itself for a period of two months. Additionally, Logs of all supplied components shall also be pushed to the central logging solution of the purchaser in real time.

(ee) Implement and sustain ISO 20000, ISO 27001 certification for the GSOC.

(ff) MSP shall get the GSOC assessed and complied for SOC-CMM and maintain the same throughout the period of the contract.

(gg) Provide requisite cyber security trainings to the officers of the Purchaser's team through OEMs of the provisioned solutions. The scope of the trainings to be held over the contract period shall be as per section 5.10 of this RFP.

(hh) Ensure logging is enabled on all supplied on-premise ICT systems of the Purchaser and the raw logs (unprocessed) thereof are streamed in real time to the Purchaser's log management platform without any alterations. Establish security hardening policies and create documentation for all supplied components, and subsequently implement the security hardening measures.

(ii) The MSP shall facilitate integration of logs from purchaser's ICT systems with the supplied SIEM solution.

(jj) Ensure one day quarterly switchover drill in first fifteen days of every Quarter after Go-Live. During this switchover drill the ICT operations of the components shall be switched over to the DR location at Hyderabad and manpower deployed at Chennai location shall take over SOC operations/work in coordination with SOC manpower deployed at New Delhi.

(kk) The MSP shall provide a single unified dashboard showing an integrated view of all components of the SOC. The dashboard should also have role-based views and customised views for specific organisations, combination of organisations, users, roles and use cases.

(ll) Shall support the cybersecurity teams of various ministries and departments and shall coordinate with SOC teams in various Ministries/departments in handling their respective cyber security incidents and preparation of RCAs.

(mm) Shall respond to queries from other cyber security agencies of the Government through NIC Cyber Security Group.

(nn) Shall perform Vulnerability Assessment (VA) of servers/VMs/Containers and applications hosted at Purchaser's Data Centres using purchaser supplied VA tools.

(oo) Shall visit various ministries and departments as per requirement for onsite resolution of cyber security incidents based on tickets assigned.

(pp) Shall perform detailed log analysis and prepare & submit analysis reports with findings and RCA.

(qq) Shall provide 24X7X365 helpdesk support at the SOC (Delhi) using resources deployed at the location for providing 24X7 cyber security support to various Government Ministries and Departments.

(rr) Ensure compliance with respect to the Service Level Agreement (SLAs)

(ss) Shall lay Inter building fiber cable between adjacent buildings for connecting the GSOC with NICNET/NKN.

(tt) Shall supply, install and configure the Active LAN components (Router, switches, access points etc.) for Approx. 1200 nodes at GSOC LAN.

5.2 Solutions to be provided

5.2.1 The MSP shall be responsible for providing the following solutions, including the necessary hardware, storage, operating systems, software, licenses, AMC and support required for the deployment and operations of the solutions over the period of the contract and any extensions thereof:

S.No.	Required Solutions
1.	Security Incident Event Management (SIEM)
2.	Security Orchestration Automation Response (SOAR)

3.	Threat Intelligence Platform (TIP)
4.	Information Technology Services Management (ITSM)
5.	Attack Surface Management
6.	Attack Simulation Platform
7.	Security Testing Platform
8.	Dynamic Application Security Testing (DAST) tool
9.	IP & Web Reputation Feeds
10.	Threat Intelligence IOC Feeds
11.	Deep Web, Dark Web, Social-media & OSINT Feeds
12.	Incident Response Retainer Service
13.	Digital Forensics Incident Response (DFIR)
14.	Portable Log Analyzers
15.	Disk Imager with Write Blockers
16.	Magnetic Media Degausser & Secure Drive Eraser
17.	Static & Dynamic Analysis Sandbox from 3 OEMs
18.	Digital Forensic Suite
19.	Mobile Forensic Suite
20.	Memory Forensic Solution
21.	Mac Forensics Suite
22.	Cloud Forensic Solution
23.	Steganography Forensic Solution
24.	eDiscovery Forensic Data Analytics Platform
25.	Network Forensics
26.	Data Recovery Tools
27.	SOC Logistics Tools and standalone storage systems for system Image storage.
28.	SOC and Forensics work stations, laptops etc.
29.	Forensic Tools
30.	Laying of Inter building fiber cable between adjacent buildings for connecting GSOC with NICNET/NKN
31.	Supply and installation of Active LAN components (Router, switches, access points etc.) for Approx. 1200 nodes at GSOC LAN.
32.	Hardware appliances / solutions for security of the supplied SOC solution(Indicative): (a) NGFW (b) WAF (c) Server Load Balancer (d) SSL Off Loader (SSLO) Proxy etc.
33.	Governance Risk & Compliance Solution (To be supplied, installed, configured and made Go-Live in first year of the operational phase of the contract)

The sizing and specifications of the above-mentioned solutions are to be submitted as part of Detailed Project Plan to be evaluated as part of TEC based on the sizing and specifications of other SOC components. If any solution is declared *End-of-Life* (EOL) or *End-of-Support* (EOS) by the respective OEMs during the

contract period, the same shall be upgraded/replaced at no additional cost to the Purchaser, to meet the performance requirements and SLAs during the contract period.

5.2.2 The MSP is responsible for upgrading or changing any of the deployed solutions and tools as necessary to meet the SLAs, without any additional cost to the Purchaser.

5.2.3 **Any component (H/W and/or S/W) quoted by the bidders should not be in use as an R&D product in NIC and/or funded by Government of India.**

5.2.4 If there is continuous degradation in performance due to any of the component the same shall be replaced by the MSP at no cost to the Purchaser within three months of the notice.

5.2.5 All ICT Infrastructure supplied as part of the contract that includes but not limited to servers, active and passive network components, backup components, storage, workstations, all passive cabling for supplied components, including supply, installation, operation and maintenance shall be provided by the MSP.

5.2.6 The MSP shall ensure requisite manpower (Refer Section 14.2) for required uptime of all supplied components, cybersecurity operations, and SLA compliance at both Primary and DR sites. Any Additional manpower required by the MSP for ensuring; uptime of the supplied components, cyber security & operations and services as per the SLAs shall be provided by the MSP without any additional cost to the Purchaser. This is applicable to both Primary and DR sites.

5.2.7 Data Centre Space including necessary UPS power, Cooling, access controls and Building Management System (BMS) shall be provided by the purchaser.

5.3 MIS Solution showcasing all information pertaining to the SOC components

5.3.1 The MSP shall provide a Managed Information System (MIS) to capture, present, and manage all information pertaining to the SOC components.

MIS reports shall be supplied in a format and mode mutually agreed upon with the Purchaser, and at a periodicity defined in the SOC Operations Manual (e.g., yearly, quarterly, monthly, weekly, or daily).

At a minimum, the MIS reports shall include:

(a) Uptime and availability of systems.

(b) Incident reports covering disruptions, downtime, security violations, etc.

(c) Any other report relevant to the scope of work, as required by the Purchaser.

5.3.2 The MIS Solution shall have the following features:

(a) The MIS solution shall be a web-based portal.

(a) The MIS solution shall be integrated with the supplied solutions except the forensics.

(b) The MIS Solution should be able to ingest data from the supplied solutions and generate various customized dashboard as per the requirements of the purchaser.

(c) The MIS solution shall seamlessly integrate with the ITSM solution for SLA measurement, penalty calculation, reporting etc. and shall provide customised dashboards related to SLAs and penalties.

(d) The core features of the MIS solution should include but not limited to following:

i. Availability of the supplied components.

ii. Health and performance of the supplied components.

iii. Track changes and revisions to the supplied components.

iv. Track SLA compliance for the supplied components.

v. Generate SLA reports and other custom reports for the data ingested in the MIS.

vi. Perform predictive analytics based on past data and forecast future performance, downtimes, impacts.

vii. Track availability and performance of the supplied manpower.

viii. Track incident lifecycle.

ix. Identify potential areas of underperformance and improvement.

x. Calculate the applicable penalties as per the SLA compliance and the contractual terms.

xi. Generate Business Intelligence and Analytics Reports as per the requirements of the Purchaser.

xii. Build custom dashboards, reports and live analytics based on custom queries from the user.

xiii. Advanced Search Functionality to search through all the data ingested into the MIS platform.

(e) Define multiple templates for monitoring and tracking different contracts and their respective SLA compliance.
(f) Retention of all ingested data and generated reports for the entire contract period.
(g) Integrate MIS with new data sources.
(h) Patching and bug fixing for the MIS Platform.
(i) Generate Alerts based on specific user defined conditions.
(j) Send reports, alerts, notifications through email, SMS, other messaging platforms.
(k) MIS should also integrate with SIEM, SOAR and other platforms.

5.3.3 **Unified Cyber Security Portal**

a) The MSP shall also implement and maintain a **Cyber Security Portal** of the Purchaser, serving as a broader organisational platform for cyber security awareness, coordination, and reporting. This system shall be distinct from the SOC MIS but capable of **securely interfacing** with it to receive selective, non-sensitive information for wider organisational visibility.
b) The Unified Cyber Security Portal shall:
    a. Serve as a central repository of alerts, advisories, threat bulletins, and incident summaries, including a facility for internal and external stakeholders to securely report cases.
    b. Enable publishing of advisories, guidelines, and awareness material, with both public and restricted-access sections.
    c. Integrate with existing NIC applications, ITSM, ITAM, vulnerability management tools, and other security or asset-related platforms through APIs as required by the Purchaser.
    d. Provide AI-driven search and analytics to quickly surface relevant alerts, advisories, historical incidents, and associated knowledge base articles.
    e. Support internal engagement features such as discussion threads, case tracking, and status updates for reported incidents.
    f. Ensure role-based access controls, logging, and auditing for all user interactions.
    g. Be scalable to integrate new data sources and tools over the duration of the contract.

h. The MSP shall ensure that the Unified Portal integrates with SOC MIS for high-level reporting.

5.4 Manpower Support for 24x7x365 Operations

5.4.1 The MSP shall supply technical resources for all components and solutions, including, but not limited to SIEM, SOAR, Storage, Network, Cyber Security, System Administration, Forensics, Threat hunting, Threat detection, Incidence analysis and response etc., who possess the requisite experience stated in the RFP document. The MSP shall ensure that the deployed product sets are supported 24x7x365.

5.4.2 The Bidder is required to submit a comprehensive resource deployment plan as part of the technical Bid submission, outlining how technically qualified staff shall be allocated at SOC and DR locations to execute the project. The MSP shall be responsible for the monitoring and management of the resources/manpower throughout the project.

5.4.3 The specific manpower requirements are outlined in (paragraph 16.1), which provide only an indication of the minimum number of resources needed to undertake various activities as given in the scope of work. The MSP bears the responsibility of allocating and supplying adequate number of resources/manpower to fulfil the scope of work and ensure compliance to Service Level Agreements (SLAs).

5.4.4 **Terms and Conditions for Resources/Manpower**

(a) The proposed resources/manpower shall be on the payroll of the MSP or the OEM (based on the requirements outlined in paragraph 16.1) during the course of their deployment

(b) The personnel deployed by the MSP under this Contract/Agreement, under no circumstances, be considered employees of the Purchaser. The MSP shall have the sole responsibility for the supervision and control of the personnel deployed in the Project and for payment of such personnel's compensation, including salary, provident fund, withholding of income tax and other taxes, worker's compensation, employee and disability benefits and the like, and shall be responsible for all obligations of an employer, subject to Applicable Law.

(c) The MSP shall designate an experienced and qualified Project Manager as per (paragraph 16.1) as a single point of contact (SPOC) for the Purchaser.

(d) During the Implementation phase, the MSP shall establish a **project governance team** which shall include the Manpower proposed as part of Technical Bid including Project Manager, designated Team Leads and required number of personnel within MSP's hierarchy in order to support the escalation matrix as evaluated in the TEC. The project Governance team shall continue to function for entire contract period. The project governance team shall be responsible for ensuring compliance, conducting reviews, overseeing the project, and providing status reports as defined in the operations manual or any status report as and when desired by the purchaser.

(e) The MSP shall, to the best of its efforts, avoid any change in the organisational structure proposed for execution of this contract or replacement of any human resource appointed. The MSP shall promptly inform the Purchaser in writing if any such change is necessary. In case of replacement of any human resource, the MSP shall ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate handholding period and training for the incoming resource. However, for Deployment of resources as per CVs and deployment plan submitted as part of Technical Bid, penalties shall be applicable as specified in Manpower SLAs in paragraph 6.3.1 Table 6.

(f) The project governance team and resources shall be continued to be deployed post Go-Live according to the deployment plan shared as part of the Technical Bid, and their CVs submitted during the Technical Bid phase. Throughout the contract, these resources cannot be changed, replaced, or have their level of involvement in the services reduced for any reason. In exceptional circumstances, the Managed Service Provider (MSP) is permitted to replace up to 20% of these resources per year after written confirmation from the Purchaser and after proper knowledge transfer.

(g) Post implementation, during the Operational phase, project governance meetings shall be scheduled as defined in the operations manual or at a mutually agreed-upon interval with the Purchaser.

(h) If the deployed resources don't possess the required skill set or if the resources are not able to deliver on the assigned tasks, the resources shall be replaced (with similar or higher skill set and experience as specified in the RFP) within 30 days of receiving such an intimation from the Purchaser (refer Section6)."The Resources are expected to work in a 24x7 security operations environment.

(i) If a resource is not available at the place of duty for more than 3 consecutive days, the MSP shall provide an alternative resource with similar or higher skill set and experience as specified in the RFP at no additional cost to the Purchaser (refer Section 6).

(j) The MSP shall be required to provide dedicated professional grade laptops from well-known OEMs with at least 8 Core latest gen 2.4 GHz CPU, 16 GB RAM and 1TB SSD, standalone MS Office professional (latest version) with perpetual license to the deployed resources as per need. The laptops shall not have any MSP provided applications, MDM, DLP, Endpoint security or other endpoint solution of the MSP. The resources shall install on their laptop, the security and ICT solutions provided by the Purchaser and only applications permitted by the purchaser shall be installed. The resources shall not connect these dedicated laptops anywhere outside Purchaser's network, without an explicit written permission from the Purchaser.

(k) The MSP shall provide atleast 75 number of latest dual screen desktop systems (with latest generation i9/AMD Ryzen 9 or higher, at least 64 GB RAM and 1TB SSD, standalone MS Office professional (latest version) with perpetual license) to be used as SOC workstations. The workstations shall have only the latest version of Windows Operating Systems and shall not have any other applications, MSP provided applications, MDM, DLP, Endpoint security or any other endpoint solution of the MSP. These desktop systems shall be installed with Purchaser provided EDR, UEM and shall be hardened as per Purchaser's policy.

(l) Any MFPs, Printers/Scanners to be used by the MSP deployed teams shall also be provided by the MSP.

(m) The MSP shall be required to provide the documentary proof of the qualifications and experience of the manpower being provided by it during the selection process by the Purchaser.

(n) All manpower shall report to the designated nodal officer(s) assigned by the Purchaser. The MSP must ensure proper planning for backup manpower to comply with the SLAs. This backup manpower must possess equivalent qualifications and experience as the person(s) they shall replace.

(o) MSP/OEM shall furnish the proof of employment of the manpower on the payroll of the MSP/OEM as and when requested by the Purchaser.

(p) Prior to Go-Live, the MSP shall carry out background checks of the resources identified to work on this project and submit the background check reports, along with copies of any of the

officially valid documents as defined under the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, in respect of each such resource. The same process shall be followed post Go-Live in respect of any resource who may be replaced or added, prior to his/her deployment on the project. The Purchaser shall also extend necessary cooperation, which may extend to disclosure of income-tax Permanent Account Number and other identification details, professional history including directorships, disclosure regarding criminal prosecution if any and organisational affiliations, and shall require any resources as aforesaid to so cooperate, for such person to undergo security vetting by such government-designated agency as the Purchaser may communicate in writing. If the Purchaser communicates in writing the fact of a resource having been identified as unsuitable by such agency as aforesaid, at any point of time, the MSP shall take action to promptly revoke all the access to the SOC and its DR locations on immediate basis and remove such resource from the project immediately in any case not later than 24 hours from the receipt of such communication.

(q) The Purchaser shall have the authority to remove or cause to be removed any person employed at the Project site who carries out duties incompetently or negligently, from both in-person and virtual access to the Project resources.

(r) If the Purchaser asks the MSP to remove a person who is a member of the MSP's staff or work force, stating the reasons, the MSP shall ensure that the person leaves the site within seven days and has no further connection with the Services under this Contract. All the access to the deployed and integrated components for the said resource shall be revoked on an immediate basis by the MSP.

(s) The Purchaser reserve the right to change the quantity and location of deployed manpower during the contract period with a written notice, 60 days in advance at no additional cost to the Purchaser.

5.5 Key Deliverables of MSP

5.5.1 The Managed Service Provider (MSP) shall be responsible for end-to-end provisioning, deployment, operation, and management of all supplied components, licenses, and manpower for entire contract duration.

(a) All the supplied components shall:

i. Be provided with full feature and functionality, with the required licensing with no restrictions/limitations for delivering on the required SLA at no additional cost to the Purchaser.

ii. Exhibit high scalability and be deployed exclusively on-premises, unless stated otherwise with minimum N+1 high availability (Excluding standalone SOC tools) mode at each site of deployment.

(b) The MSP must include Annual Maintenance Contracts (AMC), warranty coverage, and provision for office consumables to be used by the MSP deployed team throughout the contract period.

(c) The Gross Total Value shall include the cost of hardware, software, licenses, manpower and other required components.

(d) The MSP is required to provide a comprehensive breakdown of costs for each individual component, including AMC, warranty, and other associated expenses. This detailed breakdown

shall contribute to price discovery and can be utilized by Purchaser for any future procurements, up to 25% of the total contract value.

(e) The Bidder is free to quote a solution with higher capacity and capability, which exceeds the requirements provided in this RFP.

(f) The MSP shall setup dashboard and alerts as per the requirement of Purchaser.

(g) In addition to O&M of the supplied solutions, the MSP shall carry out SOC operational tasks, including but not limited to:

i. Incident Handling and Response
ii. Log monitoring
iii. Dashboard design and customization
iv. Query formulation
v. Correlation rule creation
vi. YARA rule configuration
vii. Snort rule development
viii. Filter and playbook design/implementation
ix. Threat detection and Threat hunting, security threat mitigation and other SOC-related activities.

(h) The MSP shall ensure that the Proof of Delivery/Installation duly signed by the nodal officer(s) assigned by the Purchaser at respective SOC, DR locations, with his name, date of delivery, designation, and office seal, legibly recorded, shall reach NIC Head Quarters, New Delhi within 30 days with the bills, after the date on which the item(s) was delivered / installed.

(i) After the deployment of the supplied components and when they are prepared for Go-Live, the MSP shall get a thorough review and assessment of the architecture and configuration through the respective Original Equipment Manufacturers (OEMs) and shall submit the same to the Purchaser for signoff prior to Go-Live.

(j) The MSP shall integrate the supplied ITSM with all supplied components (Except standalone SOC tools). In addition, the ITSM shall also integrate with Purchaser services like NOC Services, Endpoint security, ZTA, NAC, DRM, DLP, NDR, SSO, SMS Gateway, Email etc.

(k) The SLAs for all purchaser supplied components and services shall be configured on the ITSM.

(l) The MSP is responsible for ensuring complete automation of the entire solution stack, encompassing both the infrastructure and software aspects. This entails providing the necessary technology solutions for end-to-end automation and management as part of the comprehensive solution offering.

(m) All required Hardware, software, database and operating system licences etc. shall be offered as a part of the solution.

5.6 User Acceptance Testing

5.6.1 The MSP shall prepare UAT document comprising of test cases for functional and performance testing.

(a) The UAT document shall be duly approved by the purchaser or purchaser designated agency and the MSP shall submit the same to the Purchaser for Signoff.
(b) The MSP shall ensure that all the test scenarios are identified and provide comprehensive coverage of all aspects.
(c) If any additional test cases are required by the Purchaser, the same shall be included by the MSP and the revised UAT document shall be resubmitted to the Purchaser for the signoff.
(d) The **final approved/signed off UAT document** shall serve as the baseline for testing, and results shall be submitted to the Purchaser for formal acceptance .

5.6.2 The UAT process shall incorporate the below indicative list of stages given below:
(a) Submission of documentations including design, architecture, configuration, troubleshooting, Standard Operating Procedures, Operations Manuals etc.
(b) Test Planning and preparation of test scenarios and test cases
(c) Testing
(d) Reporting
(e) Reviewing
(f) Signoff

5.6.3 The User Acceptance Testing (UAT) shall be conducted by the MSP, after the installation, commissioning and integration has been completed in accordance with the requirements specified in the RFP in the presence of the Purchaser and purchaser designated agency (if any).

(a) The UAT shall be approved by the Purchaser and the MSP shall promptly rectify any deficiencies or non-compliances identified during UAT or as indicated by the Purchaser.
(b) Upon successful completion, the MSP shall submit a duly signed UAT Report to the Purchaser for final sign-off.

5.7 Product Support (Hardware, Platform, Components and Software)

5.7.1 The MSP must ensure the product(s) supplied as part of the contract are supported from the respective OEMs for entire period of the contract, and any extensions thereof, as provided for in the contract, starting from the date of completion of installation and commissioning of the product(s) delivered.

5.7.2 The MSP is required to submit a confirmation/undertaking from the respective OEMs for the same as per **Annex 11**, as part of its technical Bid submission.

5.7.3 The licenses supplied, if any, as part of the solution deployed, shall also include timely supply and deployment of all their upgrades & updates for the entire Contract Period, and any extension thereof.

5.7.4 The MSP must ensure that product(s) supplied as a part of the solution is/are of the latest version at all times during the contract period and any extensions thereof. Any replacement/upgrade of the product that shall ensure better delivery of Service to the Purchaser shall be made available to the Purchaser at no additional cost.

5.7.5 During the Contract Period, if the component/subcomponent goes end of life/ support during the validity of contract, then the MSP shall upgrade the component/ sub-component with an equivalent or superior alternative that is acceptable to the Purchaser at no additional cost to the Purchaser without causing any downtime, performance degradation or non-compliance with SLAs.

5.7.6 The Purchaser shall not bear any responsibility for disputes related to Intellectual Property Rights (IPR) involved in supply/use of the supplied product(s). The Purchaser is not responsible for resolution of such disputes. Resolution of such disputes shall rest entirely with the MSP and/or the concerned OEM.

5.8 Project Delivery Timelines

5.8.1 Following are the timelines for product / service delivery in the Implementation phase of the project. The Implementation phase shall commence after the issuance of the Work Order for Implementation phase. Post Go-Live, annual work orders shall be issued for the Operational phase.

TABLE 3: PROJECT DELIVERY TIMELINES

S. No.	Product / Service Delivery	Timeline
1	Issuance of work order (WO) for Implementation phase which shall include items from S. No. 2 till Go-Live of TABLE 3.	T
2	(a) Complete delivery of Hardware as per BoM and Inspection thereof. (b) Installation of complete hardware and mounting of hardware in the racks (wherever required) and power-on of the hardware. (c) Installation and configuration of software as per BoM for UAT.	T +14 weeks, or earlier = T1
3	System Integration of all MSP supplied platforms for SOC readiness, approved by the respective OEMs for compliance with the technical specifications of the platforms and components as specified in the Contract. For the purpose of integration and testing the MSP may use demo licenses for the S/W.	T1 + 4 weeks, or earlier = T2
4	i. Comprehensive Security Audit of the entire supplied and deployed components by the MSP through a CERT-In empanelled auditor and fixing of vulnerabilities found during the audit based on the scope of work as approved by the Purchaser. ii. Commencement of Deployment of Operational Manpower	T2 + 6 weeks, or earlier = T3

	iii. MSP to acquire acceptance of Tech signoff and UAT from the Purchaser (UAT should be on actual production licenses and not on Demo licenses)	
7	Completion of deployment of Operational Manpower and Go-Live	T3 + 1 weeks, or earlier = T4 (i.e. 25 weeks from Issuance of the work order for Implementation phase)
9	Issuance of first work order for Operational phase including software licenses.	T5 (Within 10 working days of T4)
10	Documentation as per paragraph 5.13	Within the first quarter of issue of first Work Order of Operational phase.
11	i. ISO 20000, ISO 27001 certification ii. Security Operation Centre Capability Maturity Model (SOC-CMM) and Lead Auditor training & certification for ISO 20000 and ISO 27001 to the Purchaser's team as per section 5.10 of this RFP. iii. All Trainings and certifications to members of the purchasers team as per section 5.10 of this RFP.	Within 12 months after T5 (i.e. the date issuance of first work order of Operational phase.)
12	SOC-CMM5 Assessment and Compliance	Within 12 months after T5 (i.e. the date of issuance of first work order of Operational phase.)
13	Governance, Risk Management and Compliance (GRC).	Within first year of the operational Phase.

Note: No SLA/penalty shall apply for the manpower (except Project manager) deployment between T3 to Go-Live.

5.8.2 Acceptance criteria for hardware/software supplied:

a) All hardware/software shall be deployed as per deployment locations in Clause 14.1, Table 14.

b) Delivery shall be accompanied by:

i. Delivery Challan / E-Way Bill

ii. OEM Test Certificates for specific delivered items

iii. OEM sign-off for commissioning

c) Basic inspection shall be conducted jointly by the Purchaser's designated nodal officer and the MSP at the deployment location.

d) Upon successful inspection, the nodal officer shall accept the delivered items and countersign the OEM Test Certificates.

5.8.3 The Project Manager shall share a weekly progress report as per project timelines with the Purchaser.

5.8.4 The software licenses (Perpetual or annual subscription as the case may be) and hardware warranty shall start from the date of Go-Live.

5.8.5 The Tech Sign Off criterion for each Hardware, Platform, Components and Software shall include demonstration of all relevant features as per the defined technical specifications. Minimum sign off criterion is defined below:

TABLE 4: TECH SIGN OFF CRITERIA

Sr. No.	Technology/ Solution	Signoff Criteria
1.	Security Incident Event Management (SIEM) with at least 7 Lakh EPS, extendable upto 10 Lakh EPS and more.	(i) Demonstration of all use cases along with integration with at least 50 unique log sources (comprising of compute, network, storage, security, application, email, database, Operating system and website logs) and integration of the integrated logs with SOAR (ii) Demonstration of all features and functionalities as per RFP
2.	Security Orchestration Automation Response (SOAR)	(i) Demonstration of at least 30 playbooks, covering all the log sources and devices integrated with the SOAR. (ii) Demonstration of all features and functionalities as per RFP
3.	ITSM	(i) Demonstration of all use cases along with demonstration of its integration with MSP supplied components and SIEM, SOAR, SSO, Email etc. of the Purchaser as defined in the technical specifications of the ticketing tool. (ii) Demonstration of all features and functionalities as per RFP (iii) Discovery of 10,000 Assets. (iv) Demonstration of SLA Monitoring and Compliance (in accordance with Tender) dashboards, alerts and reports.

4.	Attack Surface Management Platform	(i) Demonstration of all features and functionalities as per RFP. (ii) Enumerate Attack surface of IP Ranges and domains shared by Purchaser (iii) Fingerprint the services exposed on the IPs and Domains shared by the Purchaser (iv) Enumerate the vulnerabilities on Purchaser's assets exposed on the internet
5.	Incident Response Retainer service from a security OEM	(i) Written agreements from the security OEM, including online portal access for raising security incidents with the OEM, confirming the provision of incident response retainer service to NIC during the contract period. (ii) The OEM should provide a provision to convert the unused incident response retainer hours to training and certification for Purchaser's employees.
6.	Digital Forensic Suite	(i) Demonstration of all features and functionalities as per RFP. (ii) Conduct digital forensic image acquisition, forensic analysis, triage (local and remote) and share the detailed forensic report containing the full details of the incident. (iii) The Report should contain the full timeline of malicious activities and their artefacts.
7.	Data Recovery tools	(i) Demonstration of all features and functionalities as per RFP. (ii) Recover data from a disk / system, supplied by the purchaser (iii) Reporting template finalisation
8.	Static and Dynamic Analysis sandbox from 3 OEMs	(i) Demonstration of all features and functionalities as per RFP.

		(ii) Demonstrate static and dynamic analysis of at least 30 unique file samples with various attachment types across windows, linux and Mac OS environments. (iii) Submit detailed report of the static and dynamic analysis of the 30 unique file samples. (iv) Demonstrate analysis of samples with anti-evasion techniques, debug mode detection, VHD & ISO files.
9.	SOC Logistics tool and standalone systems for system Image storage.	1. Signoff to be decided during design phase.
10.	Mobile Forensic Suite	(i) Demonstration of all features and functionalities as per RFP. (ii) Acquire digital image from a mobile device, perform forensic analysis of the acquired digital image. (iii) Submit forensic analysis report.
11.	Memory Forensic Suite	(i) Demonstration of all features and functionalities as per RFP. (ii) Acquire memory dump from at least 10 remote systems comprising of windows, linux and Mac OS (iii) Aggregate the gathered memory dumps in central server and analyze the memory dumps for potential threats/anomalies. (iv) Submit memory analysis report
12.	Mac Forensic Suite	i. Demonstration of all features and functionalities as per RFP. ii. Conduct digital forensic image acquisition, forensic analysis, triage (local and remote) for mac systems and share the detailed forensic report containing the full details of the incident.

		iii. Report should contain the full timeline of malicious activities and their artefacts.
13.	Cloud Forensic Suite	i. Demonstration of all features and functionalities as per RFP. ii. Conduct digital forensic image acquisition, forensic analysis, triage for cloud environment and share the detailed forensic report containing the full details of the incident. iii. Report should contain the full timeline of malicious activities and their artefacts
14.	Steganography Forensic Suite	i. Demonstration of all features and functionalities as per RFP. ii. Demonstrate steganography payload generation
15.	e-Discovery Forensic Data Analytics Platform	i. Demonstration of all features and functionalities as per RFP. ii. Aggregate all forensic evidences captured from other forensic solutions iii. Perform analytics on the composite forensic data/evidence and provide meaningful insights to aid investigation iv. Submit detailed analytics report
16.	Network Forensics	i. Demonstration of all features and functionalities as per RFP. ii. Capture network traffic of at least 5 Gbps for 30 mins and perform forensic analysis on the captured traffic. iii. Submit detailed forensic analysis report, covering all network protocols captured in the traffic.
17.	SOC and Forensics Workstations and Laptops etc.	N/A

18.	Forensic Tools (Accessories and logistic tools)	Demonstration of products
19.	Forensic disk Imager with hardware write blocker	i. Demonstration of all features and functionalities as per RFP. ii. Perform at least 3 parallel disk image acquisition and demonstrate the write blocker functionality.
20.	Magnetic Media Degausser & Secure Drive Eraser	i. Demonstration of all features and functionalities as per RFP. ii. Perform drive erasure on at least 3 Magnetic hard disk using Degausser. iii. Perform drive erasure on at least 3 SSD/NvMe based hard disk with 7-pass erasure, using secure drive erasure iv. Submit Disk Erasure report
21.	Digital Forensic Incident Response Tool	i. Demonstration of all features and functionalities as per RFP. ii. Perform live incident remote triaging on windows, linux and Mac systems parallelly. iii. Collect forensic artefacts from the 3 Operating Systems. iv. Conduct IOC based and YARA rule based search on the 3 Operating Systems for any threats or anomalies v. Execute live queries on the 3 Operating systems from a central management console
22.	Threat Intelligence (IOC Feeds, IP and web reputation feed, Deepweb Dark Web, Social Media and OSINT Feeds)	i. Demonstration of all features and functionalities as per RFP.
23.	Portable Log Analyzer	i. Demonstration of all features and functionalities as per RFP.
24.	Hardware appliances/software solutions for securing MSP supplied solutions.	i. Demonstration of all features and functionalities as per RFP. ii. Presentation on sizing and integration of such appliances/solutions in the

		overall design of the proposed SOC.
25.	MIS solutions and its components	i. Demonstration of all features and functionalities as per RFP. ii. Rest to be developed during the contract period.
26.	Governance, Risk & Compliance solution	i. Signoff to be decided during system integration phase.

5.9 Terms and Conditions for Proposed Infrastructure

5.9.1 The scope entails the establishment of crucial components of Purchaser's SOC, including hardware and software installations, as well as the commissioning of the supplied items. This may necessitate additional items/accessories such as sub-components, assemblies, sub-assemblies, cables, connectors, sockets, and patch cords, all of which shall be provided by the MSP at no extra cost.

5.9.2 All equipment/platforms shall be IPv4 and IPv6 compliant (dual-stackable)

5.9.3 **For technical evaluation purposes, the unpriced bill of materials (BOM) containing hardware and all software components shall be included as part of the technical Bid submission.** The unpriced BOM shall not deviate from the one submitted in the financial Bid, or it may lead to rejection of the Bid. Bidder to ensure that unpriced BOM submitted as part of the technical Bid does not include any pricing or financial details but it should include the product name, OEM and Sizing etc. All such components shall be verified as part of the **Tech Sign-Off process in Clause 5.8.5** prior to acceptance.

5.9.4 In case any component provided by the MSP doesn't meet the functional and/or performance parameters specified by the MSP in the proposal and demonstrated during **Tech sign-off**, then the additional/replaced component shall be immediately provided and installed at the MSP's expense without impacting service continuity. Clause 5.7.4 of this RFP shall also apply.

5.9.5 The MSP shall adhere to the high-level features and detailed functional specifications provided in Section 15 (Technical Specifications) and Annexures. All necessary software, hardware, peripherals, and accessories (indicative list in Annex 17) required for end-to-end functioning of the SOC solution shall be provided, even if not explicitly listed in the BoM, at no additional cost to the Purchaser. Specifications mentioned in this RFP are minimum requirements; the MSP may quote higher or equivalent specifications. The RFP and Annexures together constitute the overall requirements of the solution.

5.9.6 The Bidder shall quote the products strictly meeting or exceeding the tendered specifications/requirements. All relevant technical details, including those relating to the make, model, specifications and salient features of the solutions and tools offered, shall be furnished with the Bid. Clause-wise compliance with the specifications/requirements, along with documentary proof and references in support of the same, shall be furnished by the Bidder.

5.9.7 The MSP shall be responsible for implementing and maintaining infrastructure and documentation in accordance with industry best practices such as NIST 800-53, ISO 20000, ISO 27001, SOC-CMM etc. Additionally, the MSP shall obtain ISO 20000 and ISO 27001 certifications for Primary GSOC (New Delhi) and DR (Hyderabad), Channai covered under the contract within twelve months of Go-Live. The cost of ISO certification, facilitated by an authorised agency, shall be incurred by the MSP. It is crucial that the MSP maintains these standards throughout the period of the contract.

5.9.8 All failed or decommissioned disks from any of the supplied products shall remain the property of the Purchaser and must be handed over to the Purchaser securely after removal.

5.9.9 Interoperability/compatibility of different passive components shall be responsibility of the MSP.

5.9.10 The MSP shall architecture the solution with no single point of failure (SPOF). The MSP shall demonstrate redundancy and failover capabilities during Tech sign-off.

5.9.11 The MSP shall provision all tools/software/hardware/appliances meeting or exceeding the specifications as per Section 15 to ensure quality and performance.

5.9.12 MSP shall provide necessary redundant Fiber Channel/converged switches and modules/cables (if required) for the storage solution to meet the storage port controller connectivity and performance.

5.9.13 The US Dollar foreign exchange component as specified in **Annex 5, Table-3** quoted by the Bidder shall be as per RBI website (closing rate) for the foreign currency indicated (as import component) on last date of final Bid submission shall be taken as reference for Financial Bid Evaluation.

5.9.14 The costs provided shall include rates for installation, commissioning, testing, and any other related activities.

5.9.15 Unit Price shall be exclusive of the price for packaging, forwarding, freight, insurance charges, logistics or any other charges cost for deployment at locations specified for delivery in/under this RFP.

5.9.16 The entire solution is for on-premise. All the features requested with the exception of Attack Surface Management Platform in the RFP document shall function on-premise without the requirement for any external connectivity to the internet or cloud except for obtaining any updates etc. The deployment environment shall be verified during **Tech sign-off** For platforms offered on cloud, the Hardware components asked for in the BoM need not be quoted.

5.10 Training & Support

5.10.1 As a part of deliverables, the MSP has to provide the following trainings:

(a) **Training on SOC Operations:**

(i) The MSP shall impart yearly operational training to at least 50 designated officials and resources of the Purchaser at Purchaser's location in two batches of 25 officials each. This training shall cover a session on SOC operations and best practices for information security & general cyber and information security awareness on emerging trends. The duration of each such yearly training session shall be of 3 to 5 days.

(ii) The standard contents of such training shall be documented and made available to all the users. Two copies in hard and soft format shall be made available to the in-charge of every location. Changes to the same shall be updated periodically as and when required and the same shall be communicated to the respective sites.

(b) **Technical training**

(i) Conduct half yearly training through cyber security OEMs on provisioned OEM components and multiple emerging threat scenarios as per NIC's requirement. The biannual training shall be provided to two batches of 25 persons each. The duration of each such half yearly training shall be of at least 5 days.

(ii) Provide Lead Auditor training with certification on ISO 20000 and ISO 27001 to ten officers from NIC.

(iii) Training on SOC capability maturity model certification (CMM5) for five officers of NIC.

(iv) The contents of such trainings would need to be documented and made available to all the Purchaser for training other officers of NIC.

(v) Provide one time training & certification on provisioned OEM components to 10 members of the Purchaser's team.

(c) **Cyber security awareness training for field units**

(i) Shall conduct cybersecurity awareness trainings to DCISOs and teams deployed by the purchaser at various Government ministries/departments/states. The trainings shall be conducted biannually at purchaser's location. In case of urgent requirement of the Purchaser, more such training shall be conducted on demand. The duration of each such training shall be at least 3 days.

5.11 Audit

5.11.1 **The MSP shall ensure the following audits and assessments:**

(a) Security Assessment: The MSP shall get the comprehensive security audit of entire SOC solution (including all MSP supplied and deployed components) done annually as per scope of work (Refer Annex 14 for guidelines for audit) through a CERT-In empanelled third-party auditor.

i. The audit shall be conducted by a CERT-In empanelled third-party auditor **not affiliated with the MSP**. If the MSP is itself a CERT-In empanelled auditor, it must engage a different, independent CERT-In auditor for compliance.
ii. The MSP shall submit the full audit report and a signed compliance closure report to the Purchaser within **two weeks** of receiving the auditor's findings. All remediation actions must be completed before submission.
iii. All costs for the annual audit shall be borne by the MSP.

(b) Forensic Investigation: NIC reserves the right to initiate a forensics investigation of the ecosystem deployed by the MSP through a 3rd party auditor, annually and also in case of specific inputs received from investigating agencies with the required evidence. The cost for such audit shall be borne by the MSP. If the forensic investigation report identifies issues due to lapses in implementation and compliance by the MSP and there are two such events wherein a lapse is found, the Purchaser reserves the right to:

i. Invoke the Termination paragraph 13.21.
ii. Forfeit the Performance Bank Guarantee (PBG).

5.11.2 **Limited Audit** - The MSP may be asked to conduct an internal limited audit at its own cost and submit the compliance to the Purchaser within two weeks of submission of the audit report by the Auditor. Refer **Annex 14** for guidelines for such audit.

5.11.3 Failure to comply with the closure of audit findings shall result in penalties as per **Section 6.3.** Repeated failures to comply with the closure of audit findings may lead to termination under Clause 13.21.

5.11.4 The MSP will ensure that the audit findings report is not shared with any third party without the prior approval of the Purchaser.

5.11.5 The MSP will ensure that the auditor hired for the audit does not have a conflict of interest with the Purchaser. Therefore, the MSP must obtain approval from the Purchaser before hiring the auditor.

5.12 Governance, Risk Management & Compliance

5.12.1 The purchaser shall order the GRC tool in the first work order of Operational phase to the MSP. Following shall be the scope of the MSP for GRC implementation.

(d) **Supply, Installation and configuration:**

(i) The MSP shall supply and install the required hardware and software of the GRC tool at Primary data centre of the purchaser i.e., NDC Delhi and at DR location i.e., NDC Hyderabad. The GRC tool should be a no code / low code product capable of customization for Governance Risk and Compliance (GRC) workflows and dashboards. This GRC tool shall be used by purchaser for GRC compliance reporting, tracking and monitoring for purchaser internal systems / assets. It should also be capable of extending GRC compliance reporting, monitoring and providing dashboard view of GRC compliance of various Govt of India Ministries / Departments.

(ii) The MSP Shall deploy the required technical resources for installation, operations and maintenance of hardware. In addition, the MSP should factor functional resources to support designing of GRC workflows and dashboards basis KPI's as and when required by the Purchaser during the course of contract execution, which shall work under the CIS Governance Division of the Purchaser.

(iii) Shall conduct internal information security audit of GRC tool before its commissioning.

(iv) Shall document security audit approach, methodology and results; same shall be submitted along with other necessary documents.

(v) Shall install and commission the GRC tool and shall be made to Go-Live within one year of receipt of the work order for the same.

(vi) Shall ensure that the GRC tool integrates online and seamlessly with other systems, software and applications (Including various security tools for VAPT, Source Code, AppSec etc.) in use within the purchaser organisation. The GRC tool should be capable of such automation integration with these security tools and should be able to automatically fetch the vulnerabilities data to populate the GRC compliance scores.

(vii) Shall prepare comprehensive documentation for each stage of the work for future reference and troubleshooting.

(viii) Shall offer continuous support to resolve any technical and functional issues that arise following implementation during entire contract period after Go-Live of the GRC tool.

(ix) Shall perform regular system updates, patching and backup of the data, application configurations.

(x) Shall ensure monthly backup and/or archival for GRC tool.

(xi) Shall support and perform incident management for GRC tool.

(e) **Implementation and operations:**

(i) The MSP shall prepare scope of GRC tool including systems, processes, assets.

(ii) The MSP shall prepare a purchaser input proforma for the information required from the purchaser for configuration of the GRC tool.

(iii) Purchaser shall supply the required information within one month of receipt of the proforma.

(iv) The MSP shall prepare Integration configuration of GRC tool with other ecosystem applications/ systems. This shall include the systems and assets of the purchaser. MSP should ensure that GRC tool is capable of integrations with other Purchaser systems and processes as and when needed by Purchaser.

(v) Shall configure fields, layouts, workflows, data driven events, calculation logic, navigation menu, reporting requirements, alerts. Such requirements shall be finalized in agreement between MSP and the Purchaser after a thorough design review. If needed, a pilot

implementation may be rolled out for select entities / assets / functions, as may be required by the Purchaser to assess the effectiveness of layouts, workflows, data driven events, calculation logic, navigation menu, reporting requirements and alerts etc.

(vi) Shall configure user access for different modules / dashboards / report as per requirement.

(vii) Shall design and document policies to be implemented on GRC tool aligned with GRC Framework, governing policies, processes, procedures and organisation structure.

(viii) Shall develop and implement scenarios and use cases and custom modules for GRC tool.

(ix) Shall impart necessary training of GRC tool to staff covering aspects i.e., generate reports on demands, enabling continuous monitoring, configuration of tool, troubleshooting basic operations and provide training material.

(x) Shall develop on-demand modules based on the requirements and implementation of Dashboard and Reporting requirements.

(xi) Populate periodic reports (Weekly, Monthly) and customized dashboard in GRC Tool

Support upgrade GRC Tool to latest version in case the supplied version goes out of support by the OEM.

5.13 Documentation

5.13.1 The MSP shall be responsible for creation and maintenance of all the documentation and shared with the Purchaser as per mutually agreed format and periodicity.

5.13.2 The documentation must be consistently updated throughout the contract period, following appropriate change management procedures and version control practices. It is recommended to adhere to international standards and best practices, such as ISO 27001, National Institute of Standards and Technology (NIST) 800-53 when creating the documentation. The documentation shall include but not be limited to the following:

(a) Design (HLD, LLD) and Architecture

(b) Installation and Configuration

(c) Operations manual for the SOC

(d) System administration

(e) Security Hardening manual

(f) Testing manual

(g) Troubleshooting Manual

(h) Standard Operating Procedure

(i) Crisis Management Plan and Manual

(j) Backup Plan and Manual

(k) ISO Compliance Documents

(l) SOC-CMM5 assessment and compliance within the first quarter of issue of first Work Order of Operational phase.

5.13.3 The MSP shall be responsible for maintaining and updating all the documents, related to the supplied components in the instance of but not limited to the following:

(a) Introduction of new ICT components or tools/ Change Management.

(b) Any configuration change impacting functionality, security, or interoperability.

(c) Policy changes issued by the Purchaser or the Government.

(d) Findings from audits (Clause 5.11) or incident Root Cause Analysis.

5.13.4 Failure to deliver, update, or maintain documentation shall:

a) Be subject to SLA penalties as per Section 6.3.
b) Be flagged as a **non-compliance** in internal and third-party audits (Clause 5.11).
c) Allow the Purchaser to withhold milestone or quarterly payments until deficiencies are rectified.

5.14 Roles and Responsibilities of the MSP

5.14.1 The responsibilities of the MSP in addition to the SOC operations, shall include, but not be limited to, the following:

(a) OEM Coordination and Integration – Manage end-to-end coordination with OEMs for all supplied components, including:
   i. Procurement, delivery, installation, configuration, and integration.
   ii. Escalation and resolution of OEM-related issues within SLA timelines.
   iii. Ensuring firmware/software upgrades and security patches are applied as per Clause 5.9 and documented as per Clause 5.12.

(b) Transparency and Reporting – The MSP is required to share all internal review documents and reports used to monitor and execute the project with the Purchaser upon request and as deemed necessary.

(c) Logistical Support – Arrange all necessary logistical and operational support for MSP resources deployed at Purchaser locations, including travel, accommodation, equipment, and consumables throughout the period of the contract.

(d) Software, Licenses, and Tools - The MSP shall arrange all the requisite software, licenses and any other items required to complete the deployment and integration.

(e) Availability and Uptime - Responsibility of availability and uptime of the complete supplied infrastructure (Hardware and software) as specified in Bid document shall rest with the MSP.

(f) Cybersecurity Responsibility - The cyber and information security of the deployed solution, shall also be the responsibility of the Bidder.

5.15 Roles and Responsibilities of the Purchaser

5.15.1 Purchaser shall provide the necessary sitting space for the resources deployed as part of this project.

5.15.2 The physical setup of the SOC and DR shall be done by the Purchaser. This shall include arranging building space, completion of required civil and electrical works, setting up of display screens, space for workstations etc. However, this shall not include the platforms and other ICT components which the MSP has to supply and setup as part of the scope.

5.15.3 The purchaser shall make arrangements for marking of attendance of the deployed manpower resources.

5.15.4 The Purchaser shall maintain such attendance records for MSP deployed manpower. These records shall be binding for SLA compliance and deduction of penalties etc.

5.15.5 Housekeeping and physical security of GSOC.

5.15.6 The purchaser's CIS Governance Division shall review GRC design proposed by the MSP and shall provide inputs to MSP on GRC design including layouts, workflows, data driven events, calculation logic, navigation menu, reporting requirements and alerts etc.

6. Service Level Agreement and Penalties

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the MSP to the Purchaser for the period of the contract. The SLA shall be binding on the MSP and will remain in force for the entire duration of the Contract.

6.1 Key definitions of Service and security SLA

6.1.1 Security Incident

A *Security Incident* is any event or series of events that results in, or poses a credible threat of, loss of confidentiality, integrity or availability of information that Purchaser's ICT system processes and/or stores and/or transmits or a violation of Government security policies/procedures/guidelines/regulations. Some of the common examples of an incident w.r.t the scope of this RFP includes but not limited to the following:

(a) Complete or partial failure of an ICT Hardware or Software or Service
(b) Non-Availability of an ICT Hardware or Software or Service
(c) Defacement, unauthorized modification, or tampering of a Website/Application
(d) Cyber Security Breach
(e) Digital Data Loss, Digital Data Leak etc.
(f) Phishing, Spam, Vishing or related social engineering attacks
(g) Infection of Malware, Trojan, Virus, Ransomware, Worms, spyware, or similar malicious software etc.
(h) Unauthorised access to a data, application, service, database, hardware, software, SOC premises etc.
(i) Cyber-attacks including hacking, exploitation of vulnerabilities, or intrusion attempts
(j) Command and Control Communication
(k) Advanced Persistent Threats (APTs)
(l) Denial of service, Distributed Denial of Service
(m) Security misconfiguration
(n) Negligence/mishandling of ICT infrastructure by the MSP team.
(o) Violation of existing security best practices and SoP defined by the Purchaser.
(p) Any act or attempt of sabotage, tampering or deliberate harm to Government ICT infrastructure.

6.1.2 Service Request

A Service Request is a request made to MSP to fulfil a requirement for day-to-day operations as per scope specified in this RFP. Some of the examples of a Service Request includes but not limited to the following:

(a) Request to create/delete or modify a user account
(b) Request to integrate an asset with the ITSM.
(c) Request to investigate or analyse a system for potential security threats or compromise
(d) Request to collect forensic evidence from an asset suspected/confirmed to be infected or compromised.
(e) Request to conduct forensic analysis of ICT systems.
(f) Request to conduct Root Cause Analysis (RCA) of the incident.
(g) Request to review configuration, design, architecture, deployment of an Application/Hardware/Database/Service etc. from the cyber security perspective.
(h) Request to analyse logs for a specific anomaly or attack or compromise

(i) Request to conduct a security breach assessment.

6.1.3 Problem

A problem ticket shall be generated for recurring incident or for incidents whose actual root cause is not known. The problem ticket shall be used for further investigation to determine the actual root cause. It is mandatory to identify the root cause for all problem tickets. The root cause shall be clearly recorded in detail in the internal knowledge base as part of ITSM and tagged appropriately. The identified root cause shall be validated and technically accepted by the end User to whom the problem ticket belongs or the Purchaser. The problem report shall also mandatorily include appropriate corrective action and preventive action to prevent the re-occurrence of the incident/problem.

6.2 Priority types of Service SLA

6.2.1 Any incident, service request, problem can be categorized as P1, P2 or P3 based on the impact of the incident as given in the Priority Table.

6.2.2 The penalties and closure timelines shall be applied based on the priority of the ticket for any incident/service request/problem as described below.

6.2.3 Any security incident relating to the supplied components must be promptly notified by the MSP to the Purchaser and necessary corrective actions must be taken by the MSP to protect the security of the components and the data.

6.2.4 Addressing the issue of advanced threats and cyberattacks, the supplied components shall be monitored by the MSP round the clock for any potential threats/risk and the same needs to be detected immediately and resolved within the timelines defined as per their priority type.

6.2.5 MSP must submit Monthly SLA Compliance report to the Purchaser including reports of component health monitoring, availability etc. The necessary solutions for generating SLA Compliance reports shall be provided by the MSP. Any SLA breach must be reported with reasons and corrective action plan immediately.

TABLE 5: PRIORITY TABLE FOR SERVICE SLAS

Priority Type	Description	Impact	Target/Timelines for closure
Priority-1 (P1)	1. Incident Monitoring, detection/reported and response till resolution which have the potential to— (a) cause severe damage/impact to multiple Systems/Assets; or (b) Results in Reputational Risk of Purchaser/Organisation. (c) Critical security vulnerabilities or exploits	Multiple systems or services are impacted OR complete service unavailability.	1. Incident resolution with required finding, and recommendation, corrective, preventive measures • within 3 hours 2. Service Request closure • within 3 hours 3. Problem closure/resolution including submission of Root Cause Analysis • within 12 hours 4. Audit finding closure/resolution

	affecting core infrastructure 2. Service Request whose non-fulfilment could lead to a security incident or security vulnerability or service disruption 3. Audit findings related to supplied and deployed platform and components that are rated as critical and high		• within 18 hours 5. Downtime/ Unavailability of any of the supplied Hardware/Platforms /Components • Resolution within 3 hours
Priority-2 (P2)	1. Incident Monitoring, detection, reported and response till resolution which have the potential to cause— (a) considerable damage to few systems/Assets; or (b) results in a security threat to the Purchaser/Organisation. 2. Service Request whose non-fulfilment could lead to a security incident or security vulnerability or service disruption 3. Audit findings related to supplied and deployed platform and components that are rated as medium	Few services of one system are impacted	1. Incident resolution with required finding, recommendation, corrective, preventive measures • within 6 hours 2. Service Request closure • within 10 hours 3. Problem closure/resolution including submission of Root Cause Analysis (RCA) • within 24 hours 4. Audit finding closure/resolution • within 48 hours 5. Downtime/ Unavailability of any of the supplied Hardware/Platforms /Components • Resolution within 6 hours
Priority-3 (P3)	1. Any other category of Incident/Problem/ Service which is not covered under P1 and P2 category 2. Service Request whose non-fulfilment could lead to a security incident or security vulnerability or service disruption 3. Audit findings related to supplied and deployed platform and components that are rated as low	No immediate impact on Operations	1. Incident resolution with required finding, and recommendation, corrective, preventive measures • within 12 hours 2. Service Request closure • within 20 hours 3. Problem closure/resolution including submission of RCA • within 48 hours 4. Audit Finding closure/resolution • within 72 hours 5. Downtime/ Unavailability of any of the supplied

			Hardware/Platforms /Components • Resolution within 10 hours

6.3 Penalties on SLA

6.3.1 Applicable penalties are defined in table below:

TABLE 6: PENALTIES ON SLAS

Sl. No	SLA Type	SLA Parameter	Target/Timelines for closure	Penalty
1	Service	Incident Resolution	Refer Priority Table under paragraph 6.2	0.002% of quarterly payment for every 1-hour delay beyond the timelines as specified in paragraph 6.2 with maximum capping of 10% of quarterly payments
		Service/Problem Resolution	Refer Priority Table under paragraph 6.2	0.01% of quarterly payment for every 1-hour delay beyond the timelines as specified in paragraph 6.2 with maximum capping of 10% of quarterly payments
1a		The incidents raised with the incident response retainer service provider shall be resolved as per the following service levels : • P1 Incidents shall be resolved within 6 hrs • P2 Incidents shall be resolved within 12 hrs • P3 Incidents shall be resolved within 24 hrs All incidents shall be acknowledged within 15 minutes and incident response personnel should be	Refer Priority Table under paragraph 6.2	0.01% of quarterly payment for every 1-hour delay beyond the timelines as specified in paragraph 6.2 with maximum capping of 10% of quarterly payments

		assigned for the ticket.		
2		Non-Submission of RCA	Refer Priority Table under paragraph 6.2	0.01% of quarterly payment for every 8 hours delay beyond the timelines as specified in paragraph 6.2 with maximum capping of 10% of quarterly payments.
3		Recurring Problem for which RCA was submitted	Non-occurrence of Problem after RCA	Double the relevant penalty shall be levied for recurring problems during the contract period.
4		Closure of Audit Findings with respect to paragraph 5.11	Refer Priority Table under paragraph 6.2	0.05% of quarterly payment for every 24 hours delay beyond the timelines as specified in paragraph 6.2 with maximum capping of 10% of quarterly payments.
4a		Failure to conduct annual/half-yearly audits	Refer Paragraph 5.11	0.05% of quarterly payment of the quarter in which half yearly or annual audit was to be completed.
5	Availability	Availability of all components from the Supplied Hardware.	99.97%	0.05% of quarterly Payments for every 0.1% reduction from the target SLA, for each individual component. with maximum capping of 10% of quarterly payments.
6		Downtime/ Unavailability of all supplied components/platforms due to changes/ modifications made in the supplied hardware/ solution during the contract period.	Refer Priority Table under paragraph 6.2	0.25% of quarterly payment for every 2-hour delay beyond the timelines as specified in paragraph 6.2 with maximum capping of 10% of quarterly payments.
7		Availability of Supplied platforms, software, Applications, Databases and Services.	99.97%	0.05% of quarterly payments for every 0.5% reduction from the target SLA, for each individual component. with maximum capping of 10% of quarterly payments.

8		Health/Performance of Supplied Components.	99%	0.05% of quarterly payments for every 0.5% reduction from the target SLA, for each individual component. with maximum capping of 10% of quarterly payments.
9	DR Drill	Quarterly DC (NDC, New Delhi) to DR (NDC, Hyderabad) switchover drill along with DR Drill report.	First fifteen days of every Quarter.	For each week, or part thereof, of delay in the DR Drill beyond the first fifteen days of every Quarter, a penalty of 0.05% of the total Quarterly payment shall be deducted with a maximum capping of 10% of Quarterly payment.
10	Security	Deployment of latest security patches on all supplied hardware and software components.	Within 24 hrs. from the time the patch was made available to the MSP by OEM unless an extension is given by the Purchaser in writing to the MSP.	0.05% of quarterly payments for every 12-hour delay for each individual component, with a maximum cap of 10% of total quarterly payment.
11		Detection of Zero-day vulnerabilities and any security incident which goes undetected.	The MSP has to provide the solution within 12 hours after reporting the incident	0.25% of quarterly payment for every 1-hour delay beyond the 12 hours, with a maximum cap of 10% of total quarterly payment.
12		Deployment of mitigation measures for preventing the exploitation of unpatched vulnerabilities (whose patch is yet to be released by OEM)	Within 72 hrs. from the time the information about the unpatched vulnerability is received from OEM or through any other source	0.25% of quarterly payments for every 24-hour delay for each individual component, with a maximum cap of 10% of total quarterly payment
13		Deployment of software updates (including BIOS, Firmware, OS, etc.) on all supplied components	Within 7 days from the date of update release by OEM	0.25% of quarterly payments for every 72-hour delay for each individual component, with a maximum cap of 10% of total quarterly payment.
14		Security breach related the	No Security Breach is acceptable either due to the provided	A penalty of 8% of the Quarterly payment shall be levied on every breach.

		ecosystem deployed by the MSP Note: It includes any type of security breach in the solution provided or due to the solution provided by the MSP which includes but not limited to all the hardware, software, and tools.	solution or in the provided solution.	
15		Detection of Security Incident	Within 30 Minutes from the time of incident occurrence	0.005% of quarterly payment for every 30-minute delay for each incident with maximum capping for 10% of quarterly payment.
16		Detection of brand monitoring, brand protection Threat Intel – Deep Web, Dark Web, OSI NT, Social Media	Within 72 hours of creation / hosting of brand abuse e.g., incident types given below but not limited to: Trademark/copyright impersonation, Counterfeit website, mobile app, Phishing website, Internal source code leak, API keys, secret keys, authentication tokens, Repo containing usernames, passwords, Internal documents leak, Brand pages on social media, social media posts and fake citizen service numbers, toll free numbers etc.	0.001% of quarterly payment for every 12-hour delay from average detection time of 72 hours for the quarter with maximum capping for 10% of the quarterly payment.
17	Manpower	Penalty for unauthorised absence of onsite resources	Absence of an onsite deployed resource	Penalty at the rate of Rs. 15000 per day of absence of Project Manager and Rs. 5000 per day for all other

				resources shall be levied on the MSP and no payment shall be made for the duration of unauthorised absence. The penalty shall be deducted from the quarterly payments with the maximum capping of 10% of the quarterly payment.
		Delay in deployment of Project manager during Implementation phase	MSP shall ensure the presence of Project Manager to be deployed at the initiation of the implementation of the project.	Penalty at the rate of Rs. 15000 per day of absence of Project Manager with maximum capping of 10% of quarterly payments.
		The deployed manpower resources shall mandatorily use the email id provided by NIC for all official communications related to The Purchaser.	Use of any other email id/other unauthorised mode of communication is strictly prohibited	In the instance of any manpower violating this condition; 1. 0.1% of quarterly payments shall be levied for each such instance of violation, with maximum capping of 10% of quarterly payments. 2. He/she shall be immediately removed from the project and replacement for the same shall have to be provided by the MSP within 15 days of removal of the manpower.
		Removal of manpower by the purchaser due to any default.	MSP shall provide replacement for the removed manpower within 15 days	Failure to provide replacement within 15 days shall further invite a penalty of 0.01% of quarterly payments per day beyond the permissible time of 15 days with maximum

				capping of 10% of quarterly payments.
		Resignation/ Replacement of Resource based on confirmation of The Purchaser.	1) The MSP shall provide in writing at least 30 days prior to the last working day of the deployed resource at deployment location or from the date of submission of resignation. 2) The resource shall not be relieved without proper exit management and written No objection certificate (NoC) from The Purchaser. 3) The MSP shall replace the resource at its own cost and deploy the new resource for Knowledge Transfer (KT) at least 15 days prior to the last working day of the outgoing resource. 4) Removal of two or more resources by the Purchaser based on performance in one quarter.	1. If any resource absconds or resigns or shifted out of deployment location in violation of these terms and 1% of quarterly payment in case of absconding, with maximum capping of 10% of quarterly payments. 2. If the resource is removed without proper No Objection Certificate (NoC), a penalty of 0.1% of quarterly payments shall be applied for each such resource, with maximum capping of 10% of quarterly payments. 3. A penalty of 0.01% of quarterly payments shall be applied per day for the number of days which are less than the required number of 30 days of Knowledge Transfer, with maximum capping of 10% of quarterly payments. 4. A penalty of 2% of quarterly payments shall be applied for first such instance with maximum capping of 10% of quarterly payments. 5. A penalty of 5% of quarterly payments shall be applied for second such instance with maximum capping of 10% of quarterly payments.

		The resources deployed not be used by the MSP for any other project.	The resources deployed through this RFP shall work for the Purchaser only and shall not be used by the MSP for any other project.	1. If any resource is found to be working on any project/activity, which is not assigned by Cyber Security Group of The Purchaser, then such manpower shall be immediately terminated from the project. A penalty of 1% of quarterly payments shall be levied, for each such instance with maximum capping of 10% of quarterly payments.
		Deployment of Resources (as per Contract)	The MSP has to complete the manpower deployment at respective locations as per defined timelines (refer paragraph 5.8)	0.01% (of the quarterly payment shall be deducted as penalty) for each day of delay with maximum capping of 10% of quarterly payments.
	Manpower	Deployment of resources as per CVs and deployment plan submitted as part of Technical Bid	Managed Service Provider (MSP) is permitted to replace up to 20% of the resources per year after written confirmation from the Purchaser.	Penalty at the rate 2 x (rate quoted for the replaced Manpower) per such Manpower replacement beyond 20%
18	ISO 20000, ISO 27001 Certification and SOC-CMM 5 implementation after Go-Live	Implementation of ISO 20000, ISO 27001 and SOC-CMM 5 for DC (NDC, New Delhi) and DR (NDC, Hyderabad)	The MSP has to obtain ISO 20000 and 27001 certifications and implement SOC-CMM 5 for GSOC (New Delhi) and DR (Hyderabad) covered under the contract within twelve months of Go-Live. (Refer paragraph 5.9.7)	INR 15,000 per week of delay with a maximum capping of 10% of the subsequent quarter billed amount. i.e., 10% of the total billed amount of immediate next quarter after completion of 12 months from Go-Live.
19	Sustenance of ISO 20000 & ISO 27001 Certification	Sustenance of ISO 20000, ISO 27001 after the expiry of any certification and	The MSP shall sustain the ISO 20000, ISO 27001 and compliance to SOC-CMM5	INR 15,000 per week of delay after the expiry of the ISO 20000/ISO 27001 certification, with a

	and compliance to SOC-CMM5	compliance to SOC-CMM throughout the period of the contract for DC (NDC, New Delhi) to DR (NDC, Hyderabad)	throughout the period of the contract for GSOC (New Delhi) and DR (Hyderabad) (Refer paragraph 5.9.7)	maximum capping of 10% of the subsequent quarter billed amount. i.e., 10% of the total billed amount of immediate next quarter in which the default occurs.
	Others			
20	Documentation	Submission of documents mention as per paragraph 5.13	Non submission of specified document within the specified timeline as per paragraph 5.13	For each week, or part thereof, of delay in submission beyond the defined timeline as per paragraph 5.8.1, Table 3, 0.5% of every week delay from the Go-Live payment milestone as per paragraph 12.2
21	Training	Training to the purchaser's teams as per section 5.10	Default on conduct of required trainings as per section 5.10	A penalty of 2% of the quarterly payment shall be applied on the quarterly payment of the quarter in which the required training was to be held, with maximum capping of 10% of quarterly payments.
22	Implementation and sustenance of GRC processes and procedures.	Implementation of GRC tool for Primary SOC and DR SOC and furnishing of weekly, monthly reports along with live dashboard.	The MSP shall implement and sustain the GRC processes and procedures through supplied tool and shall furnish weekly, monthly reports along with 24*7 live dashboard throughout the period of the contract for SOC after Go-Live of the GRC. (Refer paragraph 5.12)	INR 2,000 per day of delay in furnishing of reports with a maximum capping of 10% of the subsequent quarterly billed amount i.e., 10% of the total billed amount of immediate next quarter.

6.3.2 Additional Conditions

(a) Each SLA as mentioned above is independent and accordingly the penalties shall be calculated.

(b) Overall penalty for any quarter shall be capped at 10% of the quarterly payment.

(c) For calculation of penalties as percentage of the quarterly payment for Sr. No. 1,2,3,4,4a,9,11,15,16,17,18,19,20 and 21 as per Table 6 above, the quarterly payment shall be taken as: Total cost of manpower during the Qtr. + other miscellaneous expenses payable in the quarter.

(d) For calculation of penalties as percentage of the quarterly payment for Sr. No. 5,6,7,8,10,12,13 and 14 as per Table 6 above, the quarterly payment shall be taken as: Total cost of manpower during the Qtr. + (Yearly cost of AMC of platform and components whose AMC commences in the quarter or is under the AMC)/4 + other miscellaneous expenses payable in the quarter.

(e) If the maximum penalty cap is breached more than 2 times during the entire contract period, then the Purchaser reserves the right to terminate the contract and forfeit the PBG by invoking paragraph 13.21.3 of this RFP i.e., Termination for default/breach.

(f) If at any time during performance of the Work Order/SLA, the MSP encounter conditions impeding timely performance of the above services/SLA, having dependencies of third party (excluding OEMs of the supplied components) or the Purchaser, the MSP shall notify the Purchaser in writing immediately with the reasons of delay, its likely duration, and its cause(s).

(g) Delay for such period as may be caused by any act of the Purchaser, force-majeure or omission of anything required to be done by the Purchaser shall not be taken into account for the purpose of calculating SLA/penalties.

(h) The MSP shall maintain adequate documentation of all delays, incidents, and communications related to SLA breaches to support penalty calculations and dispute resolution.

6.4 Penalty – Product/Platform

TABLE 7: PENALTY ON PRODUCT/PLATFORM DURING IMPLEMENTATION PHASE

S No.	Penalty Definition	Description	Penalty Level in Case of Default
1	Delay in: (a) Complete delivery of software and licenses Hardware as per BoM and Inspection thereof. (b) Installation of complete hardware mounting of hardware in the racks (wherever required) and power-on of the hardware (c) Installation and configuration of software as per BoM for UAT	Any delay in delivery, and deployment of Hardware , Installation and Configuration with reference to timelines defined in paragraph 5.8	0.3% of the total H/W cost as per the Implementation Work Order per day with a maximum capping of 10% of the H/W cost as per the Implementation Work Order
2	Delay in System Integration of all supplied platforms by the MSP as specified in the Contract.	The MSP must ensure Integration of all components with each other as specified in paragraph 5.8	1% of the total one-time cost for Installation, commissioning of all H/W, per day with a maximum capping of 10% of the total one-time cost for Installation, commissioning of all H/W till Go-

			Live as per the Implementation Work Order
3	Delay in UAT and Go-Live	As specified in paragraph 5.8	0.3% of the total value of the implementation work order per day with a maximum capping of 10% of the total value of the implementation work order.

Note:-

1. The overall penalty for product/platform as given in the table above shall be capped at 10% of the total value of the implementation work order. If the maximum penalty cap is breached, then the Purchaser reserves the right to terminate the contract and forfeit the PBG by invoking paragraph 13.21.3 of this RFP i.e. Termination for default/breach.
2. Delay for such period as may be caused by any act of the Purchaser or omission of anything required to be done by the Purchaser or Force Majeure shall not be taken into account for the purpose of calculating the penalty. The MSP must provide written notice to the Purchaser immediately upon recognizing any such cause, specifying cause, estimated duration, and mitigation plans.

7. Invitation of Bids

7.1 The invitation of Bids is for Selection of Managed Service Provider for Setting up, Operating and Managing the Government Cyber Security Operation Centre for NIC, for a period of three years from the date of signing of the Contract, and extendable by up to two years, as per the scope of work defined in Section 5 of this RFP.

7.2 Bidders are advised to study the RFP carefully. Submission of Bid shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications.

7.3 Sealed Bids prepared in accordance with the procedures enumerated in Section 8 Bid Submission of this tender document shall be submitted not later than the date and time laid down at GeM Portal.

7.4 The tender document is not transferable.

7.5 For procedure of submission of Bids refer Section 8 of this RFP.

8. Bid Submission

8.1 Overview

8.1.1 The Bidder must strictly adhere to the timelines and deadlines specified on the GeM portal. Bids submitted after the specified deadline will be summarily rejected and will not be considered under any circumstances.

8.1.2 Bids **submitted online only through the GeM portal** shall be accepted and considered for the bid processing. Any Bid submitted through other means (physical, email, etc.) shall be rejected.

8.1.3 Bids that are incomplete, ambiguous, conditional, or non-compliant with the instructions laid out in this RFP shall be rejected without any further correspondence or opportunity for correction.

8.1.4 Bidders are advised to ensure completeness and accuracy of all submitted documents and attachments.

8.1.5 Bidders shall ensure that all uploaded documents are clear, legible, and in the prescribed formats. Any ambiguity or unreadable document may lead to rejection of the Bid.

8.1.6 Bidders shall be solely responsible for ensuring the successful submission of their Bid on the GeM portal. The Purchaser will not be responsible for any technical failures or issues faced during submission.

8.2 Language of Bid

8.2.1 The Bid prepared by the Bidder and all correspondence and documents relating to the Bid exchanged by the Bidder and the Purchaser, shall be written in English language.

8.3 Earnest Money Deposit

8.3.1 Earnest Money Deposit (EMD) must be submitted in the form of Bank Guarantee drawn in favour of National Informatics Centre, payable at New Delhi on or before the last date of bid submission and shall be valid for Bid validity period as specified in factsheet from last date of submission of Bids. For the successful Bidder i.e., the MSP, the EMD shall remain valid until the PBG (against the first WO issued by the Purchaser) is furnished by the MSP and the same is accepted by the Purchaser. In such case, the successful Bidder i.e., MSP shall extend the validity of the EMD for a period till the PBG is submitted and the same is accepted by the Purchaser. Upon the successful award of the contract, the EMD shall be returned to the successful bidder after 30 days of submission of Performance Bank Guarantee (PBG).

8.3.2 In case the EMD is not submitted by the bidder, the bid shall be summarily rejected.

8.3.3 The Earnest Money Deposit (EMD) shall be refunded without any interest accrued.

8.3.4 The Bidder has to select the payment option as “offline” to pay EMD as applicable and enter details of the instrument.

8.3.5 The Bidder shall seal the original Bank Guarantee in an envelope. The address of NIC, name and address of the Bidder and the Tender Reference Number shall be marked on the envelope.

8.3.6 The Bidder shall deposit the envelope at GeM Section, NIC HQ. on or before the Bid submission date as per the Tender Notice.

8.3.7 Bids submitted without the EMD or with an invalid/expired Bank Guarantee shall be rejected.

8.3.8 The Purchaser reserves the right to forfeit the EMD of the Bidder in case of any defaults by the bidder during the bid processing.

8.3.9 The EMD shall be forfeited in case:

a) If the bid is withdrawn during the validity period or any extension thereof agreed to by the bidder.
b) If the successful bidder fails to execute the contract or defaults on any of its obligations.
c) If the successful bidder fails to sign the contract and submit Performance Bank Guarantee within the stipulated period.
d) If the bid is varied or modified in a manner not acceptable to Purchaser after opening of the bid during the validity period or any extension thereof.
e) If the Bidder attempts to influence the evaluation process.
f) Any other reason found fit for forfeiture by the Purchaser.

8.3.10 In the event of any discrepancy or disagreement regarding the forfeiture or release of the EMD, the decision of Purchaser shall be final and binding.

8.4 Online Bid Submission

8.4.1 Online Bids (complete in all respect) must be uploaded on GeM portal as per the schedule.

8.4.2 No Bids shall be accepted post the deadline as specified in this schedule. Bids submitted online, shall only be considered for the tender opening process and further evaluation.

8.4.3 The online Bids shall be submitted as under along with the documents specified below:

TABLE 8: DETAILS OF BID SUBMISSION STAGES

Bid Type Stage Number	Documents to be uploaded	File Format
Stage- 1 (Technical Bid)	The file shall be saved and uploaded in a PDF file as "Stage 1_<Bidder Name>".pdf (a) Scanned copy of Covering Letter in Company Letter Head as per **Annex 9: Covering Letter for Bid** duly sealed & signed (PDF) (b) Scanned copy of **Original Power of Attorney letter** in a Non-Judicial Stamp Paper of at-least Rs. 100/- OR (c) **Board Resolution** in Letter Head in original in case of Registered Limited Companies OR **Original Authorization in Letter** Head in case of Partnership Firm OR **Original Self Certificate in Letter Head** in case of Proprietorship naming/indicating the person authorised to sign the Bid (PDF). (d) Scanned copy of duly filled signed and stamped **Section 15: Technical Specifications** of the tender document. Any deviation from the tendered specifications (except where the deviation is on account of being better specifications being offered by the Bidder) may make the Bid unresponsive. (e) Scan copy of duly filled signed and stamped **paragraph 10.1 Pre-Qualification Criteria** and all the supporting/mandated documents and Annexures required for eligibility criteria. (f) All the supporting documents as per paragraph **10.2.10 Technical Evaluation Criteria: Table 10: Technical Evaluation Criteria**. (g) Duly filled signed and stamped **Annex 1: Arrangement with Sub-contractors/Service Providers.** (h) Scan copy of duly filled (Without Cost for all items) signed and stamped **Unpriced Bill of Material** as per **Annex 5: Bill of Materials (BoM)** (without cost for	PDF

	all items) and technical solution along with detailed unpriced BOM with Model number, OEM and architecture diagram. (i) Duly filled signed and stamped copy of MAF and undertaking form from respective OEMs as per **Annex 8: Manufacturing Authorization Form (MAF) and Annex 11: Undertaking to be submitted by OEM.** (j) A copy of Malicious Code Certificate as per **Annex 13** Duly filled signed and stamped by the Bidder and respective OEM for all the supplied components shall be submitted. (k) A signed copy of the Integrity Pact as per the format given at Annex 12: Format for Integrity Pact. *Note: The PDF file shall not contain any details regarding the financial Bid in the explicit/implicit form and may lead to rejection of the Bid.*	
Stage-2 (Financial Bid)	Financial Bids to be uploaded as: - (l) As per BOQ: GTV Financial Bid as per **Annex 3: Abridged Financial Bid** (m) Detailed financial Bid as per **Annex 4: Detailed Financial Bid** and **Annex 5: Bill of Material (BoM)** (in .pdf format). The Detailed Financial Bid scanned pdf files, then shall be saved in a RAR 'Detailed Fin<Bidder's Name>".RAR ***Note:*** i. *Soft copy of* Annex 3**,** Annex 4 & Annex 5 *in.zip format (or as per GeM Portal provisions)* ii. *All the Bid documents duly signed by the authorised signatory of the company and stamped with company seal*	.zip

8.5 Instructions for technical Bid submission

8.5.1 All the Bid documents must be duly signed by the authorised signatory of the company and stamped with company seal.

8.5.2 It shall be the sole responsibility of the Bidder to check (and double-check) the page number referencing made for supporting documents in the checklist indicated under Pre-Qualification compliance and Technical Compliance Sheet. No relevant information/document shall be omitted/left out, whether listed above explicitly or not.

8.5.3 All pages of the Bid being submitted shall be sequentially numbered by the Bidder.

8.5.4 Relevant referencing shall be done by the Bidder, clearly indicating all page numbers where supporting documents are provided.

8.5.5 The Bid document shall include a comprehensive Table of Contents/Index showing page numbers for all supporting documents. Each page of the Bid must be sequentially numbered, stamped, and signed by the authorised signatory.

8.6 Instructions for financial Bid submission

8.6.1 The Bidder must upload the BOQ as per the format provided on GeM portal. The Bidder must adhere to terms and conditions and fill in the required details as required in BOQ.

8.6.2 The Bidder must strictly follow the prescribed format as specified in the detailed Financial Bids.

8.6.3 The Bidder shall quote only the Gross Total Value (GTV) in Abridged Financial Bid as derived from in Detailed Financial Bid.

8.6.4 During financial opening, only the Grand Total Value quoted by the Bidder on the GeM portal shall be considered for determining the LQ1 Bidder based on the GTV value.

8.6.5 All the Bid documents shall be duly signed by the authorised signatory of the company and stamped with company seal.

8.7 General instructions for Bid submission

8.7.1 OEMs of the proposed solutions must submit an undertaking as per attached annexure (**Refer Annex 11**).

8.7.2 The Bids submitted by Fax/E-mail etc. shall not be considered. No correspondence shall be entertained on this matter.

8.7.3 Conditional Bids shall not be accepted on any ground and shall be rejected straightway. (A Bid is conditional when Bidder submits its Bid with his own conditions & stipulations extraneous to the terms and conditions specified in this tender)

8.7.4 No Bids shall be accepted after the expiry of the deadline under any circumstances.

8.7.5 In case, the last day of Bid submission is declared Holiday by Govt. of India, the next working day shall be treated as the last day for submission of Bids. There shall be no change in the timings.

8.7.6 All pages of the Bid being submitted shall be signed by the authorised signatory, stamped and sequentially numbered by the Bidder irrespective of the nature of content of the documents.

8.7.7 At any time prior to the last date for receipt of Bids, Purchaser, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the Tender Document by publishing an amendment/corrigendum. The amendment shall be notified on GeM portal and shall be taken into consideration by the prospective agencies while preparing their Bids. It is the sole responsibility of the Bidder to check website for any such notice/changes and submit its Bid accordingly.

8.7.8 In order to give prospective agencies reasonable time to take the amendment into account in preparing their Bids, Purchaser may, at its discretion, extend the last date for the receipt of Bids. No Bid may be modified subsequent to the last date for receipt of Bids. No Bid may be withdrawn in the interval between the last date for receipt of Bids and the expiry of the Bid validity period specified in the tender. Withdrawal of a Bid during this interval may result in forfeiture of the EMD by the purchaser.

8.7.9 Printed terms and conditions of the Bidders shall not under any circumstances be considered as forming part of their Bid. The terms and conditions of this tender shall always overrule the printed terms and conditions submitted by the Bidder.

8.7.10 Bidder shall not upload any additional document other than that asked in the tender. Any additional documents uploaded shall not be considered for evaluation.

8.7.11 Bids not submitted as per the specified format and nomenclature may be rejected. The terms and conditions of this tender shall overrule/supersede the standard terms and conditions of the GeM portal, if any.

8.7.12 Ambiguous/Incomplete/Illegible Bids may be rejected. Not quoted Bids shall be considered as non-responsive and may be rejected.

8.7.13 Any alteration/ overwriting/ cutting in the Bid shall be duly countersigned.

8.7.14 Submission of the Bid shall be deemed to have been done only after careful study, examination and understanding of all instructions, eligibility norms, terms and required specifications in the tender document with full understanding of its implications. Failure to furnish all information required in the tender Document or submission of a Bid not substantially responsive to the tender document in all respects shall be at the Bidder's risk and may result in the rejection of the Bid.

8.7.15 Tender process shall be over after the issuance of contract letter to the MSP.

8.7.16 For additional instructions, refer Section 8.

8.7.17 Submission of false, forged, or misleading documents shall lead to immediate forfeiture of the EMD, blacklisting of the Bidder for a minimum period of 3 years, and legal action as deemed necessary by the Purchaser.

8.8 Assistance to Bidders

8.8.1 Any queries relating to the tender document and the terms and conditions contained therein shall be addressed exclusively to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender. No other channel shall be entertained.

8.8.2 Any queries relating to the process of online Bid submission or queries relating to GeM portal in general may be directed to GeM section of NIC.

8.8.3 Financial Prices shall not be indicated in the Technical Bid. Any Bid found violating this condition shall be immediately disqualified and rejected without any further communication.

8.9 Address of correspondence of the Bidder

8.9.1 The Bidder shall designate and provide an official mailing address, place, email address, phone number, and fax number to which all correspondence from the Purchaser shall be sent. It is the Bidder's responsibility to ensure these contact details are accurate and kept up to date throughout the tender and contract period.

8.10 Period of Validity of Contract/Agreement

8.10.1 The Contract shall be signed between Purchaser and successful Bidder based on terms and conditions of the Bid within 15 working days from the date of on which the letter of acceptance from the Purchaser is received, unless the Purchaser informs otherwise. The period of validity of the agreement shall be three years and extension of two more years (if any).

8.10.2 If it is considered necessary for the continuance of operation of SOC by the Purchaser, the MSP shall be required to continue delivering services as required under this Project, on the same terms and conditions or additional mutually agreeable conditions, even beyond the contract period (such period may be extended up to two more years by way of one or more extensions) till an alternate arrangement is made by the Purchaser to manage the operations.

8.11 Cost of Bid

8.11.1 The Bidder shall bear all costs associated with the preparation and submission of its Bid, including cost of presentation for the purposes of clarification of the Bid, if so desired by the Purchaser. The Purchaser shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the Tendering process.

8.12 Influencing the Purchaser

8.12.1 Any effort by a Bidder to influence the Purchaser's Bid evaluation, Bid comparison or contract award decisions may result in the rejection of the Bidder's Bid.

8.13 Purchaser Clarification

8.13.1 When deemed necessary, as part of Technical and financial Evaluation, during the tendering process, the Purchaser reserves the right to seek clarifications or ask the Bidders to make presentations/ clarifications on any aspect from any or all the Bidders.

8.14 Bidder's Clarification on Tender Document

8.14.1 Bidders requiring any clarification on the Tender Document may submit their queries, exclusively on GeM portal. Queries submitted through any other channel shall not be considered.

8.14.2 All queries on the Tender Document in a prescribed format shall be received on or before as prescribed by the Purchaser in **Section 1: Summary Sheet** of this tender document. Purchaser's response (including the query but without identifying the source of inquiry) would be uploaded in the GeM portal. Bidders are responsible for duly checking the website for any clarifications. The Purchaser shall not respond to any queries not adhering to the above-mentioned format.

8.15 Amendment of Tender Document

8.15.1 At any time prior to the last date for receipt of Bids, the Purchaser, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the Tender Document by an amendment. The amendment shall be notified on GeM portal and shall be taken into consideration by the prospective agencies while preparing their Bids.

8.15.2 In order to provide prospective Bidders reasonable time in which to take the amendment into account in preparing their Bids, the Purchaser may, at its discretion, extend the last date for the submission of Bids.

8.15.3 Purchaser at any time during the tendering process reserves the right to request all the prospective Bidders to submit revised Technical/ Financial Bids and/or Supplementary financial Bids without thereby incurring any liability to the affected Bidder or Bidders.

8.16 Price Stability

8.16.1 The prices quoted by the Bidder shall remain firm and fixed, without any escalation or revision for whatsoever reasons, till the completion of contract period including the extension period (if any).

8.17 Revelation of Prices

8.17.1 Prices in any form or by any reason before opening the Financial Bid shall not be revealed, failing which the bid shall be liable to be rejected.

8.17.2

8.18 Sub-Contract

8.18.1 MSP may appoint a subcontractor for execution under this contract only for the following:

(a) Maintenance and installation of MSP supplied ICT infrastructure;
(b) Training, Support and Documentation.
(c) Laying of inter building fiber cable.
(d) Installation and configuration of active components of GSOC LAN.

8.18.2 The MSP may do subcontracting as per 8.18.1; however, MSP shall ensure that there is only one level of subcontracting during entire contract period. No further subcontracting by the first level subcontractor shall be permitted.

8.18.3 MSP may appoint independent third parties selected by the purchaser or with the prior approval of the purchaser for the following:

(a) Conducting of ISO certifications assessment;
(b) Third party audits;

Subcontracting for any other component of the SOC shall be on the basis of mutual agreement during the contract between the Purchaser and the MSP as per terms and conditions defined by the Purchaser.

8.18.4 The subcontracting details and documents supporting the same shall be submitted as a part of Technical Bid as per Annex 1.

8.18.5 In case of addition of a new or replacement of an existing sub-contractor, prior approval of the Purchaser shall be sought by filling in details in the form provided in Annex 1 along with supporting documents. No new subcontracting work shall commence without such approval.

8.18.6 The MSP shall be solely responsible for performance of all obligations under the tender document irrespective of the failure or inability of the subcontractor chosen by the MSP to perform its obligations. The MSP shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits for its employees and sub-contractors, ensuring no liability to the Purchaser.

8.18.7 The MSP shall be held responsible and accountable for any non- performance or breach or SLA violations by the sub-contractor. MSP shall be liable for any resulting penalties

8.18.8 The MSP indemnifies and shall keep the Purchaser indemnified against any losses, damages, claims, liabilities, costs, or other consequences arising directly or indirectly from acts, omissions, negligence, breach, or misconduct by the subcontractor or its personnel.

9. Bid Opening

9.1 A technical evaluation committee (TEC) shall be formed for opening and evaluation of the technical Bids. Decision of the TEC shall be final and binding upon all the Bidders.

9.2 A financial evaluation committee (FEC) shall be formed for opening and evaluation of the financial Bids.

9.3 GeM Section of the Purchaser shall download the Bids from GeM portal.

9.4 The Bids shall then be passed on to the duly constituted Technical Evaluation Committee (TEC).

9.5 The TEC shall open the technical Bids and shall evaluate the technical Bids as per **paragraph 10.2.**

9.6 Financial Bids of only those Bidders whose Bids are found qualified by the Technical Evaluation Committee (TEC) as per both Pre-Qualification (PQ) & Technical Qualification (TQ) criteria shall be opened for further evaluation on a notified date and time.

9.7 The financial Bids shall then be passed on to the duly constituted Financial Evaluation Committee (FEC) for evaluation, which shall evaluate the technically qualified Bids as per **Section 10**.

10. Evaluation of Bid

10.1 Stage 1 – Pre-qualification

10.1.1 Purchaser shall validate the “Earnest Money Deposit (EMD)”) submitted by the Bidder to ensure compliance with the tender requirements.

10.1.2 If the EMD is found valid, Purchaser shall assess the documents pertaining to the "Pre-Qualification Criteria". It is mandatory to fulfil each of the conditions stated in the Qualification Criteria. If the Bidder fails to satisfy any of the conditions, Purchaser reserves the right to disqualify the Bidder.

10.1.3 Documentary evidence supporting compliance with each pre-qualification criterion must be enclosed along with the Bid, together with references as required.

10.1.4 Relevant portions, in the documents submitted in pursuance of eligibility criterion specified above, shall be highlighted and all pages of the Bid document shall be serially numbered for easy reference.

10.1.5 Undertaking for subsequent submission of any of the above document shall not be entertained under any circumstances. However, Purchaser reserves the right to seek required/additional documents and/or seek clarifications on the already submitted documents.

10.1.6 All documents shall be submitted electronically in PDF format.

10.1.7 **Pre-Qualification Criteria:**

TABLE 9: PRE-QUALIFICATION CRITERIA

Sr. No.	Criteria	Documents to be Provided	Compliance (Yes/No/NA)
1	**Legal Entity:** The Bidder must be incorporated and registered in India under the Indian Companies Act 1956/2013 LLP Act 2008 / Partnership Act 1932 & subsequent amendments thereto and shall have been operating for the last five years as on 31st March 2025 (including name change/ impact of mergers or acquisitions).	Valid documentary proof of: i. Certificate of incorporation / Certificate of Commencement ii. Certificate consequent to change of name if applicable. iii. Copy of Memorandum of Association (if applicable) (In addition, the Bidder shall also submit last 5 Audited balance sheets.)	
2	**Presence in India:** The Bidder should have a permanent office in India as on bid publishing date.	i. Self-Declaration from the Authorised Signatory	
3	**Land Border Sharing:** Any Bidder from a country which shares a land border with India will be eligible to bid in this bid only if the Bidder is registered with the Competent Authority (i.e., Registration Committee constituted by Department for Promotion of Industry and Internal Trade (DPIIT)). Refer paragraph 13.28.1 of the bid.	i. Declaration by the Bidder on their letter head that the Bidder has proposed no such Solution in response to the bid.	
4	**Identity Proof:** The Bidder must have a registered number of: • GST Registration. • Income Tax / PAN / TAN.	i. Certificate of GST registration. ii. Copy of PAN / TAN / Income tax number.	
5	**Financial Net Worth:** The Bidder must have positive net worth during any three consecutive financial years, out of the following: a) 2021-22 b) 2022-23 c) 2023-24 d) 2024-25 and also, the net worth of the bidder should not have been eroded by	**The latest three** Audited Balance Sheets for **consecutive financial years** out of the following: a) 2021-22 b) 2022-23 c) 2023-24 d) 2024-25 where financial turnover is segregated. Every sheet shall be duly certified by	

	more than 30% (thirty percent) in the last three financial years.	a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for the three financial years.	
6	**Project Experience (Financial):** The Bidder must have implemented and maintained (completed/ in process) at least 3 projects of setting up the SOC for Govt./Private sector clients in last 5 financial years. The value of the projects must be at least 50 crore or more in total with at least 1 project of minimum Rs. 20 Cr. The projects may include dedicated on-premises/cloud SOC for an organisation or managed service offering of SOC as a service.	Copy of: i. Letter of Award (LOA) or ii. Purchase Order (PO) or iii. Work Order (WO) or iv. Contract or v. Agreement, containing: Scope of Work (SOW) and Order Value or Certification of Acceptance for ongoing projects/ Completion certificate for completed projects by client. (The WO/ letter shall be in the name of the Bidder and clearly mention the scope of work.)	
7	**Project experience (Sizing):** The Bidder must have at least 1, SOC deployment (completed/in process of implementation) with a scale of 500TB (Per Year) or more capacity and / or 50000 Event Per Second (EPS) of Log ingestion/Data Analytics and Management platform.	Copy of: i. Letter of Award (LOA); or ii. Purchase Order (PO); or iii. Work Order (WO); or iv. Contract; or v. Agreement, containing: Scope of Work (SOW) and Order Value; or Certification of Acceptance for ongoing projects/ Completion certificate for completed projects by client. (The WO/ letter shall be in the name of the Bidder and clearly mention the scope of work.)	
8	**Authorisation:** Authorization of signatory for the purpose of this tender	Letter of Authorization/Power of Attorney/Board Resolution	
9	**Resource deployment:** The Bidder shall give declaration	Undertaking to this effect shall be submitted by the Bidder on their	

	stating that the resources deployed under this project shall be dedicated for this project (not deployed for other projects/ internal activities) and reporting to Government during the entire project	letter head by the authorised signatory	
10	**Financial Turnover:** The Bidder must have an annual turnover of at least **INR 750** crore each year for any of the three consecutive financial years, out of the following: a) 2021-22 b) 2022-23 c) 2023-24 d) 2024-25 for which audited annual financial statements are available.	Audited annual financial statements for any of the three consecutive financial years, out of the following: a) 2021-22 b) 2022-23 c) 2023-24 d) 2024-25 for which such audited statements are available.	
11	**Certifications:** The Bidder shall submit certification for ISO 9001:2015 and any two of the following: (a) ISO 27001:2013 (b) ISO 20000:2018 (c) ISO 22301 (d) CMMi3 or CMMi4 or CMMi5	Copy of certificates to be submitted.	
12	**OEM Authorization Certificate:** Bidder shall provide valid OEM Authorization Certificates for all the products quoted as well as certify that the proposed product is not declared end of sale.	Copy of MAF certificate for all solution proposed as part of Bid submission as per Annex 8	
13	**Malicious Code Certificate:** Duly filled signed and stamped Malicious Code Certificate as per Annex 13 shall be submitted by the Bidder and respective OEM(s) for all the supplied components.	Copy of Malicious Code Certificate as per Annex 13	
14	**DPDP Act:** Bidder to submit an undertaking that states as follows- "We hereby undertake to comply with DPDP Act for the deployed solution (as part of this Bid) within	Undertaking from Bidder by the Authorised Signatory.	

	six months from the date of Go-Live or the implementation duration given post its announcement, whichever is earlier".		
15	**OEM Support:** Bidder shall provide back-to-back support from OEM for a period of contract i.e Three years from the date of Go- Live and any extension period.	Undertaking from Bidder as per Annex 11	
16	**Manpower Resources:** The Bidder must have at least 100 (twenty-five) full time technical support professionals on its permanent roll in India and preferably at least 25 (ten) full time technical support professionals in Delhi/NCR (as on 31st March, 2025) who have relevant skill, competency/Certification in OEMs proposed solutions.	Certificate from the statutory auditor/a practicing Chartered Accountant/Company Secretary regarding such EPF-enrolled employees, along with a list of such employees.	
17	**Non-Blacklisting Undertaking:** The Bidder must not be blacklisted by Central /State Government Ministry/ Department/ PSU/ Government Company. Bidder also must not be under any litigation/legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry / Department/ PSU/ Government Company. The bidder must not have faced any contract terminations, in the last 3 years with any Indian Central/ State Government Ministry / Department/ PSU/ Government Company.	Self-certification duly signed by authorised signatory on Bidder's firm letter head.	

10.2 Stage 2 – Technical Evaluation

10.2.1 Only those Bidders who qualify all Pre-Qualification (PQ) Criteria requirements shall be qualified for technical Bid evaluation.

10.2.2 Technical presentation/demonstration shall be a part of the process for evaluation of the Bids.

10.2.3 The TEC reserves the right to reject a Product/ Service if it is of an opinion that the offered product/ service does not match the technical requirements/ objectives specified in Technical Bid – Purchaser's Requirements

10.2.4 Bidders shall submit the technical specification compliance sheet as a part of technical Bid as specified in Section 15: Technical Specifications of the tender document.

10.2.5 **Bidder shall submit unpriced Bill of Material along with technical Bid as per Annex-5. i.e. Annex-5 filled with all details except price/costing details.**

10.2.6 Bidder shall provide references to the relevant documents/datasheets for each technical compliance wherever required.

10.2.7 The TEC will assign a technical score to each Bidder based on the Technical Evaluation Criteria outlined in paragraph 10.2.

10.2.8 Technical Bids receiving a score greater than or equal to a cut-off score of 65 out of 100 shall be eligible for consideration in the subsequent rounds. If required, the Purchaser may seek clarifications from any or all Bidder(s) at this stage. The Purchaser would determine the Bidders that qualify for the next phase after reviewing the clarifications provided by the Bidder(s).

10.2.9 In cases where the Manufacturing Authorization Form (MAF) deviates from the prescribed RFP format, the TEC reserves the right to accept such deviations or seek clarifications as considered appropriate.

10.2.10 **Technical Evaluation Criteria:**

TABLE 10: TECHNICAL EVALUATION CRITERIA

S. No.	Criteria	Scoring criteria	Required Documents / Basis of Evaluation	Total Marks	Qualifying Marks
1	Project Plan and adherence to Project Timelines	Detailed Project Plan adhering to Project Timelines: **5 marks**	Proposed Project plan	5	2
2	Resource Quality and Management	**i.** Location-wise Manpower deployment plan: **5 Marks** ii. Qualification, Skillset, experience of proposed resources: **5 marks** iii. Relevant security certification: **5 marks**	i. Deployment plan and CVs of Proposed Manpower mentioned below: • Project Manager (1), • Security Breach Investigation Specialist (3), • Log Analysis & Threat Hunting Specialist (3), • SIEM Administrator (3), • SOAR Administrator (3),	15	10

			• Forensic Experts (3) ii. Proof of relevant certification as asked under the skill set requirement of proposed Manpower in section 16 table 17.		
3	Technology Stack	i. Proposed Technology Stack for platforms in compliance to technical specification: **6 marks** **ii.** Specifications of Proposed Supporting component (Hardware appliances / software platforms/ solutions etc.) : **6 marks** iii. Value added features provided in proposed solution in addition to technical specification: **3 marks**	i. Technology Stack, features, functionalities, as per un-priced BoM as per Annex 5 ii. Data Sheets/ reference documentation of proposed platform and components iii. Supporting documentation for value added features, specifications of supporting components to be submitted as part of the bid document.	15	10
4	Solution Design & Architecture and Project Governance	i. Overall solution architecture design: **8 marks** ii. Total rack space (in U) and power requirement (in KW) for all proposed components as per BoM: **6 Marks** (Calculation of these marks shall be on	i. Proposed High Level Design, Architecture, process flow, integration ii. Proposed implementation strategy as per quoted number of racks and power. iii. Implementation plan including Approach and Methodology iv. Plan showcasing	40	30

		percentile basis from across all bidders who are eligible for the technical presentation.) iii. Approach for Implementation of proposed platform and components: **12 marks** iv. Approach to meet the SLAs: **6 marks** v. Project Governance structure and escalation matrix: **3 marks** vi. Exit Management Plan: **3 Marks** vii. Additional marks will be given to be Bidders who do not opt for subcontracting for any of the services/manpower under this RFP : **2 Marks**	methodology to meet the SLAs v. Bidder's Project Governance structure and escalation matrix vi. Exit Management Plan vii. Subcontracting details.		
5	Technical Presentation & Demonstration (Purchaser reserves the right to seek a demo on any of the proposed solutions.)	i. Overall solution design and Architecture: **4 marks** ii. Demonstration of Key features: **4 marks** iii. Response to queries raised by TEC: **2 marks**	Technical Presentation and Demonstration based on Design and Architecture, Response to queries raised by TEC	10	6
6	Evidence demonstrating that the Bidder has been involved in	i. Project value of minimum Rs. 50Cr. = **3 Marks** ii. Apart from above clause, additional	Submit relevant certified documents i.e., Work Order/signed contract /user certification or Certificate by the a	5	3

	providing Security Operations Centre Services including Incident Response / Cyber Forensic Services	marks will be given if the Bidder submits projects of value exceeding Rs. 50 Crore, **(Max. 2 Marks)**	practicing Chartered Accountant/ Company Secretary of the Bidder indicating the scope of work, in case of projects are under non-disclosure agreement and confidentiality		
7	The Bidder must have at least 1 deployment (completed/in process of implementation) with a scale of 500TB (Per Year) or more capacity and / or 50000 Event Per Second (EPS) of Log ingestion/Data Analytics and Management platform.	**i.** One project of more than 500TB (Per Year) capacity and/or more than 50000 EPS shall qualify for **Max. 4 marks.** ii Additional projects of more than 500TB (Per Year) capacity or more than 50000 EPS shall qualify for additional marks **(Max. 6 marks)**	Submit relevant certified documents i.e., Work Order/signed contract/ Letter of Award (LOA)/ Customer Certification. (Archival and backup solutions shall not be considered)	10	4
	Total			**100**	**65**

ST = Each Technical Proposal shall be assigned a Technical Score (ST). The **highest technical proposal (HT)** shall be given a Technical Score (ST) of 100 points based on technical evaluation by TEC. The technical scores of other proposals shall be computed as follows.
ST = 100xT/HT, where T= marks obtained for Technical Proposal in Technical Evaluation

Note:

1. Supporting documentation for value added features, specifications and sizing of supporting components and CVs of Proposed Manpower as mentioned in the table above, are to be submitted as part of the bid document.

10.3 Stage 3 – Evaluation of Financial Bids (Selection of LQ1 Bidder)

10.3.1 Financial Bids submitted by only those Bidders, who have qualified the Pre-Qualification criteria and technical evaluation shall be eligible for further evaluation.
10.3.2 The Financial Bids of only those Bidders short listed from the Technical Bids by TEC shall be opened electronically in the presence of their representatives on a specified date and time to be intimated to the

respective Bidders by GeM Section of NIC, and the same shall be evaluated by a duly constituted Finance Evaluation Committee (FEC).

10.3.3 SF = Each Financial Proposal shall be assigned a financial score (SF). The lowest financial proposal (FM) shall be given a financial score (SF) of 100 points. The financial scores of other proposals shall be computed as follows:

SF = 100 x FM/LQx (1,2,3…), where LQx = Amount of Financial Proposal (GTV)

TABLE 11: CRITERIA FOR DECIDING LQ1 BIDDER

Criteria for deciding LQ1 Bidder	The **Lowest Quoting Bidder (LQ1)** shall be determined as specified below and shall be given a financial score of 100
	1) Grand Total Value quoted by the Bidder on the GeM platform shall be considered for all the technically qualified Bidders on a specified date.
	2) **LQ1, LQ2, LQ3……** Bidders shall be decided on the Gross Total Value (GTV) of this Annexure i.e., Annex 3 (Abridged Financial Bid).
	Thus, the LQ1 Bidder shall be decided as per the above-mentioned procedure. **NOTE:** 1. In case of any mismatch in the GTV quoted in Annex 3 and the Grand Total Value provided by the Bidder on the GeM Portal, the discrepancy between these two values shall be removed as per para 10.4.3. 2. The next subsequent low quoting Bidder shall be selected if the low quoting Bidder withdraws or gets rejected due to any reason(s).

10.4 Stage 4 – Final Bid Evaluation (Selection of Final Bidder)

10.4.1 The evaluation of the tender shall be based on QCBS (Quality and Cost based Selection).

10.4.2 Thereafter, Combined and Final evaluation shall be done on the following basis:

(a) Proposals shall finally be ranked according to their combined Final Score (FS) based on their Score technical (ST) and financial (SF) scores as follows:

FS (Final Bidder) = ST x 0.7 + SF x0.3

(a) The MSP shall be the first ranked Bidder having the highest combined Final Score (FS). The Combined Final Score contains 70% weightage for technical evaluation and 30% weightage for financial evaluation. The subsequent Bidder shall be the second ranked Bidder and so on.

(b) The detailed financial Bid (Annex 4) shall be opened only for the MSP having highest combined final score.

(c) The first ranked Bidder shall be selected as the final Bidder (L1) only when there is no discrepancy in the detailed financial Bid. In case of any deviations/ discrepancy, the Purchaser reserves the right to disqualify the first ranked Bidder and select the subsequent second ranked Bidder as per the process specified above and so on until a Bidder is identified with no deviations and discrepancies.

10.4.3 Further, in the event of any mismatch in the GTV value provided at Annex 3 (Abridged Financial Bid) and GTV of Annex 4 (Detailed Financial Bid) of the Bid, the following criteria shall be adopted to remove the discrepancy between these two values:

(a) When Grand Total Value given in Annex 3 (Abridged Financial Bid) is greater than the Grand Total Value given in Annex 4 (Detailed Financial Bid), the value given in Annex 4 (Detailed Financial Bid) shall be taken as the final quoted value by the Bidder and the same shall be accepted by the bidder, before signing of the contract. In case, the bidder does not accept the revised value, the Purchaser reserves the right to reject the bid and forfeit the EMD.

(b) When Grand Total Value given in Annex 3 (Abridged Financial Bid) is less than the Grand Total Value given in Annex 4 (Detailed Financial Bid). The value given in Annex 4 (Detailed Financial Bid) shall be replaced with the value given Annex 3 (Abridged Financial Bid) and the item-wise value for each item in Annex 5 (Bill of Material) shall be reduced on Pro-Rata basis and consequently unit values shall be worked out. The AMC rates shall be calculated at the same percentage as quoted by the bidder (Condition mentioned at **para d of 5A at Annex 5** shall apply) and the same shall be accepted by the bidder, before signing of the contract. In case, the bidder does not accept the revised value, the Purchaser reserves the right to reject the bid and forfeit the EMD.

10.4.4 If only single Bid is submitted, Purchaser reserves the right to proceed with the evaluation of the Bid.

10.4.5 If there is only one qualified Bid Purchaser reserves the right to process the single Bid and negotiate with the Bidder on reasonable pricing if required.

10.4.6 Any decision taken by NIC, or the evaluation committees shall be final and binding on the Bidders. All the Bidders are required to agree to this clause and must sign an undertaking/covering letter accepting this clause without any conditions (Refer Annex. 9).

10.5 Consideration of Abnormally Low Bids

10.5.1 An Abnormally Low Bid is one in which the GTV, or any of its components, appears so low that it raises substantive concerns as to the Bidder's capability to perform the contract at the offered price. The Purchaser may in such cases seek written clarifications and supporting documents from the Bidder, including detailed price analyses of its GTV, and/or any of its components, concerning scope, schedule, allocation of risks and responsibilities, and any other requirements of the RFP. The Bidder shall provide the requested information within the stipulated time frame, failing which the Bid can be rejected without further consideration. If, after evaluating the price analysis, the Purchaser determines that Bidder has substantively failed to demonstrate its capability to deliver the contract at the offered price, the Purchaser may reject the Bid, and evaluation may proceed with the subsequent second ranked Bidder and so on.

10.5.2 If the Total Cost of Manpower (Refer Annex 5, Table - 6) in a bid is considered not in line with the industry standards with respect to the skillset asked by the Purchaser, thereby raising concerns about the bidder’s ability to provide the manpower with the required skillsets and experience, the Purchaser may reject the Bid, and evaluation may proceed with the subsequent second ranked Bidder and so on.

10.6 Reasonability of Prices Received

10.6.1 The Purchaser shall evaluate whether the GTV, and/or any of its components mentioned in Annex 5 (Bill of Materials), received as part of the Bid are reasonable. If the prices received are considered abnormally low or unreasonably high, the Purchaser reserves its right to take action as per paragraph 10.5, or reject any or all Bids, or abandon/ cancel the Tender process and issue another tender for identical or similar Services.

11. Contract

11.1 Contract Process

11.1.1 The Managed Service Provider (MSP) shall be required to unconditionally agree to and honour all tender terms and conditions, Service Level Agreements (SLAs), and the full scope of work laid down in this RFP, throughout the execution of all Work Orders issued by the Purchaser.

11.1.2 Purchaser reserves the right to cancel this tender or modify the requirement, at any stage of Tendering process.

11.1.3 Purchaser also reserves the right to modify/relax any of the terms & conditions of the tender by declaring / publishing such amendments in a manner that all prospective vendors / parties to be kept informed about it.

11.1.4 Purchaser, without assigning any further reason can reject any tender(s), in which any prescribed condition(s) is/are found incomplete in any respect and at any processing state.

11.2 Award of Contract

11.2.1 The Bidder achieving the highest Total Score in QCBS evaluation shall be awarded the contract. In case of a tie, where two or more Bidders achieve the same highest Total Score, the Bidder with the higher Technical Score shall be awarded the contract.

11.2.2 The acceptance of the tender shall be intimated to the successful Bidder by Purchaser/ through a letter/email. Purchaser would be the sole judge in the matter of award of contract and the decision of Purchaser shall be final and binding.

11.2.3 The selected bidder shall sign the Contract as per tender terms and conditions with Purchaser within 15 working days of award of contract or such other extended time period as approved by the Purchaser in writing or else the Purchaser reserves the right to cancel the award of contract and forfeit the EMD.

11.2.4 Period of the contract shall be Three years of operational phase from the date of signing of contract + the implementation phase and shall be extendable by another two years of operational phase. Work Order shall be issued on yearly basis (or as deemed appropriate by the Purchaser).

11.3 Scope of Contract

11.3.1 Scope of the Contract shall be as defined in the tender document.

11.3.2 The MSP is required to provide such services, support and infrastructure and resources as the Purchaser or Purchaser's Technical Representative may deem proper and necessary, during the term of this Contract.

11.4 Placing of Work Order (WO)

11.4.1 The Purchaser reserves the right to procure any of the platforms and components and its quantity/licenses and associated number of required manpower as deemed appropriate from the Bill of Material quoted by the Bidder placed at Annex 5. The indicative list of platforms and components along with associated manpower as part of the work order for Implementation phase is given at **Annex 10.** A combination of platforms and components & services as deemed appropriate by the Purchaser shall constitute a Work Order (WO). Work Orders shall be issued on yearly basis, or as deemed appropriate by the Purchaser.

11.4.2 Objection, if any, to the Work Order must be reported to the Purchase by the MSP within five (5) working days counted from the date of issuance of Work Order for modifications, otherwise it shall be assumed that the MSP has accepted the Work Order. This is applicable in case of electronic delivery of Work Order also.

11.4.3 Upon receipt of any Work Order, the MSP shall promptly obtain and submit all necessary documentation, permits, approvals, or clearances required for the timely execution and delivery of the services outlined in the Work Order.

11.4.4 The details of Bill of Materials (BoM) submitted through Annex 5 are only for rate discovery of individual components, services, platforms and manpower. The Purchaser reserves the right to use these discovered rates to place additional Work Orders for any of the components, services, platforms and manpower over and above the contracted quantities at the rates discovered through this process, subject to the terms of the Contract.

11.5 Performance Bank Guarantee

11.5.1 The MSP is required to ensure submission of Performance Bank Guarantee (PBG) equivalent to 5 % (Five Percent) of the Work Order value issued by the Purchaser in accordance with the proforma given at **Annex 6: Proforma for Bank Guarantee for Contract Performance**. PBG must be furnished within 15 days of issue of WOs or as informed by the Purchaser. In the event of default/delay in submission of PBG within the stipulated time, the MSP shall be liable for a penalty amounting to 0.1% (Zero Point One Percent) of the WO value per day delay/default with a maximum penalty capping of 10% of Work order value. Beyond the maximum capping of 10% of Work Order value, in respect of the first WO issued under the contract, the Purchaser reserves the right to forfeit the PBG, terminate the contract with immediate effect.

11.5.2 The PBG shall be in the form of an unconditional and irrevocable Bank Guarantee/ e-Bank Guarantee from a Commercial bank in the name of National Informatics Centre (NIC), New Delhi.

11.5.3 The Performance Bank Guarantee shall remain valid for a period of 90(Ninety) days beyond the date of completion of all contractual obligations of the supplier for that Work Order.

11.5.4 Performance Bank Guarantee would be released only after successful completion of tasks assigned to MSP for respective WO and only after adjusting/ recovering any dues recoverable/ payable from/ by the MSP on any account under the contract.

11.5.5 The PBG shall be released (without any accrued interest) after the completion of all tasks (deliverables) as assigned in the WO.

12. Payment Terms

12.1 Payment Terms

12.1.1 The MSP shall submit a pre-received bill (three copies) quarterly/as per the payment schedule, in the name of "NATIONAL INFORMATICS CENTRE" at NIC, New Delhi.

12.1.2 MSP has to install the complete solution and prepare the installation report as per the prescribed format (to be shared by the Purchaser at the time of installation) and get it signed by the Authorised Representative of the Purchaser with date and stamp. For the overall project commissioning, the MSP shall submit UAT report for sign off by the Purchaser.

12.1.3 If the MSP fails to deliver as per the project timelines, penalties as per (paragraph 6.4 of this RFP) shall be applicable.

12.1.4 All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the prevailing Income-Tax Act.

12.1.5 Payment against Work Order shall be made as per payment schedule specified in paragraph 12.2.

12.1.6 If the Operational phase starts in between the ongoing calendar Quarter, the payment quarter shall start from the next calendar quarter however the residual amount of the previous quarter shall be calculated on pro-rata basis.

12.1.7 For subsequent Work Orders, placed during the lifecycle of the contract, the payment quarter shall start from the next calendar quarter however the residual amount of the previous quarter shall be calculated on pro-rata basis and shall be incorporated in the payment of the subsequent quarter.

12.1.8 For the purpose of any payment, the quarter shall be the same as the calendar quarter; that is

Q1: January – March
Q2: April – June
Q3: July – September
Q4: October – December

12.1.9 Payment shall be made after deduction of all applicable penalties, as per Service Level Agreement (as defined in Section 6 of the RFP), the SLAs compliance shall be measured on monthly basis.

12.1.10 SLA penalties during the operations phase (post go-live) shall be calculated on a Monthly basis and shall be liable to be deducted from payments due to the MSP. Monthly MIS report shall be submitted by the MSP covering all the key details including SLA compliance of all the functions as per Section 6 of the RFP.

12.1.11 Purchaser will release the payment, subsequent to the receipt of the certificate from respective OEMs involved in the solution regarding extension of the services with the MSP for the year/quarter for which payment is to be made.

12.1.12 The Purchaser shall process and pay the bill within 30 days of receipt of the bill from the MSP in accordance with the provisions of Section 12. MSP shall provide all necessary documentation related to the invoice raised and such other documents as may be demanded by the Purchaser. Invoice without any of the said documents shall be deemed incomplete and not acceptable.

12.2 Payment Schedule

TABLE 12: PAYMENT SCHEDULE

S No.	Billing Cycle	Payment Milestone
1	i. Complete delivery of Hardware & Software as per BoM and Inspection thereof. ii. Installation of complete hardware mounting of hardware in the racks (wherever required) and power-on of the hardware. iii. Installation and configuration of software as per BoM.	60% cost of delivered hardware. Penalties shall be deducted as per paragraph 6.4 Table 7: Penalty on Product/Platform

2	On Go-Live, post successful installation, commissioning, integration and UAT	Remaining 40% cost of deployed hardware + One Time cost for Installation, commissioning of all H/W, S/W licenses for the UAT period + Actual cost for the manpower which is deployed between T3 till date of Go-Live as per Table 3 (For a maximum period of 5 weeks) Penalties shall be deducted as per paragraph 6.4 Table 7: Penalty on Product/Platform
3	Subsequent quarter-wise payment in respective years of Operational phase after Go-Live	Total cost of manpower deployed during the Qtr. + (Yearly cost of AMC of platform and components whose AMC commences in the quarter or is under the AMC)/4 + (license cost of the software platforms as per BOM for the respective year of the Operational phase)/4 + 100% cost of any new hardware as per PO (subsequent to delivery, installation, integration and sign-off which is added to Go-Live solution/Operational phase) + other miscellaneous charges payable in the quarter. **Penalties shall be deducted as per paragraph 6.3 Table 6: Penalties on SLA**

12.2.1 Payments shall be made subject to the following—

(c) Strict Adherence to project delivery times as per paragraph 5.8.

(d) Payment shall be released on deployment of all hardware and software components specified in the respective Work Order.

(e) The Three-year period and any extensions thereof for the software licenses and hardware warranty shall be from the date of Go-Live.

(f) The MSP shall provide all necessary documentation related to the Services consumed and any other documents as demanded by the Purchaser. Invoice without any of the said documents shall be deemed incomplete and not acceptable.

(g) The Purchaser shall release the payment for Services rendered and accepted, subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the contract and meet SLA requirements.

(h) For release of payment for annual license subscription of the supplied software the MSP shall share the required documents from the respective OEM indicating that the annual subscriptions have been renewed.

(i) The Purchaser shall not make payment for manpower deployed between T3 and T5 (as per Table 3: Project Delivery Timelines) beyond 5 weeks from T3 (on actual basis) till Go-Live.

12.2.2 The MSP Shall provision and deploy all hardware required for the entire period of the contract prior to Go-Live. For any change in the requirement of hardware and software due to change in the scale of the project, paragraph 5.5 shall apply and the payment for the procured items shall be as follows:

Table 13: Payment Schedule (if there is any change in hardware/software requirement due to scale of the project)

1	(a) Complete delivery of Hardware & Software	60% cost of deployed hardware + 50% of license cost of the first year for the deployed software platforms.

	and Inspection thereof. (b) Installation of complete hardware mounting of hardware in the racks (wherever required) and power-on of the hardware (c) Installation and configuration of software.	
2	Go-Live	Remaining 40% cost of deployed H/W and 25% cost of the first year for the deployed S/W platforms.
3	Payment for the remaining 25% annual subscription license for the software procured shall be included in the payments of subsequent four quarters of the contract.	

12.3 Payment against time-barred claims

12.3.1 All claims against the Purchaser shall be time-barred after a period of three years, reckoned from the date on which payment falls due, unless the payment claim has been under correspondence. The Purchaser shall be entitled to reject such claims.

12.3.2 In respect of any claim where the same is raised without furnishing the documents as required under the Contract and the Purchaser, as a result, is not in position to claim input tax credit under the Applicable Law(s) governing taxation, the MSP shall not be entitled to payment of such input tax credit amount as the Purchaser would not be in position to claim.

13. Other Terms & Conditions for Bidder/MSP

13.1 General Conditions

13.1.1 As a matter of policy and practice and on the basis of Notification published in Gazette of India dated 14th March 1998, it is clarified that services and supplies of the MSP selected through this tender can be availed by National Informatics Centre (NIC). The Bidder which shall be called MSP, shall be obliged to render services to Purchaser as per the Work Order(s).

13.1.2 Consortium is not allowed.

13.1.3 The MSP/OEM shall undertake to provide support for the supplied solution for entire contract period and any extension thereof.

13.1.4 The warranty of all supplied solutions shall commence after the date of Go-Live.

13.1.5 Any deviation in Bid terms and conditions may lead to rejection of the Bid.

13.1.6 In case the MSP is found in-breach of any condition(s) of tender or supply order, at any stage during the course of supply/ installation/commissioning or warranty period, the legal action as per rules/laws, shall be initiated against the MSP and Security Deposits shall be forfeited.

13.1.7 Any attempt by Bidder to bring pressure towards Purchaser's decision-making process, such Bidders shall be disqualified for participation in the present tender.

13.1.8 Printed conditions specified in the tender Bids submitted by Bidders shall not be binding on Purchaser. All the terms and conditions for the supply, testing and installation, payment terms, penalty etc. shall be as those specified herein and no change in the terms and conditions by the Bidders shall be

acceptable. Alterations/overwriting, if any, in the tender Bids shall be attested properly by the Bidder, failing which, the tender shall be rejected.

13.1.9 Upon verification, evaluation / assessment, if in case any information furnished by the Bidder is found to be false/incorrect, their total Bid shall be summarily rejected and no correspondence on the same, shall be entertained.

13.1.10 In case the manpower is required to travel outside the city of location of his/her deployment as per approval of the Purchaser or on request of the purchaser, the Purchaser shall bear the travel and boarding expenses of the manpower as per entitlement of a central government officer at the Level 10 of 7th CPC or the guidelines/rules of the Government for non-officials shall be followed, as deemed appropriate by the Purchaser. The MSP shall include these expenses in the quarterly invoice along with all relevant documents that include travel tickets, boarding passes in original. However, no expenses are admissible on account of relocation of MSP resources on projects anywhere in India.

13.1.11 Purchaser shall not be held responsible for any misinterpretation, presumption or misunderstanding of the RFP by the Bidder, while responding to this tender.

13.1.12 EMD of the unsuccessful Bidders shall be returned to the respective Bidders at the earliest after expiry of the final Bid validity and latest on or before the 30th day after the award of the contract results. However, in case of two stage Bidding, EMD of unsuccessful Bidders during first stage i.e., technical evaluation, shall be returned within 30 days of declaration of results of first stage i.e., technical evaluation.

13.2 Warranty

13.2.1 The MSP warrants that all the Goods are new, unused, and of the most recent or current models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the Contract.

13.2.2 The MSP further warrants that the Goods shall be free from defects arising from any act or omission of the Supplier or arising from design, materials, and workmanship, under normal use in the conditions prevailing in the country of final destination.

13.2.3 Unless otherwise specified in the other terms and conditions, the warranty shall remain valid for at least twelve (12) months after the Go-Live as indicated in Section 5, scope of work.

13.2.4 The Purchaser shall notify the MSP in writing of any defects discovered within the warranty period, providing a detailed description and all available evidence of such defects promptly upon discovery. The Purchaser shall provide the MSP with reasonable opportunity to inspect and verify the defects.

13.2.5 Upon receipt of such notice, the MSP shall, at its own cost and expense, promptly repair, replace, or rectify the defective Goods or parts thereof to the satisfaction of the Purchaser within a mutually agreed reasonable timeframe.

13.2.6 If having been notified, the MSP fails to remedy the defect within the specified period, the Purchaser may proceed to take within a reasonable period such remedial action as may be necessary, at the MSP's risk and expense and without prejudice to any other rights which the Purchaser may have against the MSP under the Contract.

13.3 Change Request

13.3.1 Due to the evolving nature of the project requirements and the complexity of the project, the Purchaser recognizes that frequent changes may be required after implementation of GSOC. The Purchaser also recognizes that these changes may require modification to the software, manpower and hardware

infrastructure and underlying processes and may thus have a financial impact. MSP shall work with the Purchaser to ensure that all change requests related to effective SOC management are addressed.

13.3.2 All significant change requests and especially, the ones with a financial impact, shall necessitate an amendment to the contract with respect to scope and price of the contract. The contract price may be increased up to a maximum of 25% of the initial awarded contract price after accounting for all the change requests during the period of the contract.

13.3.3 The change request will be initiated only in case, if the Purchaser directs in writing to the MSP or MSP requests to carry out the changes in relation to the services rendered by the MSP. No changes shall be implemented without prior written approval of the Purchaser.

13.4 Change Management Process

13.4.1 Change Request in respect of the contract will emanate from the Purchaser or MSP. The change request shall be initiated only in case, if the Purchaser directs in writing to the MSP or the MSP requests to carry out the changes in relation to the services rendered by the MSP. A Change Request shall be initiated after completing Change Control Note (CCN) (refer Annex 15). The MSP and the Purchaser, during the term of the Agreement and while preparing the CCN, shall determine whether the change is beyond the scope of services of work.

13.4.2 It is hereby also clarified that any change control suggested beyond 25% (forty percent) of the total contract value will be beyond the scope of the change control process. It is hereby clarified that the 25% (Twenty Five percent) of the total contract value as stated in herein above is calculated on the basis of Bid value submitted without tax by the MSP and accepted by the Purchaser or as decided and approved by the Purchaser. For arriving at the cost or change up to 25% (Twenty Five percent) of the total contract value, the payment terms as defined in Section 12 shall apply.

13.4.3 The change request can include items which are in addition to the BOM submitted as part of the Bid and are required for effective delivery of the SOC services.

13.4.4 As part of the change management, the Purchaser is not bound to purchase any item from the MSP only and may procure the item from elsewhere and get it installed and inducted as a part of the solution set up by MSP The MSP will be required to extend full cooperation and such item shall be part of the services being rendered by the MSP and all provisions including SLAs shall be applicable on MSP.

13.4.5 If the items submitted as part of the change request by the MSP are in addition to the BOM submitted, the rate reasonability shall be approved through a duly constituted committee by the Purchaser.

13.5 Confidentiality

13.5.1 All documents, data, associated correspondence or other information furnished by or on behalf of the Purchaser to the MSP, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract, are confidential and shall remain the property of the Purchaser and shall not, without the prior written consent of Purchaser neither be divulged by the contractor to any third party, nor be used for any purpose other than the procurement, maintenance or other services and work required for the performance of this Contract. If advised by the Purchaser, all copies of all such information in original shall be returned on completion of the MSP's performance and obligations under this contract.

13.5.2 The MSP shall not use Confidential Information, the name, or the logo of the Purchaser except for the purposes of providing the Service as specified under this contract.

13.5.3 The term "Confidential Information", as used herein, shall mean all business strategies, plans and procedures, proprietary information, software, tools, processes, methodologies, data and trade secrets, and other confidential information and materials of the Purchaser, its affiliates, their respective clients or suppliers, or other persons or entities with whom they do business, that may be obtained by the MSP from any source or that may be developed for the Purchaser as a result of the Contract.

13.5.4 The MSP shall be responsible for providing a signed NDA by its antecedents, delegates, and the sub-contractors to the Purchaser. The MSP shall be held responsible for any breach of the NDA by its antecedents, delegates, or sub-contractors. The MSP and all the deployed resources shall sign the NDA with reference to "THE OFFICIAL SECRETS ACT, 1923" before starting the installation / commissioning of SOC.

13.5.5 The provisions respecting confidentiality shall not apply to the extent, but only to the extent, that the information or document is:

(a) already known to the MSP free of any restriction at the time it is obtained from the Purchaser,

(b) subsequently learned from an independent third party free of any restriction and without breach of this provision.

(c) is or becomes publicly available through no wrongful act of the MSP or any third party.

(d) is independently developed by the MSP without reference to or use of any Confidential Information of the Purchaser/organisation; or

(e) is required to be disclosed pursuant to an applicable law, rule, regulation, government requirement or court order, or the rules of any stock exchange (provided, however, that the MSP shall advise the Purchaser of such required disclosure promptly upon learning thereof in order to afford the Purchaser a reasonable opportunity to contest, limit and/or assist the MSP in crafting such disclosure).

13.5.6 The MSP must ensure to provide the signed NDA in case of change in antecedents, delegates, and the sub-contractors from time-to-time.

13.5.7 The MSP shall notify the Purchaser promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Contract or with the authority of the Purchaser.

13.5.8 The MSP shall not use Confidential Information (CCTV records, Biometric Records, etc.), the name or the logo of the Purchaser except for the purposes of providing the Service as specified under the contract.

13.5.9 The MSP may only disclose Confidential Information in the following circumstances—

(a) with the prior written consent of the Purchaser.

(b) to a member of the MSP's Team ("Authorised Person") if:

(i) The Authorised Person needs the Confidential Information for the performance of obligations under the contract.

(ii) The Authorised Person is aware of the confidentiality of the Confidential Information and is obliged to use it only for the performance of obligations under the contract

13.5.10 The MSP shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidentiality contract with the members of the partners and other Systems Integrator's team members to the satisfaction of the Purchaser.

13.5.11 The MSP shall treat all the information provided by Purchaser such as IP schema, DC and Cloud architecture, block diagrams, manuals, policies, procedure, guidelines, employee details etc. (but not limited to) as top-secret information and shall not disclose the information without explicit written permission for the same by Purchaser.

13.5.12 The obligations under this clause shall survive for three years from termination or expiration of this Contract/agreement.

13.5.13 The Work Order/contract with the organisation may define more stringent confidentiality obligations depending on the nature of information / data being shared. In such event, the more stringent obligations shall prevail.

13.6 Integrity Pact

13.6.1 In compliance with the Central Vigilance Commissioner Circular No. 06/05/21 dated 3rd June 2021 regarding adaptation of Integrity Pact- Revised Standard Operating Procedure to ensure transparency, equity and competitiveness in public procurement, the Bidder(s) are required to sign an Integrity Pact with Purchaser.

13.6.2 The pact essentially is an agreement between the Bidder(s) and the Purchaser, committing the persons/Officials of both sides, not to resort to any corrupt practices in any aspect/stage of the contract. Only those Bidders, who commit themselves to such a pact with the Purchaser, would be considered competent to participate in the bidding process.

13.6.3 The Bidders are required to submit the signed Integrity pact along with the Technical Bid, failing which, the Bids would not be considered for evaluation for such Bidders and may get disqualified. The format for the integrity pact is attached as Annex 12: Format for Integrity Pact.

13.6.4 The Integrity pact shall be applicable from the date of Bid submission or from the date when the Purchaser sends signed copy of the Integrity Pact to the Bidder, whichever is later. Further, any violation of Integrity pact would entail disqualification of the Bidder(s) and forfeiture of EMD.

13.7 Obligation to Indemnify Purchaser

13.7.1 For breach of IPR Rights

(a) The MSP shall indemnify and hold harmless, free of costs, the Purchaser and its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Services provided by the MSP under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with:

   i. Any designs, data, drawing, specification, or other documents or Services provided or designed by the MSP for or on behalf of the Purchaser.
   ii. The sale by the Purchaser in any country of the services/ products produced by the Services delivered by the MSP, and
   iii. The delivery of the Services by the MSP or the use of the Services at the Purchaser's Site

(b) Such indemnity shall not cover any use of the Services or any part thereof other than for the purpose indicated by or to be reasonably inferred from the contract, neither any infringement resulting from the use of the Services or any part thereof, or any service/ products produced thereby in association or combination with any other service, equipment, plant, or materials not delivered by the MSP.

(c) If any proceedings are brought, or any claim is made against the Purchaser arising out of the matters referred above, the Purchaser shall promptly give the MSP a notice thereof. At its own expense and in the Purchaser's name, the MSP may conduct such proceedings and negotiations to settle any such proceedings or claim, keeping the Purchaser informed.

(d) If the MSP fails to notify the Purchaser within twenty-eight (28) days after receiving such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its behalf at the risk and cost to the MSP.

(e) At the MSP's request, the Purchaser shall afford all available assistance to the MSP in conducting such proceedings or claim and shall be reimbursed by the MSP for all reasonable expenses incurred in so doing.

13.7.2 For Losses and Damages Caused by MSP

(a) The MSP shall indemnify and keep harmless the Purchaser, from and against, all actions, suit proceedings, losses, costs, damages, charges, claims, and demands of every nature and description brought or recovered against the Purchaser because of any act or omission or default or negligence or trespass of the MSP, his agents, or employees despite all reasonable and proper precautions may have been taken, during the execution of the Services. The MSP shall make good at his own expense all resulting losses and/ or damages to:

i. the Services themselves or
ii. any other property of the Purchaser or
iii. the lives, persons, or property of others / third parties.

(b) In case the Purchaser is called upon to make good such costs, loss, or damages, or to pay any compensation, including that payable under the provisions of the Workmen's Compensation Act or any statutory amendments thereof; the amount of any costs or charges including costs and charges in connection with legal proceedings, which the Purchaser may incur about it, shall be charged to the MSP. All sums payable by way of compensation under any of these conditions shall be considered as reasonable compensation to be applied to the actual loss or damage sustained and whether or not any damage shall have been sustained.

(c) The Purchaser shall have the power and right to pay or to defend or compromise any claim of threatened legal proceedings, or in anticipation of legal proceedings being instituted consequent on the action or default of the MSP, to take such steps as may be considered necessary or desirable to ward off or mitigate the effect of such proceedings, charging to MSP, as aforesaid, any sum or sums of money which may be paid and any expenses whether for reinstatement or otherwise which may be incurred and the propriety of any such payment, defence or compromise, and the incurring of any such expenses shall not be called in question by the MSP.

13.8 Liquidated Damages

13.8.1 The delivery dates, timetables, milestones and other requirements specified in the RFP and this contract are binding on the MSP and the MSP agrees to accomplish the user requirement specified and Scope of Work under this contract as per the Timelines specified in the RFP.

13.8.2 If the MSP fails to achieve the Timelines or the Service Levels due to reasons solely attributable to the MSP, the Purchaser shall be entitled to recover from the MSP the liquidated damages as per the SLAs specified in Section 6 of this RFP.

13.8.3 In the event MSP is not solely responsible for such failure in Timelines and Service Levels, the Purchaser shall have the right to determine such extent of fault and liquidated damages in consultation with the MSP and any other party it deems appropriate. In such cases, the proportionate Liquidated Damage as mutually determined shall be levied.

13.8.4 Recovery of liquidated damages shall not be the sole and exclusive remedies available to the Purchaser and the MSP shall not be relieved from any obligations by virtue of payment of such liquidated

damages. Liquidated damages shall be capped at 10% of the Total Contract Value. If the liquidated damages cross the cap on liquidated damages specified herein, the Purchaser shall have the right to terminate the contract for default and consequences for such termination as provided in this contract shall be applicable.

13.9 Limitation of Liability

13.9.1 Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the MSP to the Purchaser, whether under the contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the MSP to indemnify the Purchaser concerning IPR infringement.

13.10 Labour Laws

13.10.1 The MSP shall, and hereby agrees to, comply with all the provisions of Indian Labour Laws and industrial laws in respect of the resources employed thereof.

13.10.2 Wherever necessary, the MSP shall apply for and obtain license as provided under Contract Labour (Regulation and Abolition) Act, 1970, and strictly comply with all the terms and conditions that the licensing authority may impose at the time of grant of license. The Purchaser shall not be held responsible for any breach of the license terms and conditions by the MSP.

13.10.3 The MSP shall be solely responsible for the payment of wages to the deployed resources and ensure its timely payment thereof.

13.10.4 The MSP shall duly maintain a register giving particulars of the deployed resources, nature of work, rate of wages, etc.

13.10.5 The MSP shall also ensure compliance to the following labour legislations:

(a) Minimum Wages Act
(b) Employees Provident Fund Act
(c) Employees State Insurance Act
(d) Workmen's Compensation Act, if the ESI Act does not apply
(e) Maternity Benefit Act
(f) Code on Wages 2019,
(g) The Industrial Relations Code 2020,
(h) The Social Security Code 2020, and
(i) The Occupational Safety, Health and Working Conditions Code 2020
(j) Any other laws, as applicable, time to time

13.10.6 The MSP shall be solely responsible to adhere to all the rules and regulations relating to labour practices and service conditions of its workmen and at no time shall it be the responsibility of Purchaser.

13.10.7 The resources deployed under this tender shall be on pay roll and full-time employee of the MSP or OEM" Subcontracting of the resources/manpower is only allowed in case as defined in (paragraph 8.18).

13.10.8 It is expressly understood and agreed to between the parties that the resources deployed by the MSP shall be the employees of the MSP for all intents and purposes.

13.10.9 The said manpower is not entitled to any claim, right, preference, etc. over any job/regular employment of Purchaser or its users. The MSP or its resources shall not at any point of time have any claim whatsoever against Purchaser.

13.10.10 In case any employee of the MSP so deployed enters in dispute of any nature whatsoever, it shall be sole responsibility of the MSP to contest the same at appropriate forum(s).

13.10.11 Medical benefits should be provided by the MSP to the resources deployed.

13.11 Conflict of Interest

13.11.1 The MSP shall disclose to the Purchaser in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the MSP or the MSP's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

13.12 Severance

13.12.1 In the event any provision of this Contract is held to be invalid or unenforceable under the applicable law of India, the remaining provisions of this Contract would remain in full force and effect.

13.13 Force Majeure

13.13.1 For the purposes of this RFP, "Force Majeure" means an event which is beyond the reasonable control of a Party, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, landslide, fire, explosion, storm, tempest, flood, hurricane, cyclone, lightning, thunder, other adverse weather conditions, volcanic eruption, pandemic, quarantine, plague, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by government agencies.

13.13.2 Force Majeure shall not include any event that is caused by the negligence or intentional action of a Party or its agents or its employees, or any event which a diligent Party could reasonably have been expected to have considered at the time of the conclusion of the Contract and to have avoided or overcome in the carrying out of its obligations hereunder, through exercise of reasonable skill and care.

13.13.3 Force Majeure shall not include insufficiency of funds or failure to make any payment required hereunder.

13.13.4 If at any time, during the term of the Contract, the performance in whole or in part by any Party of any obligation hereunder is prevented or delayed by reasons of occurrence of Force Majeure events as defined above, and notice of such occurrence is duly furnished by such Party, seeking concession, to the other, as soon as practicable, but within 21 days from the date of such occurrence, and satisfies the party adequately of the measures taken by it, no Party shall, by reason of that event, be entitled to terminate the Contract, nor shall any Party have any claim for damages against the other Parties in respect of such non-performance or delay in performance, and deliveries under the Contract shall be resumed as soon as practicable after such event has come to an end or ceased; and the decision of the Purchaser as to whether the deliveries have resumed or not shall be final and conclusive.

13.14 Events of Default by MSP

13.14.1 The failure on the part of the MSP to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of the MSP. The events of default as specified above may include inter-alia the following:

(a) The MSP has failed to perform any instructions or directives issued by the Purchaser which it deems proper and necessary to execute the scope of work under the Contract, OR

(b) The MSP/MSP's Team has failed to conform with any of the Service/Facility Specifications/standards as set out in the scope of work of this Tender document or has failed to adhere to any amended direction, modification or clarification as issued by the Purchaser during the term of this Contract and which the Purchaser deems proper and necessary for the execution of the scope of work under this Contract

(c) The MSP has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid, the Tender and this Contract

(d) The MSP has failed to comply with or is in breach or contravention of any applicable laws of India.

13.14.2 Failure of the successful MSP to comply with the Tender requirements shall constitute sufficient grounds for the annulment of the award and forfeiture of the PBG.

13.14.3 In case of exigency, directly and solely attributable to MSP, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the MSP. Such work shall be got done by the Purchaser from elsewhere by following approved Government procurement procedures.

13.15 Dispute Resolution /Arbitration

13.15.1 Amicable settlement

The Parties shall, in good faith, endeavour to settle amicably all disputes arising out of or in connection with this Agreement or interpretation thereof.

13.15.2 Dispute Resolution

(a) Any dispute, difference or controversy whatsoever, howsoever arising under or out of or in relation to this Agreement (including its interpretation) between the Parties, and so notified in writing by any Party to another Party (the "Dispute") shall, in the first instance, be attempted to be resolved amicably in accordance with the conciliation procedure set forth in paragraph 13.15.

(b) The Parties agree to use their best efforts for resolving all Disputes arising under or in respect of this Agreement promptly, equitably and in good faith, and further agree to provide each other with reasonable access during normal business hours to all non-privileged records, information and data pertaining to any Dispute.

(c) Any Dispute which is not resolved amicably by conciliation as provided in paragraph 13.15, shall be finally decided by reference to Arbitration.

(d) This Agreement and the rights and obligations of the Parties shall remain in full force and effect, pending the award in any Arbitration proceedings hereunder.

13.15.3 Conciliation

In the event of any Dispute between the Parties, any Party may call for amicable settlement, and upon such reference, the nominated persons shall meet not later than 10 days from the date of reference to discuss and attempt to amicably resolve the Dispute. If such meeting does not take place within the said period of 10 days, or the Dispute is not amicably settled within 15 days of the meeting, or the Dispute is not resolved as evidenced by the signing of written terms of settlement within 30 days of the notice in writing referred to in Section 13 or such longer period as may be mutually agreed upon by the Parties, any Party may refer the Dispute to Arbitration in accordance with the provisions of Section 13.

13.15.4 Arbitration

(a) Without prejudice to the right of the Purchaser to terminate the Contract and pursue other remedies thereunder, if a dispute, controversy or claim arises out of or relates to the Contract, or breach, termination, or invalidity thereof, and if such dispute, controversy or claim cannot be settled and resolved by the Parties through discussion and negotiation, then the Parties shall refer such dispute to sole Arbitrator appointed with the mutual consent of the Purchaser and

the MSP. The Arbitration proceedings shall be conducted in English and a written order shall be passed. The venue of the Arbitration shall be Delhi. The Arbitration shall be held in accordance with the provisions of the Arbitration and Conciliation Act, 1996. The Parties agree to have their dispute(s) or difference(s) resolved in terms of section 29B of the said Act.

(b) The Arbitration award shall be final, conclusive and binding upon the Parties and judgement may be entered thereon, upon the application of either Party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of Arbitration, including fees and expenses of the Arbitrator, shall be shared equally by the Parties, unless the award otherwise provides.

(c) The courts in Delhi shall have exclusive jurisdiction in relation to this Contract.

13.16 Applicable Laws

13.16.1 The MSP shall be governed by the laws of India and shall include any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, byelaw, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on or until the date of the execution of the Agreement, and during the subsistence thereof, that the Purchaser may get into with the MSP, applicable to the Project.

13.17 Adherence to safety procedures, rules, regulations & restriction

13.17.1 MSP shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. Purchaser's employee shall also comply with safety procedures/policy.

13.17.2 The Purchaser shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

13.17.3 MSP shall also adhere to all security requirement/regulations of the Purchaser during the execution of the contract.

13.17.4 Access to the Purchaser's SOC and Data centre shall be strictly restricted in the following manner:

13.17.5 No access to any person except one explicitly authorised by the Purchaser shall be allowed entry. Even if granted, access shall be restricted to system/equipment necessary to run the engagement and access to any other equipment must be strictly precluded by necessary means, locks, video surveillance, etc.

13.17.6 No access to any employee of the MSP, except the essential staff who has genuine work-related need, shall be furnished.

13.18 Statutory Requirements

13.18.1 During the tenure of the contract nothing shall be done by the Purchaser in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange, etc.

13.18.2 The MSP and their personnel/representative shall not alter / change / replace any hardware component proprietary to the Purchaser and/or under warranty or AMC of third party without prior consent of the Purchaser.

13.18.3 The MSP and their personnel/representative shall not without consent of the Purchaser install any hardware or software not purchased / owned by the Purchaser.

13.19 Information Security

13.19.1 The MSP shall not carry and/or transmit any material, information, layouts, diagrams, storage media or any other goods/material in physical or electronic form, which are proprietary to or owned by the Purchaser, out of SOC and extended location premises without prior written permission from the Purchaser.
13.19.2 MSP acknowledges that Purchaser proprietary information or materials, whether developed by Purchaser or being used by Purchaser pursuant to a license Work Order with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to Purchaser; and MSP agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorised use or disclosure thereof, which care shall not be less than that used by MSP to protect its own proprietary information. MSP recognizes that the good shall of Purchaser depends, among other things, upon MSP keeping such proprietary information confidential and that unauthorised disclosure of the same by MSP could damage Purchaser and that by reason of MSP's duties hereunder. MSP may come into possession of such proprietary information, even though MSP does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by the contract. MSP shall use such information only for the purpose of performing the said services.
13.19.3 Any proprietary tools of the MSP, if any used for the project and MSPs Pre-existing IPR will remain with the MSP.
13.19.4 The authorised signatory of the MSP shall sign the NDA with reference to this tender and "The Official Secrets Act, 1923" within 7 days and submit the same along with the acceptance of the Work Order letter.
13.19.5 All the deployed resources shall also sign the NDA with reference to "The Official Secrets Act, 1923" within 7 days after confirmation of acceptance of the resource by Purchaser.

13.20 Continuance of Contract

13.20.1 Notwithstanding the fact that settlement of dispute(s) (if any) under arbitration may be pending, the parties hereto shall continue to be governed by and perform the work in accordance with the provisions under the Scope of Work to ensure continuity of operations.

13.21 Termination of Contract

Purchaser reserves the right to suspend any of the services and/or terminate the agreement in one or more of the following circumstances by giving 90 days' notice in writing:

13.21.1 Termination process

Upon occurrence of an event of default as set out in above clauses, Purchaser shall deliver a default notice in writing to the other party which shall specify the event of default and give the MSP an opportunity to correct the default. At the expiry of notice period, unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the agreement.

13.21.2 Termination for insolvency, dissolution, bribery

(a) The Contract may be terminated by the Purchaser and the deposits/guarantees in possession of the Purchaser (Performance Bank Guarantee) may be forfeited in case a public officer is bribed by the MSP or the MSP becomes insolvent or in case of dissolution/winding up of MSP, provided that

such termination shall not prejudice or effect any right of action or remedy which has accrued thereafter to Purchaser.

(b) In case of Contract termination for reasons specified in Section 13, the Purchaser reserves the right to recover any dues payable by the MSP from any amount outstanding to the credit of the MSP, including on account of any pending bills and/or by invoking the Performance Bank Guarantee in possession of the Purchaser and the remaining amount may be paid to the liquidator/MSP, as applicable.

13.21.3 Termination for default/breach:

Purchaser may without prejudice to any other remedy for breach of contract, (including forfeiture of Performance Bank Guarantee) by written notice of default sent to the MSP, terminate the contract in whole or in part after sending a notice to the MSP in this regard. Further, Purchaser may afford a reasonable opportunity to the MSP to explain the circumstances leading to such a breach and may increase the time limit for curing such breach before terminating the contract. Any notice served pursuant to this Clause shall give reasonable details of the breach. Following conditions shall be considered as breach of contract:

(a) If the MSP fails to accept the Work Order(s).

(b) The MSP/MSP's Team has failed to conform with any of the Service/Facility Specifications/standards as set out in the scope of work of this Tender document or has failed to adhere to any amended direction, modification or clarification as issued by the Purchaser during the term of this Contract and which the Purchaser deems proper and necessary for the execution of the scope of work under this Contract.

(c) The MSP goes into liquidation, voluntarily or otherwise.

(d) The MSP/MSP's Team has failed to comply with or is in breach or contravention of any applicable laws.

(e) If the MSP fails to deliver services within the time period specified in the Work Orders granted by Purchaser.

(f) If the MSP fails to meet any other terms and conditions under the contract.

13.21.4 Termination for convenience

Purchaser may by written notice, sent to the MSP, terminate the Work Order and/or the Contract, in whole or in part at any time of its convenience. The notice of termination shall specify that termination is for Purchaser's convenience, the extent to which performance of work under the work-order and/or the contract is terminated and the date upon which such termination becomes effective. Purchaser reserves the right to cancel the remaining part and pay to the MSP an agreed amount for partially completed Services.

13.21.5 Termination for violation of law/agreement

(a) In the event of any content found to be in violation of any law or direction of statutory authority or found to be in contravention of Intellectual Property Rights (IPR) etc., Purchaser may suspend / terminate the Agreement. The Purchaser reserves the right to terminate the Agreement for any breach or non-observance or non-fulfilment of Agreement conditions that may come to its notice through complaints or as a result of the regular monitoring. Notwithstanding any other rights and remedies provided elsewhere in the agreement, upon termination of the Agreement:

(b) Neither Party shall represent the other Party in any of its dealings.

(c) The expiration or termination of the Agreement for any reason whatsoever shall not affect any obligation of either Party having accrued under the Agreement prior to the expiration or termination of the Agreement and such expiration or termination shall be without prejudice to any liabilities of either Party to the other Party existing at the date of expiration or termination of the Agreement.

(d) Purchaser reserves the right to terminate the Contract in the event of data breach or stealing of data or unauthorised access.

(e) Payments for all satisfactorily completed services till the time of completion of agreed exit management period shall be made to the MSP in the event of termination.

13.21.6 Consequences of termination

(a) In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], Purchaser shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the MSP shall be obliged to comply with and take all available steps to minimize loss resulting from the termination/breach, and further allow the next successor MSP to take over the obligations of the erstwhile MSP in relation to the execution/continued execution of the scope of the Contract.

(b) Nothing herein shall restrict the right of the Purchaser to invoke the MSP's, enforce the indemnity as defined under Section 13, and pursue such other rights and/or remedies that may be available to the Purchaser under law or otherwise.

(c) The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

(d) In case of termination, all hardware, software, licenses, tools and any other components for which the payment has been made by the Purchaser shall be the property of the Purchaser.

(e) Post the termination notice, the MSP shall provide support, as per the exit management provisions hereunder.

13.22 Exit Management

13.22.1 The MSP may also prepare a structured and detailed exit management plan prior to submission of the Bid. Post signing of the contract, the exit management plan shall be finalized by the MSP in consultation with the Purchaser.

13.22.2 The exit management requirements as elaborated below must be read in conjunction to and in harmony with related clauses of the contract.

13.22.3 Given the critical nature of the service, it is imperative that a well-defined exit management strategy be made ready which shall enable easy transition of activities when the contract expires/ is truncated.

13.22.4 Accordingly, the MSP shall finalize the exit management plan within two months of Go-Live, which shall focus on the key activities it shall perform to ensure that a seamless transition of knowledge and activities be possible, and the same shall be evaluated. The exit management plan shall be based on the plan proposed by the MSP in its technical proposal. The final exit management plan shall have to be mutually agreed upon by Purchaser and the MSP.

13.22.5 The MSP shall understand that ensuring a smooth transition at the end of the project period is a key requirement from Purchaser. The MSP needs to update the exit management plan on half yearly basis or earlier or whenever required by Purchaser in case of major changes during the entire contract period. While proposing the exit management plan, the MSP shall ensure that the subsequent points are taken care of.

13.22.6 At the end of the contract period or during the contract period or contract termination, if any other agency is identified or selected for providing services related to the scope of work as in the contract, the MSP shall ensure proper and satisfactory transition is made to the other agency. In case Purchaser wants to take over the project itself, then MSP has to ensure proper transition to the team designated by Purchaser.

13.22.7 All risks during transition stage shall be properly documented by MSP and mitigation measures be planned in advance and recorded in the exit management plan so as to ensure smooth transition without any service disruption.

13.22.8 The MSP shall provide all knowledge transfer of the system to the satisfaction of Purchaser as per the specified timelines.

13.22.9 The exit management period starts:

(a) In case of expiry of Contract, at least 12 Months prior to the date when the Contract comes to an end, or

(b) In case of termination of Contract, on the date when the notice of termination is sent to the MSP.

13.22.10 The exit management period ends on the date agreed upon by the Purchaser or 12 Months after the beginning of the exit management period, whichever is earlier. In case of termination 12 Months exit period applies there also until Purchaser decides otherwise.

13.23 Applicability of the IT Act and Rules

13.23.1 Adherence to IT Laws and Government Regulations

The solution from the OEM should comply to standards (ISO 27001:2013, ISO 22301:2019, ISO 20000-1:2018 etc.) and regulations as notified by Government of India from time-to-time including but not limited to IT Act 2000 and its subsequent amendments, Digital Personal Data Protection Act 2023, RBI Guidelines, Ministry of Electronics and Information Technology (MEITY), CERT-IN, NCIIPC, NIC, etc. MSP need to ensure that offered solution as part of project scope and ensuing policies and procedures to have strict compliance to all cyber/information security policies, procedures and regulation and its subsequent updates issued by Government of India or its authorized agencies during the entire Project duration.

13.24 Intellectual Property Rights

13.24.1 Subject to the other provisions contained in this Clause, the MSP shall agree that all deliverables created or developed by the MSP, specifically for the Purchaser, together with any associated copyright and other intellectual property rights, shall be the sole and exclusive property of National Informatics Centre (Purchaser).

13.24.2 The Purchaser shall acknowledge that:

(a) In performing services under the Contract, the MSP may use MSP's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or

were developed or owned by the MSP prior to or independent of the services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the services hereunder, ("the MSP's Pre-Existing IP").

(b) Notwithstanding anything to the contrary contained in the Contract, the MSP shall continue to retain all the ownership, the rights title and interests on all the MSP's Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the MSP from using the MSP's Pre-Existing IP in any manner.

(c) If any of the MSP's Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the MSP hereby grants to the User Department/Purchaser a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license of the deliverables with the right to sublicense through multiple tiers, to use, copy, install, perform, display, modify and create derivative works of any such deliverables and only as part of the deliverables in which they are incorporated or embedded.

(d) Purchaser being the owner of all the IPs created in the deliverables, except the Pre-Existing IPs of the MSP used in the development and deployment, shall have exclusive rights to use, copy, license, sell, transfer, share, deploy, develop, modify or any such act that the organisation/Purchaser may require or find necessary for its purpose. The IP rights of the Purchaser shall indefinitely subsist or continue in all future derivatives of the deliverables.

(e) The MSP or its deployed resources shall have no claims whatsoever on the deliverables and all the IPs created in deliverables except its Pre-Existing IPs for which it shall grant all authorizations to the organisation/Purchaser for use as detailed in the Clause (c) above.

(f) Except as specifically and to the extent permitted by the MSP, the organisation/Purchaser shall not engage in reverse compilation or in any other way arrive at or attempt to arrive at the source code of the MSP's Pre-Existing IP, or separate MSP's Pre-Existing IP from the deliverable in which they are incorporated for creating a standalone product for marketing to others.

(g) The organisation/Purchaser shall warrant that the materials provided by the organisation/Purchaser to MSP for use during development or deployment of the application shall be duly owned or licensed by the organisation/Purchaser.

(h) The Purchaser's contractual rights to use the Standard Software or element of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with relevant licence to a legally constituted successor organisation (e.g., a reorganisation of a public entity formally authorised by the government or through a merger acquisition of a private entity).

13.25 Transfer of Project documentation and data

13.25.1 Before the expiry of the exit management period, the MSP shall deliver relevant records and reports pertaining to the Project and its design, implementation, operation, and maintenance including all operation, maintenance records and manuals pertaining thereto and complete as on the divestment date. All such materials shall be in formats and media reasonably acceptable to the Purchaser.

13.25.2 The MSP shall provide the Purchaser with a complete and up to date list of the documents, data and relevant system details to be transferred to the Purchaser within 30 days of start of Exit Management Period.

13.25.3 The MSP shall pass on to the Purchaser, the subsisting rights in any licensed products on terms not less favourable to the Purchaser, than that enjoyed by the MSP.

13.25.4 Even during the Exit Management period, the MSP shall continue to perform all their obligations and responsibilities as stipulated under the contract, and as may be proper and necessary to execute the Scope of Work in terms of the RFP, to execute an effective transition and to maintain business continuity.

13.25.5 All solutions provided by MSP under the scope of the RFP should be interoperable during the transfer/hand over at time of exit/contract termination. No proprietary service is to be used/implemented by the MSP. Any customization/ tools/ effort required for smooth transfer of documentation and data arising out of interoperability issue will be borne by the MSP.

13.25.6 The MSP shall assist the Purchaser to migrate the current services from the current infrastructure to Purchaser.

13.25.7 All equipment and solutions utilised to deliver the project scope should have valid service contract and should not be under end of life/end of support during contract period and any extensions thereof.

13.25.8 The MSP shall share the details of all existing service contracts and agreements, executed with current vendors, sub-contractors, Service Providers related to this RFP with the Purchaser on yearly basis under an NDA.

13.26 Official secrets

13.26.1 The Service Provider shall ensure and inform all persons employed by it in any works in connection with the Contract that the Official Secrets Act, 1923 shall apply and continue to apply to them even after execution and expiry of the Contract or resignation by any employee and that they shall be bound to not disclose any information regarding this Contract to any third party. The Service Provider shall bring to the notice of the Purchaser any information found to be leaked or disclosed. Where such leakage or disclosure is brought to the notice of the Purchaser or the Purchaser detects any leakage or disclosure during the Contract Period (including any period for which the Contract is extended) or after its expiry, the person concerned as well as the Service Provider shall be liable for penal action. The Purchaser shall have the liberty to terminate the Contract without notice, thereby invoking the exit management provisions of this Agreement.

13.27 Publicity

13.27.1 The MSP shall not, without the prior written consent of the Purchaser, make, permit, or authorise any press releases, public announcements, advertisements, case studies, marketing materials, or any other form of public disclosure relating to this Project, the Contract, or the Purchaser, whether in print, electronic, or any other medium.

13.27.2 The restriction under Clause 13.27.1 shall apply both during the term of this Contract (including any extensions) and after its expiry or termination, irrespective of the reason for termination.

13.27.3 Any unauthorised publicity or disclosure by the MSP or its employees, agents, subcontractors, or representatives shall constitute a material breach of this Contract, entitling the Purchaser to impose penalties, recover damages, and/or terminate the Contract forthwith without prejudice to any other remedies available under law.

13.28 Restriction under rule 144 (xi) of the GFR 2017

13.28.1 Any bidder from a country which shares a land border with India will be eligible to bid in this RFP only if the bidder is registered with the Competent Authority (i.e., Registration Committee constituted by Department for Promotion of Industry and Internal Trade (DPIIT)). Further, any bidder (including bidder from India) having specified Transfer of Technology (ToT) arrangement with an entity from a country which shares a land border with India, shall also require to be registered with the same Competent Authority. Please refer to the Govt. notifications provided at https://doe.gov.in/procurement-policy-divisions for details & updates [under Rule 144 (xi) of the General Financial Rules 2017].

13.28.2 The bidder shall submit a certificate to this effect. If such certificate, given by a bidder whose bid is accepted is found to be false, this would be a ground for debarment and further legal action in accordance with the law.

13.28.3 The Purchaser reserves the right to verify the authenticity of the certificate with the issuing authority at any stage of the procurement process or during the currency of the contract. Failure to maintain the validity of the registration throughout the contract period shall be deemed a material breach of contract, entitling the Purchaser to terminate the agreement forthwith without prejudice to other legal remedies.

13.28.4 For details, clarifications, and updates, bidders are advised to refer to the Government of India notifications available at https://doe.gov.in/procurement-policy-divisions.

13.29 Compliance to Digital Personal Data Protection Act, 2023

13.29.1 MSP shall ensure all the personal data in the MSP supplied components and platforms is stored in compliance with Digital Personal Data Protection Act, 2023. The MSP shall also ensure that personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and the access privileges to the back-end data segment are limited to the minimum necessary set of authorised users and are protected with multi-factor authentication.

13.30 Completion Certificate and Final payment

13.30.1 Completion Certificate:

Upon a written intimation from the MSP, the Purchaser shall issue a certificate of completion duly indicating the date of completion after satisfying itself of the following. The Purchaser may also issue such a certificate indicating the date of completion concerning any part of the service (before the completion of the whole of service), which has been completed to the satisfaction of the Purchaser:

(a) that the whole of the Services to be done under the provisions of the contracts have been completed or when any such certificate is given in respect of part of a service, such part shall be considered completed.

(b) that they have been inspected by him since their completion and found to be in good and substantial order,

(c) that such completed services have satisfactorily passed any final test or tests that may be prescribed,

(d) that all properties, works and things, removed, disturbed, or damaged in consequence of the Services have been adequately replaced and

(e) that the Purchaser has returned in good condition, all assets loaned or hired from the Purchaser (if any) and has given a satisfactory account of payments made to or retained by the Purchaser for such loaned/ hired assets,

(f) that the MSP has made good and satisfied in conformity with the contract all expenses and demands:

i. incurred by or made upon by the Purchaser.

ii. for or in respect of damages or losses from or in consequence of the services.

13.30.2 Approval Only by Completion Certificate:

No certificate other than completion certificate referred to in sub-clause above shall be deemed to constitute approval of any service or other matter in respect of which it is issued or shall be taken as an admission of the due performance of the MSP or any part thereof or of the accuracy of any claim or demand made by the MSP or of additional varied Services having been ordered by the Purchaser nor shall any other certificate conclude or prejudice any of the powers of the Purchaser.

13.30.3 Cessation of Procuring Entity's Liability

After the issue of Completion Certificate, the Purchaser shall not be liable to the MSP for any matter arising out of or in connection with the contract for the delivery of the Services, unless the MSP shall have claimed in writing in respect thereof before the issue of the Completion Certificate for service in Contract.

13.30.4 Unfulfilled Obligations

Notwithstanding the issue of Completion Certificate for service, the MSP and the Purchaser shall remain liable for the fulfilment of any obligation incurred under the provision of the contract before the issue of the Completion Certificate for services, which remains unperformed at the time such certificate is issued. The contract shall be deemed to remain in force till the nature and extent of any such obligations are determined. The Purchaser's right to withhold payments, invoke the Performance Bank Guarantee, or recover losses shall survive until all such unfulfilled obligations are discharged to its satisfaction.

13.30.5 Final Payment

The MSP shall submit a Final bill on the Purchaser's certificate of completion regarding the services. The Final payment shall be made as per the following calculations to the MSP after receiving a clear "No Claim Certificate" signed from it:

(a) the total quantity of service executed by the MSP up to the completion date based on the Purchaser's or its representative's certified measurements.

(b) priced at the rates in the Price Schedule in the contract and for extra works under change management process.

(c) necessary adjustment for any payments already made or retained

(d) any deduction which may be made under the contract,

(e) a complete account of all claims MSP may have on the Purchaser, and the Purchaser gave a certificate in writing that such claims are correct.

13.30.6 No Claim Certificate and Release of Contract Securities:

The MSP shall submit a 'No-claim certificate' to the Purchaser in such form as shall be required by the Purchaser after the Services are finally admeasured and before the final payment/ PBG are released. The Purchaser shall release the contractual securities without any interest if no outstanding obligation, asset, or payments are due from the MSP. The MSP shall not be entitled to

make any claim whatsoever against the Purchaser under or arising out of this Contract, nor shall the Purchaser entertain or consider any such claim, if made by the MSP, after he/she shall have signed a "No Claim" Certificate in favour of the Purchaser. The MSP shall be debarred from disputing the correctness of the items covered by the "No Claim" Certificate or demanding a clearance to arbitration in respect thereof.

13.30.7 Post Payment Audit:

Notwithstanding the issue of Completion Certificate and release of final Payment, the Purchaser reserves the right to carry out within 180 days of such completion/ final payment, a post-payment audit and/ or technical examination of the Services and the final bill including all supporting vouchers, abstracts etc. If any over-payment to the MSP is discovered due to such examination, the Purchaser shall claim such amount from the MSP.

13.30.8 Signature on Receipts for Amounts:

Every receipt for money, which may become payable, or for any security which may become transferable to the MSP, the contract, shall if signed in the partnership name by any one of the partners of a MSP's firm, be a suitable and sufficient discharge to the Purchaser in respect of the sums of money or security purported to be acknowledged thereby. In the event of death of any MSP contractor, partners during the pendency of the contract, every receipt by anyone of the surviving constituents shall be suitable and sufficient discharge as aforesaid. Nothing in this Clause shall be deemed to prejudice or effect any claim that the Purchaser may hereafter have against the legal representative regarding any breach of any contract conditions by any MSP partner/member so dying. Nothing in this clause shall be deemed to prejudice or effect the respective rights or obligations of the MSP partners/ members and the legal representatives of any deceased MSP partners/ members.

13.30.9 Defects Liability Period

(a) the MSP warrants that the Services have been delivered as per description, scope/ quantum, performance standards and quality outlined in the contract. This Defect Liability shall be in effect for a period stipulated in the contract (or if not specified for ninety (90) days) from completing the Services. The contract shall be deemed alive during this period, even if final payment and/ or Performance Guarantee has been released.

(b) During the Defects Liability Period, upon discovering any deficiencies in outputs/ outcomes attributable to a shortfall in scope/ quantum, performance standards and quality of the performed Services, the Purchaser shall give written notice to the MSP.

(c) Upon receiving such notice, the MSP shall, within 21 days (or within any other period, if stipulated in the contract), expeditiously remedy or reperform the Services or parts thereof, free of cost, at the site.

(d) If the MSP, having been notified, fails to rectify/ replace the defect(s) within 21 days (or within any other period, if stipulated in the contract), it shall amount to breach of Contract, and the Purchaser shall proceed to take such remedial action(s) as deemed fit by it as detailed.

(e) The Purchaser may, at its sole discretion, retain up to ten percent (10%) of the final payable amount or continue to hold the Performance Bank Guarantee until successful completion of the Defects Liability Period.

Failure by the MSP to remedy or reperform within the stipulated period shall entitle the Purchaser to

(i) carry out the work at the MSP's cost,

(ii) recover liquidated damages as per the contract, and/or
(iii) terminate the contract for breach without prejudice to other remedies.

14. Minimum Bill of Quantity (BOQ)

14.1 Platforms and Components for GSOC

TABLE 14: BOQ - PLATFORMS AND COMPONENTS FOR GSOC

S. No.	Description	Total Quantity (H/W + S/W) to be supplied	Deployment Location
1	Security Incident Event Management (SIEM) with at least 7 Lakh EPS extendable upto 10 Lakh EPS	1 (Active) + 1 (passive as failover for primary site)	Delhi (Primary site) and (DR Site)
2	Security Orchestration Automation Response (SOAR)	1 (Active) + 1 (passive)	Delhi (Primary site) and (DR Site in passive mode)
3	Information Technology Services Management (ITSM) i.e. Central Ticketing Solution	1 (Active) + 1 (passive as failover for primary site)	Delhi (Primary site) and (DR Site in passive mode)
4	Threat Intelligence Platform (TIP)	2	Delhi (Primary site) and (DR Site in passive mode)
5	Attack Surface Management Platform (Unlimited cloud-based license)	1	Cloud based solution
6	Attack Simulation Platform	1	Delhi-1
7	Security Testing Platform	3	Delhi-2 Chennai-1
8	Dynamic Application Security Testing (DAST) Tools.	60	Delhi
9	Threat Intelligence (IP & Web Reputation Feeds)	1	Delhi From different OEMs as per requirement in Annex 5 / Annex 10.
10	Threat Intelligence (IOC Feeds)	1	Delhi From different OEMs as per requirement in Annex 5 / Annex 10.
11	Threat Intelligence (Deep Web, Dark Web, Social-media & OSINT Feeds)	1	Delhi From different OEMs as per requirement in Annex 5 / Annex 10

12	Incident Response Retainer service from a security OEM	1	Across India, On demand basis
13	Digital Forensic Incident Response Tool	2	Delhi
14	Portable Log Analyzer	8	Delhi-6 Chennai-2
15	Forensic Disk Imager with hardware write blocker along with required forensic hardware toolkits.	Minimum 12	Delhi-10 Chennai-2
16	Magnetic Media Degausser& Secure Drive Eraser	Minimum 8	Delhi-6 Chennai-2
17	Static & Dynamic Analysis Sandbox from 3 OEMs	2	Delhi-1 Chennai-1
18	Digital Forensic Suite	3	Delhi -2 Chennai -1
19	Mobile Forensic Suite	3	Delhi -2 Chennai -1
20	Memory Forensic Solution	3	Delhi-2 Chennai-1
21	Mac Forensics Suite	3	Delhi-2 Chennai-1
22	Cloud Forensic Solution	3	Delhi-2 Chennai-1
23	Steganography Forensic Solution	3	Delhi-2 Chennai-1
24	eDiscovery Forensic Data Analytics Platform	3	Delhi-2 Chennai-1
25	Network Forensics	3	Delhi-2 Chennai-1
26	Data Recovery tools	4	Delhi-3 Chennai-1
27	SOC Logistics Tools and standalone storage systems for system Image storage.	As per Annex-17	As per requirement at various locations
28	SOC and Forensics work stations, laptops etc.	18	

29	Forensic Logistics Tools (Hackone RFOne Bundle, Flipper Zero, Proxmark3, Rubber Ducky etc.)	6	Delhi-4 Chennai-2
30	Laying of Inter building fiber cable between adjacent buildings for connecting GSOC with NICNET/NKN.	1	
31	Supply and installation of Active LAN components (Router, switches, access points etc.) for Approx. 1200 nodes at GSOC LAN.	Router (2) L3 Switches (2) L2 Switches (30) Access Points (15)	Quantities given are minimum quantities which may vary as per actual requirement of the GSOC Site.
32	Hardware appliances / solutions for security of the supplied SOC solution(Indicative): (e) NGFW (f) WAF (g) Server Load Balancer (h) SSL Off Loader (SSLO) (i) Proxy etc.	Each solution to be provided with minimum redundancy of N+1	Delhi – 1 DR Site -1
33	Governance Risk & Compliance Solution	1 + 1 (passive as failover for primary site)	Delhi – 1 (Primary site) Hyderabad – 1 (DR Site)

Note:

(a) The hardware specified above is minimum required as per the understanding of the Purchaser. The MSP shall have the discretion to increase the quantity and/or capacity of hardware and related components as deemed necessary to meet the functional, performance, and Service Level Agreement (SLA) obligations under the Contract, without any additional financial liability to the Purchaser.

(b) All supplied components shall be delivered with complete features, functionalities, and requisite licences, without any restrictions or limitations that may hinder achievement of the agreed SLA. The MSP shall ensure that each supplied solution is fully operational and includes, at no additional cost to the Purchaser, all required hardware, compute, storage, networking equipment, operating systems, software licences, and any other Information and Communication Technology (ICT) equipment necessary for end-to-end delivery of the solution.

(c) All solutions provided shall be inherently scalable, designed for high availability, and deployed with a minimum redundancy level of N+1 (except for cloud-based solutions). The MSP shall ensure that the deployed architecture is capable of sustaining uninterrupted full operational functionality in the event of a component failure, in line with best industry practices.

14.2 Minimum Operational Manpower

TABLE 15: BOQ- MINIMUM OPERATIONAL MANPOWER

Sr No.	Resource Type/ Resource Profile	Quantity
1	Project Manager	1
2	SOC Analyst	16
3	Malware Analyst	12
4	Security Breach Investigation Specialist	12
5	Log Analysis & Threat Hunting Specialist	20
6	SIEM Administrator	11
7	SOAR Administrator	6
8	Ticketing Platform Administrator	6
9	Linux Expert	8
10	Windows Expert	8
11	MacOS Expert	7
12	Office Assistant/ Logistics manpower	8
13	Windows Forensic Expert	3
14	Linux Forensic Expert	3
15	MacOS Forensic Expert	3
16	Memory Forensic Expert	3
17	Android Forensic Expert	3
18	iOS Forensic Expert	3
19	Data Analytics Expert	3
20	AI Engineer	2
21	ISO 20000, 27001 and CMM Experts	At least 1 each
22	Full Stack Developers	2
23	Governance, Risk & Compliance Experts (Mix of Functional experts, Technical Experts and support personnel)	6
	Total	**149**

The numbers provided are indicative for the minimum requirements. The MSP is free to provide additional manpower as required to support the operations and maintain the SLAs. The manpower is required during the entire contract period, or any extension thereof post Go-Live. The manpower shall work in shifts as per **Annex 16**. The shifts should be overlapping with minimum one hour of handover period between the shift change. The manpower not working 24*7 shall remain available to work anytime and during holidays also as per project requirements.

14.2.1 Core Team - Functions and composition:

The MSP shall establish a core team consisting of 1 Team Lead and 10 number of team members as per details given in Annex 16, and as per same applicable SLA's. The Core team shall work in coordination with the other SOC teams and cyber security teams of various ministries and departments. The core team shall perform the following, but not limited to, activities:

(a) Assist the cybersecurity teams of various ministries and departments and shall coordinate with other SOC teams in handling their respective cyber security incidents and preparation of RCAs.
(b) Shall conduct forensic analysis of images obtained from various ministries and departments and shall prepare detailed reports of forensic analysis.
(c) Shall perform Vulnerability Assessment (VA) of servers/VMs/Containers and applications hosted at Purchaser's Data Centres.
(d) Shall visit various ministries and departments as per requirement for onsite resolution of cyber security incidents based on tickets assigned to the core team.
(e) Shall conduct cybersecurity trainings of Deputy CISOs of various organisations.

15. Technical Specifications

TABLE 16: TECHNICAL SPECIFICATIONS

SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) SOLUTION		
S.No.	**Purchaser's Requirement**	**Compliance (Y/N)**
Architecture & Sizing		
1	Solution Should support both centralized and distributed deployment of the SIEM Platform across multiple geo-graphical locations, with each instance of the solution be capable of operating independently and allow - cross location querying of logs, threat hunting, reporting, alerting, exporting...etc.	
2	Solution Should be deployed in high availability mode, with at least N+1 redundancy, across 2 geo-locations (Delhi & Hyderabad)	
3	Solution should be highly scalable supporting the handling of more than 50 petabytes of logs	
4	Solution management should be automated, with end-to-end orchestration for dynamic scaling of instances, clusters, patching, upgrading...etc., depending on the pre-defined threshold values & conditions.	
5	Solution should support the following deployment models: • Standalone hardware • Virtual machines • Private & Public Cloud • Container	
6	Solution should have a modular architecture with separate collection, queuing, streaming, parsing-correlation, storage and archival layers, with each layer operating independently and perform their functions, in case of any isolated failure restricted to a specific layer.	
7	Solution Should be deployed on-premise, without any dependency on internet or cloud hosted resource.	
8	License of the solution should be perpetual and the solution should function with all offered features, post expiry of the license, except new updates/functionalities offered after expiry of license.	
9	Solution should be offered with a complete enterprise license, without any limitations, including limitations on volume of logs, log events per day, size of infrastructure…etc.	
10	Solution should be offered with all necessary infrastructure and licenses, including hardware (servers, network, storage, security), software, operating system, databases, virtualization, containerization, cables, orchestration…etc., as applicable. NIC shall provide only hosting space in the data centre for the deployment.	
11	The hardware solution should be sized for processing 4 Petabytes of Logs, with **10 lakhs EPS (across all layers)** on day one	

12	Overall sizing and architecture of the solution should take into consideration high availability, dynamic scalability, zero data loss, optimal network utilization across the network where the log sources are located.	
13	Complete list of log sources which are supported by the proposed solution, out of the box, should be provided as a part of this bid.	
14	Bidder shall be responsible for ensuring that the implemented solution complies with the specifications detailed in the latest versions of ISO 27001, ISO 27002, MHA Guidelines, CERT-IN's advisory & guidelines, NIC's security policies & guidelines, IT ACT 2000, DPDP Act, etc. and any other law of the land applicable for NIC.	
Log Collection, Processing & Integration		
1.	The solution should be able to handle a sudden burst of 1.5 times the overall EPS capacity at any given point of time without resulting in drop or queuing of the events.	
2.	Solution should support both agent based and agent less collection of logs from any IP device/source. The solution should support various log collection methods, including but not limited to the following: • Syslog • Flat File Logs • OS Logs • FTP, S/FTP, SNMP, ODBC, SDEE, WMI, JDBC etc. • Netflow, IPFIX • Any other source which generates electronic logs	
3.	Solution should support deployment of log aggregators across multiple geo-graphical locations, which can collect logs from multiple sources and cache the logs locally before streaming it to the central log server.	
4.	Solution should support encryption of logs at rest and while in transit. This includes encryption of logs which are in transit within the different components of the SIEM.	
5.	Solution should support queueing of logs across all layers in case of non-availability of the next subsequent layer in the log ingestion pipeline.	
6.	Solution shall ensure that original logs are not tampered in any manner right from log collection to log processing and log storage.	
7.	Solution should support export of raw logs, without any enrichment/parsing at any given point of time.	
8.	Solution should have in-built parsers for parsing logs from products of all major OEMs & open-source solutions – including but not limited to the following: • Operating System • Webserver • Application server • Database • Network devices • Security devices • Endpoint solutions	

	• Security solutions • Endpoint management solutions • Wireless devices • Virtualization software • Cloud solutions • Identity and Access Management solutions	
9.	Solution should support the functionality for development of custom parsers by Users, using a low code no code feature. During the duration of the contract, the Bidder shall ensure that parsers are made available for all unique log sources of NIC.	
10.	Solution should have a robust data collection engine with real-time pipelining capabilities to dynamically unify data from disparate sources and normalize the data to different destinations including, real-time streaming of collected raw logs to multiple destinations (including other 3rd party SIEM, syslog server, custom applications etc.) before parsing of logs.	
11.	Solution should support direct fetching of logs through JDBC/ODBC connectors from supported log sources.	
12.	Solution should have necessary fail-back mechanisms in-built to ensure that no log is lost during transit or while at rest.	
13.	Solution should support out of the box integration with various proprietary and open-source Threat intelligence sources and bi-directional integration with Threat intelligence Platforms (TIP), including the TIP Solution proposed in this bid.	
14.	Solution should support out of the box parsing for threat intelligence in STIX 1.x, STIX 2.x, XML, JSON, Open IOC and other industry standard formats for threat intelligence.	
15.	Solution should support ingestion and parsing of logs or data in CSV, text or any other raw file formats	
16.	Solution should support out of the box bi-directional integration with all leading SOAR solutions, including the SOAR solution supplied as a part of this bid.	
17.	Solution should parse all the fields in the ingested logs and should not leave any field unparsed.	
18.	SIEM Solution should support out of the box integration with all the other solutions proposed in this bid.	
19.	Solution should support log compression without altering the content and maintain a compression ratio of at least 10:1 or better	
20.	Solution should support log normalization, which shall convert each log into a particular schema and categorize the fields consistently across all log sources ingested in to the SIEM solution.	
21.	Solution should include features to export data, provide access to the external data warehouse, Visualization tools and support external analytics tools.	
22.	Solution should be able to collect raw telemetry data from various IP based sources and create automated analytics dashboards, alerts for the telemetry data.	
Correlation and Analytics		

1	Solution should support querying of ingested data using various Search operators including but not limited to the following: • Comparison operators (equal to, not equal to, less than, greater than, less than or equal to, greater than or equal to) • Logical Operators (AND, OR, NOT) • Wildcard Operators • Range Operators • String Matching Operators (LIKE, CONTAINS, NOCASE) • Field Operators (search for a specific field value) • Grouping Operators (group parts of query) • Filters based on all available fields in the log post enrichment	
2	Solution should support nested queries, i.e., embedding one query within another query	
3	Solution should support regular expression-based search and time range-based searching of logs	
4	Solution should support multi-source correlation of logs through user defined and automated queries, alerts.	
5	Solution should deliver a query performance of less than 10 seconds for fetching and displaying the results of a correlation query executed over a data of 1 petabyte.	
6	Solution should support out of the box analytics and security dashboards for various log sources	
7	Solution should provide a variety of dashboard customizations including but not limited to the following: • Table • Bar Graph • Line Graph • Histogram • Pie Chart • Geographical Map (world view, continent view, country view, state view)	
8	Solution should provide various use case specific dashboards out of the box including but not limited to the following: • Attack Analysis • Timeline View of threats • Security Posture overview • Network anomaly detection • User behavior anomaly detection • Security Alerts • Compliance view • Audit log view • SIEM Health • Log Source Health • Log streaming status and volume	

9	Solution should automatically detect and alert in case of any disruption in logs streaming from a particular source, log collector or any other component of the SIEM solution.	
10	Solution must allow users to create objects such as filters or search queries that can be saved and reused for the ease of operations	
11	Solution should provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.	
12	Solution should support drill-down from all parameters in the alerts and dashboards to give a detailed view of raw and enriched data behind the parameter.	
13	Solution should support real-time as well as historical correlation of events. This includes the techniques used for correlation of different events across different monitored devices.	
14	Solution should provide real time data monitoring, retrospective data analysis along with visualization.	
15	Solution must provide a workspace for investigations and threat hunting adding alerts from multiple log sources to a Timeline view to facilitate advanced investigations.	
16	Solution must provide hunting capabilities through data of the scale of petabytes to spot long-dormant threats searching historical data for the IoCs of newly discovered exploits.	
17	The solution should offer the flexibility to develop customized correlation rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources on multiple parameters (like Hosts, Geographies, recurring activities) including OS platforms, network & security devices, applications etc. as well as threat feeds obtained from different sources	
Dashboard, Alerting & Reporting		
1	Solution should provide various use case specific dashboards out of the box including but not limited to the following: • Attack Analysis • Timeline View of threats • Security Posture overview • Network anomaly detection • User behavior anomaly detection • Security Alerts • Compliance view • Audit log view • SIEM Health • Log Source Health • Log streaming status and volume	
2	Solution should support mapping of alerts, correlation rules/use cases with MITRE ATT&CK Framework and Cyber Kill Chain for tactics and techniques to get better visibility of incidents, with automatic Severity /Risk Scoring.	

3	Solution should be able to combine multiple related alerts into a single incident	
4	The solution should provide reporting engine for out-of- box reports, customized reports, ability to schedule reports, compliance reports, historical trend reports with the various options including but not limited to the following: 1. Detailed reports of non-compliant activities and policy violations in the network. 2. Historical system-based, user-based and network-based event data for compliance auditing. 3. Information about threat response and mitigation measures carried out to prevent attacks. 4. The solution must provide reporting engine for out-of-box reports, customized reports, ability to schedule reports, compliance reports, historical trend reports etc. 5. The system should allow scheduling reports. 6. Reports should be available in pdf and csv format.	
5	The solution must provide near real time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms such as email, SMS, voice call etc. based on agreed policies.	
6	Solution should have capabilities to receive contextual alert notifications when anomalies are detected that meet certain conditions using case management or connect alerts to actions by using built-in integrations for SOAR and email for workflow management.	
7	Bidder should configure dashboard to show the status of all the solutions deployed as part of this bid, including availability, bandwidth consumed, system resources consumed (including database usage) , SLA Compliance and other parameters as per the tender and NIC's requirements.	
8	The solution should generate alerts at different level of granularities based on a variety of parameters including threshold breach, trend-based conditions and complex patterns, such as brute force attacks, backdoors, Trojans connections, C&C, Emerging Threats and fraud scenarios etc.	
Retention, Archival & Export		
1	Solution should support user defined policy-based log retention for each log source and log source groups. Necessary sizing should be made for retention as per NIC's policy (currently 2 years).	
2	Solution should support user defined policy-based log archival to various storage like SAN, NAS and Object Storage.	
3	Solution should support running search queries on archived logs and allow export of selected logs (based on user defined filters/query) from the archived logs.	
4	Solution should have a Log File Integrity Check mechanism, which must calculate a message digest / hash, for each file and help in storing the message digest/hash securely to ensure that changes to archived logs are detected.	

5	Solution should retain years of actionable data to uncover latent threats and markers of newly uncovered exploits	
6	Solution should be able to export data in various formats to be consumed by other applications / purposes, like Excel/CSV Files, JSON Files, Email, PDF, Reports etc. The solution should provide an API based mechanism to act as a data source to be consumed by various applications.	
7	Solution should support export of huge chunks of raw and enriched logs on a petabyte scale.	
Artificial Intelligence (AI) Features		
1	Solution should use the latest advancements in Artificial Intelligence (machine learning, Generative AI etc.) and provide insights, analytics, alerts based on the AI models.	
2	Solution should have capabilities to automatically learn what activities are normal using Machine learning and identify anomalies which deviate from the normal behavior.	
3	Solution should have in-built algorithms for historical data analysis, profiling and threat discovery.	
4	Solution should leverage in-built AI models for various use cases including but not limited to the following: a) password spraying, user enumeration, or brute force activity b) account takeover or credentialed access. c) unauthorized user activity during non-business hours. d) Lateral movement when a compromised account is used e) unusual user name in the authentication logs (rare Users) f) suspicious login activity g) rare and unusual errors h) anomalous network activity i) command-and-control, persistence mechanism, or data exfiltration activity. j) unauthorized software, malware, or persistence mechanisms k) Un-usual network Destination: communicate with command-and-control (C2) l) Denial-of-service attacks or traffic floods m) unauthorized software, malware, or persistence mechanisms. n) rare user: credentialed access or lateral movement. o) Credential Harvesting: anomalous access to the metadata service by an unusual user p) Un-usual user context switches can be due to privilege escalation. q) Unusual RDP (remote desktop protocol) user logins	
Administration and Audit Trail		
1	Solution should maintain a complete audit trail of all activities performed on the SIEM Solution.	
2	Solution should provide a feature to view, query, create alert, create reports, create dashboards on the complete audit trail of the SIEM solution.	

3	Any attempts to tamper the log data residing on the SIEM solution or its archival, should be automatically detected and blocked.	
4	Solution should provide a central management console, offering a single pane of view for the monitoring, management and administration of all components related to the offered solution.	
5	Solution should offer a Role Based Access Control (RBAC), with Multi-Factor Authentication (MFA) for all users.	
6	Solution should support integration with NIC's and 3rd party's Identity & Access solutions using standard protocols like SAML, OAuth and OIDC.	
7	All access to the solution's web console should be done over TLS	
8	Solution should support creation of multiple user specific dashboards based on RBAC and allow access to the raw logs based on the user's role.	
9	Solution should support customization of RBAC for each user, with granular level access controls on management, administration, dashboard, alerts, investigation, threat hunting, reports, export of logs etc.	
10	The RBAC of the solution should support both role based and log attribute-based access control	

Note: High level architecture diagram of the proposed solution along with the proposed hardware, software stack should be provided as a part of the bid.

Security Orchestration Automation and Response Solution (SOAR)		
S.No	**Purchaser's Requirement**	**Compliance (Y/N)**
Architecture & Sizing		
1	Solution Should be deployed in high availability mode, with atleast N+1 redundancy, across 2 geo-locations (Delhi & Hyderabad)	
2	Solution management should be automated, with end-to-end orchestration for dynamic scaling of instances, clusters, patching, upgrading...etc., depending on the pre-defined threshold values & conditions.	
3	Solution should support the following deployment models: • Standalone hardware • Virtual machines • Private & Public Cloud • Container	
4	Solution Should be deployed on-premise, without any dependency on internet or cloud hosted resource.	
5	License of the solution should be perpetual and the solution should function with all offered features, post expiry of the license, except new updates/functionalities offered after expiry of license.	
6	Solution should be sized (in terms of hardware and software) to handle the alerts, incidents and other orchestration activities to be processed through other solutions proposed in this bid.	
7	Solution should be offered with all necessary infrastructure and licenses, including hardware (servers, network, storage, security), software, operating system,	

	databases, virtualization, containerization, cables, orchestration…etc., as applicable. NIC shall provide only hosting space in the data centre for the deployment.	
8	Solution should be offered with an enterprise license, without any limitations.	
9	Solution should be able to handle unlimited volume of cases generated through the SOAR platform.	
10	Complete list of sources (along with make and model) which are supported with all available actions, by the proposed SOAR solution, out of the box, should be provided as a part of this bid.	
11	Solution should consume data from all integrated sources and should be able to perform all investigative and remediation actions, based on the consumed data.	
12	Solution should securely store credentials for use with integration instances.	
13	Bidder shall be responsible for ensuring that the implemented solution complies with the specifications detailed in the latest versions of ISO 27001, ISO 27002, MHA Guidelines, CERT-IN's advisory & guidelines, NIC's security policies & guidelines, IT ACT 2000, DPDP Act, etc. and any other law of the land applicable for NIC.	
Integrations & Playbook		
1	Solution should provide out of the box integration with all the solutions proposed as a part of this bid, the integration should involve automation and orchestration of all actions available in the proposed solutions.	
2	Solution should provide seamless out of the box integration with NIC's ICT Infrastructure, which includes but not limited to the following: • Servers • Storage & Backup Devices • Storage & Backup Applications/Software • Network Devices • Security Devices & Applications • Operating System • Endpoint Systems • Endpoint and Server Security Solutions • Virtualization and Cloud solutions • SIEM • Threat Intelligence Platform • DNS • Email Application • Helpdesk / Ticketing Solution • LDAP, PIM, PAM, RADIUS, TACACS, Single Sign On • Forensic Solutions	
3	Solution should support creation and execution of thousands of unique playbooks parallelly and should maintain the versioning of the playbooks.	
4	Solution should have more than 100 playbook templates out of the box for various use cases, covering the NIC's ICT Infrastructure mentioned in 2.2	

5	Solution should be able to automatically extract emails and the enclosed attachments, including URLs from email body, email fields like from, to, bcc, subject, attachment type, attachment size, total number of recipients...etc, and Should allow playbooks creation with various filters and conditions as per the aforementioned email fields.	
6	Solution should support creation of automated tasks, conditional tasks and manual tasks in playbooks and trigger each task as per the predefined event triggers.	
7	Solution should support step-wise debugging of running playbooks.	
8	Solution should support scheduling of playbooks at pre-defined time intervals	
9	Solution should support a provision to pass parameters to upstream/downstream task within a playbook	
10	Solution should support embedding of scripts (like java, js, python/ruby, bash, shell scripts etc.) in playbooks	
11	Solution should support inclusion of decision paths option in playbook workflow for manual intervention or approval, to proceed ahead with a pre-defined action flow.	
12	Solution should provide a GUI based no-code low code feature in the SOAR console for easily building playbooks, workflows and tasks.	
13	Solution should support automation of all actions that are available at a particular source, which is integrated with the SOAR.	
14	Solution should support statistical correlation on historical incidents such as frequency of incident, action taken, remediation remarks, analyst closure remarks, asset details, asset owner, playbook assigned etc. on similar alerts to provide incident context to SOC analyst.	
15	Solution should learn from previous incidents and accordingly provide recommendations to the analyst.	
16	Solution should have adequate number of out of the box workflows and pre-built playbooks.	
17	Solution should be capable to assign playbooks within playbooks.	
18	Solution should provide automated detailed post incident documentation about all the actions taken, root cause, controls implemented, collaborative actions/chats etc	
19	Solution should offer a dedicated SOAR test lab workspace, empowering users to experiment, validate, and enhance automated security workflows in a controlled testing environment	
20	Solution should support adding of new product integrations and custom integrations without any additional cost to NIC.	
21	Should support multiple methods of data ingestion, like APIs, syslog, db connections, email and online forms. In addition to this, it should also support data standards such as CEF, Open IOC, STIX/TAXII, etc.	
22	Solution should integrate with other products/sources using any of the standard protocols and interfaces including REST API, SOAP, SSH/CLI interface, and custom APIs.	
23	Solution should support email or text notifications, along with functionality to	

	email comprehensive periodic reports and dashboards.	
24	Solution should provide necessary integration with the IT/cybersecurity systems for keeping the forensics artifacts from the integrated sources of the incident before taking	
Dashboard, Reporting		
1	Solution should maintain an internal repository of various IOCs and tag the IOCs along with their contextual data obtained from various sources.	
2	Solution should provide pre-defined dashboards for measurements of KPIs including MTTR, MTTD and total recorded incidents.	
3	Solution should provide custom reporting through csv, doc and PDF with logo as desired by NIC	
4	Solution should provide a customizable widget-based dashboard	
5	Solution should support contribution of external users to an incident via email, chat, ticket etc.	
6	Solution should have an internal Knowledge base repository, which users can refer to for searching the solutions to various cases.	
7	The solution should provide management summary dashboard, information like statistics about incidents, effectiveness in terms of cyber incidents handling time and so on.	
8	The solution should provide customisation of dashboard based on type of incidents/ user preferences/ user group preferences.	
9	The Solution's playbooks should support: - nested playbooks to deploy multiple automations as part of a single use case - conditional decision trees - user surveys for input from various stake holders in the use case/reviews - time based actions - escalation actions	
Automation and Response		
1	Solution should provide a simple, comprehensive, fully automated approach to detect and stop the threats that matter, for on-premise deployments from internal & external attacks on the NIA IT and OT system.	
2	solution should support both human and machine-based automation for various tasks related to security investigations.	
3	Solution should be configured with the use cases with automation for response to the threats which includes but not limited to the following on day one : • Blacklisted IP Communication • APT Attack (min. 10 APT Types) • Possible Penetration Testing Activity • Connection to Known Malicious Actor in Published Host List • DDOS Attack • Vulnerability scan detection • Phishing detection • Brute force attack	

	• Malware /threat activity monitoring • Ransomware • Buffer Overflow attacks • Port & vulnerability Scans • Worm/virus outbreak • File access failures • Unauthorized server/service restarts • Unauthorized changes to firewall rules Cross site scripting	
4	Solution should have built in reusable playbooks for well- known Incident types (Phishing, Malware, IOC Hunt).	
5	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks. Solution should allow a single playbook to have Automated and Manual Tasks within the same playbook.	
6	Solution should allow a complete playbook to be run automatically or manually and list out any exceptions.	
7	The solution must support incident enrichment using IOCs and Indicators of Attack (IOA) received from Threat Intel feeds and unstructured threat intelligence received over email, file, etc. The solution should automatically map related current and historical incidents with common IOCs to identify nation state threat actors.	
8	The solution should auto-document the timeline of a security event along with all the investigation actions.	
9	The solution should prioritize and assign cases based on user defined logic.	
10	The solution should normalize data coming from various sources which are integrated with the SOAR platform.	
11	The solution should support creation, tracking and setting reminder of user-defined SLAs.	
12	The solution must be able to aggregate information from past investigations on the ticket (such as link to a data source, comments, involved analyst, etc.).	
Incident Management		
1	Solution should provide in-built incident/case management feature and support assigning of incident to a User.	
2	Solution should support highlighting of active incidents to quickly identify and access them.	
3	Solution should support visual mapping of an incident, its elements and correlated investigation entities, and the progression path of the incident.	
4	Solution should support external users to contribute to an incident via email, message etc.	
5	System should allow more than 1 playbook to run on any incident. All execution details should be retained and available for the reference.	
6	Solution should allow differentiation between alerts and incidents (incidents	

	could be made of multiple alerts.)	
7	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution.	
8	The system should support creation of an incident based on an email input (e.g. analyze all emails from a dedicated phishing mailbox)	
9	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response.	
Administration & Audit Trail		
1	Solution should maintain a complete audit trail of all activities performed on the SOAR Solution.	
2	Solution should maintain a complete audit trail of all activities performed by the SOAR Solution.	
3	Solution should provide a central management console, offering a single pane of view for the monitoring, management and administration of all components related to the offered solution.	
4	Solution should offer a Role Based Access Control (RBAC), with Multi-Factor Authentication (MFA) for all users.	
5	Solution should support integration with NIC's and 3rd party's Identity & Access solutions using standard protocols like SAML, OAuth and OIDC.	
6	All access to the solution's web console should be done over TLS	
7	Solution should support creation of multiple user specific dashboards based on RBAC and allow access to the playbooks and actions based on the user's role.	
8	Solution should support customization of RBAC for each user, with granular level access controls on management, administration, dashboard, alerts, investigation, threat hunting, reports, playbooks, actions...etc.	
9	Solution should be able to store historical data related to an incidents/cases/playbooks for a minimum period of 2 years.	

Threat Intelligence Platform (TIP)		
S.No	**Purchaser's Requirement**	**Compliance (Y/N)**
Architecture & Sizing		
1	Solution Should be deployed on-premise in high availability mode, with atleast N+1 redundancy, across 2 geo-locations (Delhi & Hyderabad)	
2	Solution management should be automated, with end-to-end orchestration for dynamic scaling of instances, clusters, patching, upgrading...etc., depending on the pre-defined threshold values & conditions.	
3	Solution should support the following deployment models: • Standalone hardware • Virtual machines • Private & Public Cloud	

	• Container	
4	Solution Should be deployed on-premise, without any dependency on internet or cloud hosted resource (except for receiving threat intelligence from 3rd party sources).	
5	License of the solution should be perpetual and the solution should function with all offered features, post expiry of the license, except new updates/functionalities offered after expiry of license.	
6	Solution should be sized (in terms of hardware and software) to handle the threat intelligence containing atleast 5 billion unique Indicators of Compromise (IOCs), along with their contextual information	
7	Solution should be offered with all necessary infrastructure and licenses, including hardware (servers, network, storage, security), software, operating system, databases, virtualization, containerization, cables, orchestration…etc., as applicable. NIC shall provide only hosting space in the data centre for the deployment.	
8	Solution should be offered with an enterprise license, without any limitations.	
9	Solution should be able to handle unlimited volume of threat intelligence feeds to be received from various sources	
10	Complete list of threat intelligence sources (along with make and model) which are supported out of the box by the proposed TIP solution, should be provided as a part of this bid.	
11	Bidder shall be responsible for ensuring that the implemented solution complies with the specifications detailed in the latest versions of ISO 27001, ISO 27002, MHA Guidelines, CERT-IN's advisory & guidelines, NIC's security policies & guidelines, IT ACT 2000, DPDP Act, etc. and any other law of the land applicable for NIC.	
Features & Functionalities		
1	Solution should allow ingestion and publishing of threat intel from and to many sources simultaneously.	
2	Solution should perform de-duplication of IOCs receives from multiple threat intel sources	
3	Solution should allow manual and API based upload of custom threat intel feeds by the user in CSV & JSON format	
4	Solution should provide automation and workflow capability, including a threat library or database, which allows for easy searching, manipulation and enrichment of data	
5	Solution should allow custom tagging, scoring of indicators	
6	Solution should be able to dynamically adjust scores of indicators based on external and internal data sources including SIEM, Ticketing system, Vulnerability information…etc.	
7	Solution should support all data models and standards within a single searchable repository.	
8	Solution should parse and include all additional attributes and contexts provided by threat intel sources. These additional attributes and contexts should be made	

	available in the TIP console and appropriate searching, filtering, rules etc., should be made possible on these additional attributes and contexts.	
9	Solution should offer data enrichment options from other third parties like Virustotal, Maxmind, IBM Threat xchange, Alienvault OTX, MISP, CERT-IN's Threat Intel, OSINT.. etc.	
10	Solution should record the timestamp of all indicators for facilitating historical analysis, searching, reporting.	
11	Solution should provide categorization and analysis of adversaries	
12	Solution should provide an open exchange, API, SDK etc. for seamless integrations, import and export threat intel	
13	Solution should be able to Query, Import, Export and Manage threat intel via API	
14	Solution Should support STIX 1.x, STIX 2.x, MITRE ATT&CK	
15	Solution should be able to consume intel from multiple structured data format. It should support export of data through TAXII.	
16	Solution should support bi-directional integration with other TIPs, SIEM, SOAR, Ticketing System.	
17	Solution should support ingestion of 3rd party event feeds from various sources including open and proprietary sources like security blogs, news, articles, social media, intel providers…etc.	
18	Solution should support multiple custom playbooks runs through native integration with leading industry SOAR platforms.	
19	Solution should support keyword-based search, detailed reporting, analysis, filter-based searches.	
20	Solution should support multiple searches through operators including comparative operators, arithmetic operators, Boolean operators. Should provide facility to save searches.	
21	Solution should support user defined dashboards with role-based access.	
22	Solution should provide a Graphical user interface for carrying out investigations, where multiple teams and users can collaborate in real-time. The GUI should provide timelines, enrichments from 3rd parties.	
23	Solution Should support Custom risk score - capabilities: a. The platform should provide custom scoring capabilities based on parameters like TI source weightage, source score, etc. b. The platform should support customisation of enrichment algorithms like customisable policy for removing false positives, etc. c. The platform should be able to update (reduce or increase) risk score based on new Threat intel received, actions taken by users etc	
Administration & Audit Trail		
1	Solution should maintain a complete audit trail of all activities performed on the TIP Solution.	
2	Solution should provide a central management console, offering a single pane of view for the monitoring, management and administration of all components related to the offered solution.	

3	Solution should offer a Role Based Access Control (RBAC), with Multi-Factor Authentication (MFA) for all users.	
4	Solution should support integration with NIC's and 3rd party's Identity & Access solutions using standard protocols like SAML, OAuth and OIDC.	
5	All access to the solution's web console should be done over TLS	
6	Solution should support creation of multiple user specific dashboards based on RBAC and allow access to the Threat intel based on the user's role.	
7	Solution should support customization of RBAC for each user, with granular level access controls on management, administration, dashboard, threat hunting, reports, IOCs TTPs etc.	

ITSM		
S. No.	**Purchaser's Requirement**	**Complied Y/N**
	IT Service Management: (ITSM)	
1.	Solution shall help set up helpdesk and ticketing application where an operator shall raise a ticket based on the issue mentioned over the toll-free number, helpdesk email Id. Solution should be based on latest containerized auto scalable architecture.	
2.	The solution shall provide a centralized ticket management through a single web console, with support for 2000 users. The necessary hardware, software, licenses, storage, network equipment for handling the total capacity shall be provided from day one.	
3.	The solution shall support 500 users and 250 concurrent users from day one and shall scale up in increments of 100 users.	
4.	The solution should be able to integrate with various 3rd party solutions asked in the RFP via APIs	
5.	The solution shall integrate with Security Information Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Single Sign On (SSO), Email, Instant Messaging Apps of the Purchaser and SMS solutions provided by the Purchaser, through APIs.	
6.	Solution shall be scalable and shall be deployed in high availability mode with minimum N+1 redundancy at both DC and DR locations.	
7.	The OEM of the proposed solution should possess Quality certifications ISO 9001, Information security certificate ISO 27001, Application security certificate ISO 27034. Documentary proof must be provided at the time of submission.	
8.	Solution should be aligned with ITIL framework principles and certified with ITIL4 with minimum 11 processes like practices of Monitoring and Event Management, Incident Management, Service Request Management, Problem Management, Change Enablement, Release Management and Knowledge Management, CMDB. Etc. Certification copy to be submitted	
9.	Solution shall support creation of incident, service request, problem, change request tickets in accordance with the Information Technology Infrastructure	

ITSM		
S. No.	**Purchaser's Requirement**	**Complied Y/N**
	Library (ITIL4.0), ISO 20000 and ISO 27001 Standards. The solution must be certified	
10.	Solution shall provide web access of the helpdesk to the end users at User Department for raising the tickets through online portal	
11.	Helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.	
12.	Helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.	
13.	Solution should automatically provide suggested knowledge base articles based on Incident properties with no programming.	
14.	Solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming.	
15.	Solution must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system.	
16.	Helpdesk system shall provide grouping access on different security knowledge articles for different group of users.	
17.	Helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	
18.	Solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type.	
19.	Helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.	
20.	Solution should preferably have bundled reporting module so that third-party tools may not be required to customize reports	
21.	Solution should allow console users to create custom query-based reports on tickets and asset information, which is to be retrieved by the agents.	
22.	The ticketing database shall be retained for entire contract period. However, all logs of the ticketing platform for latest two months period shall be maintained in the provided ITSM solution. All logs shall be pushed/archived to the central logging solution of the Purchaser in real-time.	
23.	The solution shall provide complete SLA measurement modules with all features, which shall accept SLA metrics mentioned in this RFP as well as SLA metrics for other projects of the Purchaser for periodic SLA measurement and penalty calculation.	
24.	The SLA module shall integrate with the MIS solution of to be developed by the MSP.	

Attack Surface Management Platform		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1.	The solution can be either on-premises or cloud deployed, and it shall have frequent, high-quality internet indexing that is proprietary to the and have a means to ensure confidence in the results.	
2.	Solution generates its own scan data and does not rely on outside, third-party providers	
3.	Solution shall report the date/time of scan results, along with the GeoIP/Geo Location and Common Vulnerabilities and Exposures (CVE) data.	
4.	Solution shall rescan daily or multiple times in a day.	
5.	Solution shall cover at least +2500 ports for broad detection	
6.	Apart from open port checks the solution shall be able to perform full protocol handshake from day one	
7.	Solution shall crawl websites and report key information, including screenshots	
8.	Solution shall support API based integration for the use of data appearing in the UI.	
9.	Solution shall be able to identify a range of assets that are exposed to the global internet including the following: • Solution shall discover IP ranges • Solution shall discover Secure Sockets Layer (SSL) Certificates • Solution shall discover all possible subdomains	
10.	Solution shall be able to discover the Purchaser's assets (such as *.gov.in, *.nic.in) in the public cloud and enumerate the services running on those assets, along with the relevant context (including the registration information).	
11.	Solution shall provide visibility into asset sprawl across SSL certificate issuers, domain registrars, and cloud providers.	
12.	Solution shall highlight stale IP registration records for update and to reflect accurate ownership	
13.	Solution shall provide advance alert/forecast on the asset expirations including certificate and domain registrations for proactive maintenance.	
14.	The ability to apply tags to enable advanced data filtering, customized data, and to restrict or permit access to data	
15.	Solution shall identify risks across your assets, categorize the risk, and prioritize incidents for remediation	
16.	Solution shall offer remediation guidance for risks	
17.	Solution shall group alerts impacting the same service together automatically	

Attack Surface Management Platform		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
18.	Solution shall have the ability to automate common actions. This includes pulling in known asset owners, sending automated emails, or automatically creating tickets for investigation.	
19.	Solution shall have the ability to automatically remediate exposures. This shall include full resolution of the incident by reaching back via API and blocking the service at the port level.	
20.	The Solution shall provide in platform instructions on how to set up integrations and use Automated Remediation	
21.	The Solution shall provide a comprehensive score on the overall security posture of the Purchaser's assets	
22.	Solution shall have the ability to allow users to customize the weight of incidents in their overall risk score based on the organisations needs	
23.	Solution shall update the score based on what new incidents are found and shall not have delays in score updates	
24.	Ability to create or remove risk scoring rules	
25.	Ability to override the default system score and enter a score	
26.	The best practice method of risk scoring is a combination of Common Vulnerability Scoring System (CVSS) and Exploit Prediction Scoring System (EPSS) data	
27.	Solution shall have a method of explaining why an asset was attributed to the organisation, along with the evidence	
28.	Solution shall offer features that improve enterprise usability and function	
29.	Solution shall support single sign on through the Purchaser's Single Sign On (SSO) platform and any other 3rd party SSO solutions supporting Security Assertion Markup Language (SAML)	
30.	Solution shall allow export of any data from the platform	
31.	Solution shall allow creation of customized dashboards and reports based on the needs of the Purchaser	
32.	The Solution shall support scheduling of reports	
33.	Solution shall be robust to ensure secure login with Multi-Factor Authentication.	
34.	Solution shall support out of the box integrations with Ticketing tools (like JIRA, Service Now) to create new tickets based on incidents, identify the owner, and close out open ones	
35.	The Solution shall provide a centralized facility for installing, exchanging, and managing of Purchaser's content including playbooks, integrations, automations, fields, layouts, etc.	
36.	The Solution shall have the capability to provide in-depth visibility into the cloud assets (Amazon Web Services, Azure, Google Cloud	

Attack Surface Management Platform		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
	Platform), provided the cloud credentials are provided by the Purchaser.	
37.	Solution shall support integration with Security Information Event Management (SIEM) and Security Orchestration Automation and Response solution (SOAR), provided by the Purchaser.	
38.	Solution shall provide compliance dashboards that map identified Issues to compliance frameworks to help the Purchaser understand their overall compliance with regulatory and organisational policies. These dashboards need to provide executive visibility, prioritize high-risk areas.	
39.	Solution shall be able to Identify Virtual Private Networks, Secure Sockets Layer (SSL) certificates about to expire, domains about to expire, etc	
40.	Solution shall provide descriptions of Common Vulnerabilities and Exposures (CVEs) and the best practices around securing the Purchaser's assets with respect to the CVEs	
41.	The solution shall be able to manage the attack surface for the Purchaser's ICT infrastructure covering the below specified assets: • Fully Qualified Domain Name (FQDN) - *.gov.in, *.nic.in, *.nkn.in and any other domain name hosted at NIC Data Centre(s). • IP Address pools(s): /16 network segment – 2 Nos. /20 network segment – 1 Nos.	
42.	The necessary hardware, software, licenses, storage, network equipment for handling the attack surface management for the entire ICT Infrastructure of the Purchaser shall be provided either on cloud or on-premises along with the solution from day one.	
43.	The OEM of the offered attack surface management solution should not be the same as that of offered Unified Intelligence Platform.	

Attack Simulation Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
1	The solution must safely conduct breach and attack simulations on a live network with minimum 500 endpoints on day one and continuously validate security controls, discover vulnerabilities in a given security posture, provide quantifiable prevention and detection scores, and provide step-by-step remediation instructions. The necessary hardware, software, licenses, storage, network equipment for handling 500 endpoints shall be provided along with the solution from day one.	

Attack Simulation Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
2	The solution must measure the security posture of the target environment, gain insights into the effectiveness of security controls with respect to standards/best practices like ISO 27001, Centre for Internet Security (CIS) Benchmarks, SANS Institute's guidelines, NIST 800-53/MITRE, SOC-CMM and Custom security policies, and provide actionable remediation steps for improvement. Where applicable, the recommendations shall align with specific security-control of various Original Equipment Manufacturers (OEMs) and align with MITRE framework.	
3	The solution must provide assessments for network security controls including but not limited to Next-Generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection system (IDS), Intrusion Prevention System (IPS), Data Loss Prevention (DLP) system, Uniform Resource Locator (URL) filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), antivirus, and malware sandboxing.	
4	The solution shall provide the capability to reveal security exposure across public, private, and hybrid networks, with the ability to automatically instantiate external entities such as command-and-control (C2) servers when required and without incurring additional costs to the end user.	
5	The platform must offer a flexible on-premises breach and Attack Simulation Platform that scales elastically as the needs of the network grow.	
6	The platform must provide an on-premises software solution without any dependency on external cloud. The necessary hardware for the solution shall be supplied by the MSP.	
7	The solution must measure and validate the security posture by simulating thousands of real-world attacks on the target production network in a safe manner without impacting any production elements.	
8	The solution shall safely exercise security controls and perform clean-up operations where applicable.	
9	The solution must be able to validate web-based infrastructure and related security controls, including workloads hosted on any cloud platforms.	
10	The solution must include a diversified library of threat vectors, attack techniques, and data exfiltration methods.	
11	The solution must have a diversified and realistic library of techniques, threat vectors, and kill chains mapped to the MITRE ATT&CK knowledge base.	

Attack Simulation Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
12	The solution must have out-of-the-box experiences that simulate the full infection kill chain for popular breaches and advanced persistent threats (APTs).	
13	The solution must have scheduling capabilities to schedule assessment	
14	The solution must support packet capture, with the ability to provide PCAP/Log downloads for assessment runs between agents.	
15	The solution must be based on an implicit microservices architecture orchestrated by APIs.	
16	The platform must provide the option to run attacks over various transports that are either encrypted or in plain text. The ports for the available transports shall also be configurable.	
17	The platform must allow access through REST API.	
18	Platform access must be based on a login and password, with the possibility to enable two-factor authentication during login.	
19	The platform must offer a simple easy to use method for users to activate or deactivate software licensing.	
20	The platform must integrate with Security Orchestration Automation Response (SOAR) to facilitate the blocking/unblocking of an asset based on the outcome of an assessment.	
21	The solution must assess host-based endpoint security controls via a native agent for target platforms such as Microsoft Windows client and server operating systems.	
22	The agent(s) must be lightweight, container-based, and infrastructure-agnostic so that the solution can operate on-premises, in private or public clouds, and on remote user laptops.	
23	The agents must maintain a minimal hardware footprint in terms of memory allocated or CPU cycles consumed.	
24	The platform must provide a capability to integrate with Security Information Event Management (SIEM) tool through APIs	
25	The installed agents within representative segments or zones shall act as simulator “targets” or “attackers” inside the network for enabling safe yet realistic attack and breach simulation scenarios (inside-to-outside, outside-to-inside, and lateral movement).	
26	The solution must support tags for the agents for efficient tracking of agents based on custom metadata.	
27	The solution must support the validation of multiple network segments at once by grouping the agents for scoring and reporting purposes.	

Attack Simulation Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
28	The solution must provide a topology viewer or any other visual/diagrammatic mechanism for seeing in real time how the agents are interconnected and the available paths that exist across all agents.	
29	The solution must include a security profile feature that allows selection from a list of supported controls and types to define a security path.	
30	The solution must be customizable, allowing the user to select an assessment, configure a scenario using it, and then run the scenario for a specific agent or set of agents.	
31	The assessments shall leverage the known and custom exploits for various vulnerabilities.	
32	The solution must enable configuration of scenarios, including choosing assessments from a menu for evaluating specific types of attacks that affect the protection zone (i.e., the systems where the agent is installed).	
33	The solution must provide assessments for evaluating security infrastructure based on policy, instrumentation, or kill chain categories.	
34	The solution shall have the ability to run atomic test cases at a per-technique level or a tactic level, with the ability to visualize and customize the tactics, techniques, and procedures (TTPs) deployed.	
35	The solution shall include MITRE ATT&CK tactics, techniques, and procedures (TTPs) from 100+ Advanced Persistent Threat (APT) groups based on the MITRE ATT&CK framework.	
36	The solution shall be able to simulate spear phishing campaigns by emulating various relevant threat actors and Advanced Persistent Threat (APT) groups.	
37	The solution must provide results for each stage of kill-chain evaluations, as well as include the ability to continue a kill-chain evaluation even if one stage of the kill chain is blocked.	
38	The solution shall adhere to the MITRE ATT&CK framework, with applicable assessments that focus on the tactics, techniques, and procedures (TTPs) documented by ATT&CK.	
39	The solution's user interface must provide the ability to derive results at a per-assessment or per-audit level with detailed descriptions and MITRE ATT&CK associations for each audit.	
40	The solution must provide the ability to test against the latest malware samples, including but not limited to ransomware, trojans, wipers, potentially unwanted applications, etc. for signature-based detection on endpoint agents via multiple vectors such as email, network, and ingress transfers on the endpoint.	

Attack Simulation Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
41	The solution must allow ATT&CK techniques to be assessed on a single-feature basis for atomic validation as well as full kill-chain simulation for well-known software threats, with detailed results on stage-by-stage execution.	
42	The solution must allow the exporting of Indicators of Compromise	
43	The solution shall provide detailed results per audit level/simulation level, complete with relevant indicators-of-compromise (IoC) and pass/fail criteria.	
44	The solution must have an intuitive dashboard that shows vulnerabilities, agent status, most commonly exploited vectors (mapped to the MITRE ATT&CK framework), and prevention and detection scores over time.	
45	The solution must provide historical context using a graph of scenario runs and prevention scores completed within a selected timeframe. Each scenario that has been run features a tooltip with a health score for the entire system and the date when the run was completed.	
46	The solution must provide results view that includes a recommendation table complete as well as relevant ATT&CK, Common Vulnerabilities and Exposure/ Common Weakness Enumeration identifiers.	
47	The solution must provide actionable remediation recommendations for optimizing the security controls of the target environment.	
48	The remediation recommendations must offer perspective on various ways of mitigating, reducing, or preventing vulnerabilities that can occur within the target environment.	
49	The platform must have integrations with leading SIEM vendors to enable end-to-end validation for how well prevention and detection measures work.	
50	The platform must provide notifications to Security Operations Team after the completion of the assessment in order to distinguish simulated attacks from non-simulated ones.	
51	When integrating with a SIEM system provided by the Purchaser, the solution must pass along the real threats and information from the simulation for analysis, enabling the SOC team to see what an actual attack looks like so they can recognize a real one in the future.	
52	The solution shall be able to integrate with Endpoint Detection Response / Endpoint Protection Platform provided by the Purchaser	

Attack Simulation Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
53	Custom integration must also support Transport Layer Security (TLS) and authentication mechanisms such as REST API, OAuth 2.0 (Client ID and Secret) or API key, REST API to query for threat detection events, and generic API parameters to allow filtering based on, at least, start/end timestamps and hostname.	
54	The platform must allow the creation of role-based tenants that can be delegated to other users for administrative or viewing roles.	
55	The solution shall have the ability to allow role-based (admin/viewer) access for custom tenants.	
56	The platform must allow a User defined upload and testing of malware in various categories such as trojans, ransomware, wipers, and potentially unwanted applications (PUA) and the platform must provide the facility to filter attacks on the basis of Cyber Control (ex: Next Generation Firewall, Intrusion Prevention System/Intrusion Detection System, Data Leakage Prevention), Location of attacker, Stage of kill chain, Target operating systems (Win, Mac, Linux)	
57	The solution must test against a continuous feed of the latest threats across different vectors (endpoint, network, and email).	
58	The solution must provide top level reporting for executives, and shall also provide detailed scenario, and recommendations reports in PDF/CSV/JSON formats as appropriate.	
59	The solution must provide comparative reporting allowing the Purchaser to compare the current results with past reports.	

Security Testing Platform		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	Solution shall be able to auto discover all assets in a network segment and capture their details	
2	Solution shall be able to identify the open ports, service enumeration and header analysis of the assets	
3	Solution shall be able to automatically scan the entire network segment and identify potential vulnerabilities, threats and risks	
4	Solution shall be able to automatically exploit the identified vulnerabilities, using inbuilt exploit database and shall also allow use of user-defined exploits	
5	Solution shall support agent-based and agent-less scanning to identify and exploit vulnerabilities	

Security Testing Platform		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
6	Solution shall be able to audit the configuration of the endpoints (windows, MAC OS, Linux), network and security devices and identify gaps, misconfigurations, weakness in the configuration	
7	Solution shall be able to run multiple parallel audits, scanning and exploitations	
8	Solution shall be able to scan and enumerate vulnerabilities in web applications	
9	Solution shall provide a Command and Control (C2) framework for emulating the compromise of a vulnerable asset and shall be able to perform various C2 actions including but not limited to deployment of keylogger, Remote Access Trojan, custom scripts, etc., and it shall support auto clean-up of the deployed artefacts post completion of the scanning/audit activity and report the whole exploitation activity details	
10	Solution shall have an in-built database of exploits for various vulnerabilities, which shall be leveraged during the automated and manual scanning and exploitation.	
11	Solution shall allow the loading of custom exploits developed by the Purchaser or the MSP's team and use those exploits during the penetration testing audit exercises.	
12	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution	

Dynamic Application Security Testing (DAST)		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
1	The solution shall be able to scan source code across multiple programming languages and Frameworks including but not limited to Java, C#, Dot Net, JSP, Java EE, Java SE, ASP.NET, VB.NET, C, C++, JavaScript, Python, PHP, HTML, Visual Basic, Ruby, Go, Angular etc.	
2	The solution shall be able to scan and test web, mobile (Android, iOS), and desktop applications	
3	The solution shall support Integration with popular Integrated Development Environments (IDEs)	
4	The solution shall support Integration with Continuous Integration/Continuous Deployment (CI/CD) pipelines	
5	The solution shall Support containerization and microservices architectures	

Dynamic Application Security Testing (DAST)		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
6	The solution shall support Integration with existing application and security infrastructure (e.g., Single Sign On, Identity Access Management, Web Application Firewall)	
7	The solution shall support Identification of vulnerabilities in the code including but not limited to the Open Web Application Security Project (OWASP) Top Ten vulnerabilities for Web Applications and Mobile Applications.	
8	The solution shall support standard secure coding rules like SANS Top 25 most dangerous software errors, SANS Common Weakness Enumeration Top 25, SEI CERT Coding Standards, ISO/IEC TS 17961:2013/C or 1:2016 C Secure Coding Rules	
9	The solution Should be able to scan code and code repository and identify vulnerable packages, including but not limited to vulnerable/outdated open-source components, libraries, plugins, software, etc	
10	The solution shall support customizable vulnerability scanning rules and policies. With ability for False positive reduction mechanisms and improved accuracy rates	
11	The solution shall have Incremental scanning capabilities to minimize scan time	
12	The solution shall have the ability to schedule and automate scans	
13	The solution shall support scalability and performance, including parallel scanning and distributed scanning	
14	The solution shall support REST and SOAP APIs for seamless integration with any other 3rd party tools	
15	The solution shall provide In-depth reporting and data visualization options	
16	The solution shall support risk prioritization and severity scoring, such as Common Vulnerability Scoring System (CVSS)	
17	The solution shall support compliance reporting for industry standards (e.g., Payment Card Industry Data Security Standard, General Data Protection Regulation)	
18	The solution shall provide detailed remediation guidance and code examples	
19	The solution shall support Integration with popular issue tracking systems (like Jira, GitHub, GitLab)	
20	The solution shall have User role management and access control capabilities	
21	The solution shall support multi-tenancy and segregated environments	

Dynamic Application Security Testing (DAST)		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
22	The solution shall support customizable notification and alerting system	
23	The solution shall support for secure coding standards/best practices, released by Computer Emergency Response Team (CERT), Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE)	
24	The solution shall support integration with other application security testing tools (e.g., Interactive Application Security Testing, Runtime Application Self Protection)	
25	The solution shall have comprehensive documentation and Application Programming Interface (API) reference materials	
26	The solution shall be deployed On-premises	
27	The solution shall support for encrypted data storage and secure data transfer	
28	The solution shall provide Regular updates and updates for the vulnerability signature database	
29	The solution shall have Security certifications and accreditations (e.g., International Organisation for Standardization (ISO), System and Organisation Controls (SOC))	
30	The solution shall support for accessibility testing and standards (e.g., Web Content Accessibility Guidelines (WCAG))	
31	The solution shall have Cross-platform compatibility (Windows, macOS, Linux)	
32	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution with support to scan at least 20 Applications concurrently	

Threat Intelligence		
S.No	**Purchaser Requirements**	**Compliance (Y/N)**
A	**IP and Web Reputation and Classification Database**	
1	On-premise database of IP and Web Reputation and Classification database, which should work in offline mode and should be ingested into the Threat Intel Platform, SOAR, Log Management platform and other platforms.	
2	The provided database should have 80+ unique categories of reputation classifications (ex: File Sharing, Peer to Peer, Hacking, Malicious..etc)	
3	Should provide WHOIS details	
4	Geo-Location	
5	Hosting Network, including ASN	

6	Current DNS and Passive DNS	
7	Content Classification	
8	Server Responses	
9	Should provide Details of Mx Records, DKIM, SPF, TXT	
10	Should provide Reverse Lookup	
11	Should provide details of Related Hosts	
12	Should provide details of Hosts sharing same IP, Same Domain	
13	Should provide details of Certificates	
14	Should provide popularity details	
15	Should provide risk rating	
16	Should provide category	
17	Should provide Threat details	

B	**Threat Intelligence – IOCs, Report**	
1	Threat Intel provider must have more than 10 years of threat intelligence collection experience, analysis and tracking of threat groups	
2	Threat Intel provider must have Intel collection in more than 20 foreign languages	
3	Threat intel reporting to include sources from incident response (victim intel) gathered through incident response work	
4	Threat intel provider should have a Collection of intel from millions of telemetry sensors including but not limited to endpoints, network, IoT and email.	
5	The threat feeds should not only be based on information gleaned from current network activities but also from information collected by infiltrating and communicating with threat actor groups	
6	The feeds should not be limited to open-source information but should extend to closed (non-public) information	
7	The feeds harvested should not be limited to only English-speaking sources but also be collected and interpreted from non-English sources like mandarin, Arabic, Russian, Korean, Urdu, Farsi(Persian)	
8	The feeds should not only provide a series of individual data points but also correlate and analysis of disparate data points and draw informed conclusions	
9	The feeds should ideally be validated by the provider by first-hand investigation. For example, behaviour of a malicious file should be analysed first-hand preferably by the provider internally using a dynamic (sandboxing) tool.	
10	The feeds should also include the indicators from dark web, social media, OSINT, third party paid sources etc	
11	The provider should be able to provide information (summary, related IPs, URLs, file hash etc) of the current threat activity.	

12	The provider should be able to provide extensive context and malware analysis in addition to the threat indicators. Information should include, but not limited to, background of the threat actors and attack methods linked to specific indicators and threat artefacts.	
13	The threat intelligence report should ideally contain, but not limited to: • Goals of the threat actor • Conditions under which the threat is likely to successfully exploit a vulnerability • Variants of the threat • Current activity implicating the threat • Outcomes for the organization if the threat is successfully executed • Indicators that the threat is currently acting against the organization or otherwise impairing the assets of the organization • Defence against the threat • An assessment of the reliability of the source of the information and the reliability of the information itself • The period of relevance of the threat.	
14	The threat intelligence information should include tags that help the organization to identify the indicators and threat artefacts relevant to the organization. For example, a tag might flag the fact that a file is used to target government or defence in the region.	
15	The threat intelligence should, preferably, be able to provide insight into how attackers and campaigns are organized and what targets are being attacked and, in addition, guidance on how to protect the organization from the attacks.	
16	The provider should be able to provide threat intelligence data in various forms (MRTI) e.g. The MRTI data should preferably contain, but not limited to, the below types: IP addresses, URLs mains, Hashes, Filenames	
17	The MRTI data should, preferably, be categorized e.g., Attacker, Compromised or Related, etc.	
18	Please provide the type and category of the MRTI data when provided. IP Address – Domain Name	
19	The provider should be able to provide the facility to analysis the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity)	
20	The provider should preferably be able to provide threat intelligence advice of adversarial capabilities and plans of future activities or possible future styles of attack (or alternatively interpret existing attacks)	
21	A facility should be available to create customized alerts	
22	The facility should preferably be there to provide visibility into the threat indicators and malicious activities seen most frequently by others in the same industry and region.	

23	The facility should, preferably, be available to be able to “Pivot” from an indicator and find related artefacts and assess the scope of an attack. For example, for a file containing malware, the portal should be able to provide the facility to search for other instances of the file, of instances of similar but not identical malware in the same family, and of other artefacts associated with the same threat campaign. The portal should provide information on the actions the file attempts to take when it executes, such as connecting to a remote IP addresses or create registry entries.	
24	The facility should be available to search for threat indicators on the portal. For example, to search for an IP address identified internally with the organization to check if it is malicious. Please mention the type of threat indicators that can be searched on.	
25	The provider should be able to disseminate the threat intelligence in a form that can be consumed by the customer. Please provide the means by how the threat intelligence can be provided (E.g. feeds, emails, and portal).	
26	The provider should be having a technology partnership with leading vendors in SIEM, EDR, and other devices to integrate the feeds. Please provide a list of supported solutions.	
27	For devices not supported, the provider should be able to provide the same via easy to use, well documented APIs with examples. Free provider support to provide assistance on using APIs would be an added advantage	
28	Bidder should quote different OEM’s product for Threat intelligence-IOCs, Reports and Threat Intel – Deep Web, Dark Web, OSINT, Social Media.	
C	**Threat Intel – Deep Web, Dark Web, OSINT, Social Media**	
1	Threat Intel provider must have more than 5 years of threat intelligence collection experience, analysis and tracking across deep web, dark web, OSINT, social media, and other sources.	
2	Threat Intel provider must have Intel collection in more than 10 languages including English, Chinese, Russian, Arabic, Farsi, Korean, French, Spanish, Italian etc.	
3	Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy of metadata	
4	Should provide facility to configure custom alerts via portal and through email.	
5	Should provide facility to configure custom assets like IP addresses, IP Segments, Domains, URLs, Keywords, email addresses etc., for monitoring across the deep web, dark web, osint, social media etc.	
6	Should provide alerts in case of any IPR exposure or leak, source code leak, credential leak, asset mention, potential threats, vulnerabilities etc.	
7	Should provide facility for monitoring activity and content related to the assets configured	
8	Monitor and alert for malicious/spoof/typosquat domains, phishing domains, mx records	

9	Monitor and alert for malicious domain certificate registration	
10	Monitor and alert mention of configured assets in social media including twitter, telegram, discord…etc.	
11	The provider should be able to provide information (summary, related IPs, URLs, etc.) of the current threat activity.	
12	The raw feeds of the dark web, deep web, osint, social media etc., should be provided through web portal and through API. There should not be any limit on the number and type of assets that needs to be monitored.	
13	The intel provided from dark web, deep web, OSINT, Social media…etc., should be full and complete and no part of the intel should be hidden or denied access.	
14	Bidder should quote different OEM's product for Threat intelligence-IOCs, Reports and Threat Intel – Deep Web, Dark Web, OSINT, Social Media.	
15	Raw feed of the dark web data should be provided through API. The raw feed should have the complete dark web data gathered by the OEM.	

Incident Response Retainer Service		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	Incident Response Retainer Service should be provided from a global OEM with more than a decade of incident response experience.	
2	The OEM should have experience in handling and responding to Advanced Persistent Threats (APTs)	
3	The OEM should have identified new APTs and published APT Reports in public domain (samples of latest 5 APT reports to be submitted along with the Bid)	
4	OEM should have a strong pool of experts i.e, atleast 50 Cyber Security Professionals stationed in India, with a dedicated global incident response team based out of India	
5	OEM should deploy incident responders on-site within 24 hrs from the time an incident is reported to the OEM by NIC	
6	OEM should bring their own tools and devices required for the investigation of the security incident	
7	Scope of the Incident Response Service would include but not limited to the following :	
	(ii) Analysis of Logs	
	(iii) Review of device and equipment configuration	
	(iv) identification, containment and eradication of the threat	
	(v) Identify the initial point of entry, and uncover the extent of activities performed by the threat actor	
	(vi) Identify the details of data that was exfiltrated/accessed by the threat actor	
	(vii) Analysis and reverse engineering of the suspicious files and malware files	
	(viii) Engage with threat actor (on behalf of NIC), if required	

	(ix) Review source code and identify potential malicious code	
	(x) Carry out forensics of digital and electronic devices related to the incident/data breach	
	(xi) Analyze Database, including SQL, NoSQL. Analysis shall include but not limited to review of schema, tables, procedures and logs	
	(xii) Conduct Purple and Red Team exercises for NIC, to identify previously unknown security vulnerabilities	
	(xiii) Prepare a detailed report containing the complete timeline of the attack, damage/impact of the attack, vulnerabilities exploited, credentials misused/compromised, details of lateral movements, details of data compromised, details of files/artefacts dropped by the attacker, indicators of compromise, attack attribution details.	
8	Additionally, the OEM should investigate and submit a detailed incident report which shall include details of the incident, including but not limited to the following : (i) Complete Timeline of the Incident (ii) Root Cause of the Incident (iii) Vulnerabilities/bugs exploited by the attacker (iv) Changes or modifications carried out by the attacker (v) Files dropped by the attacker (vi) Exploit Payloads used by the attacker (vii) attack attribution & classification (viii) indicators of compromise (ix) Sigma Rules, SIEM Rules, YARA Rules and Snort Rules for detecting similar attacks (x) Impact of the Attack (xi) Remediation for mitigation and preventive measures (xii) MITRE Mapping	
9	OEM Should investigate the attack on-premise as per purchaser's direction, anywhere across India.	
10	OEM should appoint a Single Point of Contact (SPOC) for incident response for the Purchaser	
11	IR Service should be provided for at least 100 hours per year and the number of hours may be subsequently increased on-demand as per the requirements of incident response	
12	In-lieu of unutilized IR hours, OEM should conduct training sessions, Conduct proactive security assessments, offer professional certifications to Purchaser's employees	
13	All the investigations should be conducted on-premise, no data shall be taken out of the Purchaser's premise.	
14	Remote incident response shall be strictly prohibited.	

15	Only Indian nationals residing in India shall be engaged in the incident response activities.	
16	The details of the incident, investigation details, artefacts, root cause analysis, evidence. Etc., shall not be shared/uploaded to anywhere except the Purchaser's Ticketing platform.	
	Note : The activities carried out under the Incident Response Retainer Service are highly confidential in nature. The OEM / MSP both shall mandatorily sign an NDA with NIC to maintain the confidentiality. During the investigations, the OEM/MSP may get exposure to many internal data including the indicators of compromise, forensic artefacts, technical details like architecture, network structure etc. The OEM and MSP shall not use this data anywhere, they shall not share this data through any blog or social media or through any other medium. The details about the attack shall be kept confidential and shall not be disclosed to anyone, without the written permission of NIC.	

Digital Forensic Incident Response Tool (DFIR)		
S.No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	The system must provide an administrative interface or user management panel for managing user accounts. The interface should be secure and use strong authentication mechanisms (e.g., multi-factor authentication) to prevent unauthorized access.	
2	Solution should support online and offline triaging including live investigation across multiple operating systems including Windows, Linux, MacOS.	
3	The system should offer a streamlined account onboarding/creation process with clear instructions and secure authentication mechanisms. The system should enforce encryption of data in transit.	
4	System should allow administrator to activate/deactivate data collection on endpoint devices. It should allow administrator to triage various artefacts from the endpoint devices as per the need. It should also allow the administrator to create reusable templates for artefacts that need to be collected.	
5	The system should catalog and associate evidence with respective triaging runs and events.	
6	The system should create a chronological timeline of events and activities related to the device.	
7	The system should automatically collect user account information like usernames and last login times.	
8	The system should identify users with elevated privileges and analyse their access logs for potential misuse.	
9	The system should provide information to assist in identification with device fingerprinting. (for more than one device)	

10	The system should generate cryptographic hashes of evidence artefacts to be matched at the time of presenting the evidence	
11	The system should capture and store metadata associated with the acquired evidence. The system should collect metadata like timestamps, file attributes, user information and device details.	
12	The system should offer the capability to generate an organization specific agent installer link.	
13	The system should extract: directory structures, file system-specific timestamps.	
14	The application should provide: visualization tools for exploring the file system structure.	
15	The system should automatically collect timestamps for file creation, modification, and access. The system should automatically gather information about file permissions, attributes (e.g., hidden, readonly), and owner/group information.	
16	The system should allow selective extraction of file content based on filters (e.g., file type, keywords) or for specific evidence needs.	
17	The system should allow users to search for specific keywords or phrases across file names, tags, and other descriptive information (metadata) associated with the collected data. The system should allow filtering and searching based on specific metadata fields. The system should provide efficient search functionalities to quickly locate specific evidence items.	
18	The system should support regular expressions and advanced search operators for precise targeting.	
19	The system should provide a central repository for storing all digital evidence related to investigations.	
20	The system should allow users to categorize and tag evidence based on case, incident, or relevance.	
21	The system should automatically gather information about the operating system version, including service packs and hotfixes installed. The system should automatically collect details about hardware components like CPU, RAM, storage, and network adapters.	
22	The system should retrieve and capture the contents of the clipboard	
23	The system should enumerate and list active firewall rules, system restore points, and list all installed drivers with details like name, version, and digital signatures.	
24	The system should enumerate and list all running processes with details like name, PID, associated modules	
25	The system should retrieve information about installed antivirus software (windows Defender)	
26	The system should identify and list the configured DNS servers used by the system and list any configured proxy servers.	
27	The system should enumerate and list all installed applications with details like name, version, install date, and publisher.	

28	The system should also list recently downloaded files with details like name, path and timestamps in default downloads Directory.	
29	The system should enumerate and list programs scheduled to run at startup or login.	
30	The system should access and export relevant event log data from the Event Transcript database.	
31	The system must provide information about the disk's unique identifier (e.g., serial number, model number) and the partitioning scheme (e.g., MBR, GPT). The system should list all mounted volumes with details like filesystem type, label, and mount point. The system must display the volume name and any assigned label for identification. The system must display the filesystem type (e.g., NTFS, FAT32, Ext4, XFS, APFS etc.) and version.	
32	The system must display total Memory capacity and available free space.	
33	The system should be able to collect the browsing history (Chrome Browsing History, Firefox Browsing History, Internet Explorer browser history, Edge Browsing History, Opera Browsing History). The system should collect URLs, timestamps, visited pages	
34	The system must be able to parse all Windows Registry hives (e.g., SOFTWARE, SYSTEM, SECURITY) for forensic analysis. The system should allow selection of specific registry hives (e.g., user, system, security) for targeted collection.	
35	The system should analyse ShellBags for recently accessed files and folders to find suspicious activities. The system should analyse UserAssist for frequently used programs and launched shortcuts to find suspicious activities. The system should analyse TypedPaths for frequently accessed URLs and network paths to find suspicious activities.	
36	The system should analyse RecentDocs for recently opened documents across various applications to find suspicious activities.	
37	The system should analyse ShellFolders for default folder locations and shortcuts to find suspicious activities.	
38	The system should list and analyse active TCP connections, including source and destination IPs, ports, and state.	
39	The system should retrieve and analyse historical TCP connection information (timestamps, duration, transferred data).	
40	The system should attempt to identify applications associated with TCP connections based on port numbers and traffic patterns.	
41	The system should identify and analyse suspicious TCP connection characteristics (e.g., unusual ports, high data transfer).	
42	The system should identify the default gateway and analyse its configuration.	
43	The system should retrieve and analyse configuration details of all network adapters (IP addresses, MAC addresses, enabled protocols).	
44	The system should gather information about installed network adapter drivers (versions).	
45	The system should allow filtering logs based on time range and specific criteria (e.g., event type, severity, source)	

46	The system should automatically parse logs, extract relevant information (e.g., user, timestamp, action), and present them for analysis.	
47	The system should allow selection of specific event logs (e.g., Security, Application, System), OS Logs for collection.	
48	The system should allow filtering events based on time range and specific criteria (e.g., event ID, source, category).	
49	The system should automatically parse event logs, extract relevant information (e.g., user, timestamp, action), and present them for analysis.	
50	The system should support collection of diverse event logs from various sources (Windows and applications).	
51	The system should parse and normalize collected logs into a unified format for easier analysis.	
52	The system should enable efficient filtering and searching of logs based on specific criteria (time, source, event ID, etc.).	
53	The system should support parsing and analysis of EVTX files from Windows systems (Vista and later).	
54	The system should extract relevant information from EVTX files, including timestamps, event IDs, sources, descriptions, and user information.	
55	The system should correlate timestamps from EVTX files with other log sources for unified timeline analysis.	
56	The system should parse event record metadata such as timestamps, event IDs, sources, user information, and descriptions.	
57	The system should allow filtering and searching within event records based on specific criteria for efficient analysis.	
58	The system should collect and store command line arguments used for process execution.	
59	The system should allow extraction of key SRUM data for further investigation and reporting.	
60	The system should extract and analyse relevant Powershell logs to identify commands executed and potential malicious activity.	
61	The system should parse and analyse Microsoft Mail data files (PST), including emails, attachments, and metadata.	
62	The system should extract relevant content like email text, sender/recipient information, attachments, and timestamps.	
63	The system should parse and analyse Microsoft Outlook data files (PST), including emails, attachments, and metadata.	
64	The system should extract relevant content like email text, sender/recipient information, attachments, and timestamps.	
65	The system should parse and analyse Mozilla Thunderbird data files (mbox), including emails, attachments, and metadata.	
66	The system should extract relevant content like email text, sender/recipient information, attachments, and timestamps.	
67	The system must use a lightweight passive agent for data collection, minimizing resource consumption on endpoints.	

68	The system may leverage antivirus scanners and threat intelligence databases for malware detection.	
69	The system may identify unauthorized access attempts or suspicious remote access activity.	
70	The system should enable filtering and searching of logs based on timestamps, event types, threats, and other relevant criteria.	
71	The system should Use secure communication protocols like SSL/TLS for data transmission.	
72	The system should Implement authentication and authorization mechanisms to restrict access.	
73	The system should Preserve timestamps, file metadata, system logs, and other relevant information.	
74	The system should offer users the option to export data and reports for cases.	
75	Exported data should be in a readily usable format (e.g., CSV, JSON) with clear labeling and metadata for easy identification and interpretation.	
76	System should track and log all data export requests for audit purposes.	
77	System should give analyst the capabilities to analyse forensic images in various formats like e01, l01, dd, raw, ufdr etc	
78	System should allow the users to view and analyse data in these images.	
79	System should allow the user to do deep searches in the content of these images.	
80	System should have the capability for boolean, phrase, proximity, fuzzy search for an exhaustive search within the forensic images	
81	System should have capability to extract metadata from files within the images. It should also allow searching on images (jpg,png,bmp etc) via OCR	
82	System should have capability to do visual link analysis on the content and metadata of the extracted files	
83	Solution Should support scanning the endpoints for presence of webshells, malware, trojan, ransomware and other malicious programs	
84	Solution should support IOC based scanning, Sigma rule based and YARA rule based scanning across windows, linux and Mac OS based systems.	
85	Solution should seamlessly integrate out of the box with SIEM and SOAR solutions quoted as a part of this RFP.	
86	Solution should seamlessly integrate out of the box with EDR and antivirus solutions.	
87	Solution should support acquisition of various evidence types including but not limited to the following : • Event Logs • Page File • LNK File • Jump Lists • Amcache • Activities DB • Hosts File	

	• WMI Scripts • SRUM Database • INF Setup logs • TCP, UDP, ARP and Route Tables • DNS and App Compat Cache • Crashdump • Processes and Modules list • EDR/Antivirus details • Swap File • Powershell logs • Windows Index Search • Syslog • Sudo Logs • Authentication Logs • Bash History • Cron jobs • Network configuration & Logs • Systemd journal • Tmp directory • Kernel messages and error logs • Package management logs • User home directory • Shell history • Safari history • Keychain • Quarantine events • Mac OS Crash reports • Spotlight database • Apple unified logs • USB Devices • Firewall rules • Startup programs • Time Machine Backups • Kernel Taint State	
88	The solution shall support the mobile forensics also. Full featured licenses required to cover mobile devices shall be provisioned as part of the solution.	

Portable Log Analyser		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	Portable log analyzer should be able to automatically ingest, parse, index and analyse offline logs of at least 4 TB volume. The log analyzer	

Portable Log Analyser		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
	should be able to facilitate threat hunting, correlation rules, alert rules, reporting. The necessary portable hardware should be provided along with the log analyzer solution. The hardware specifications are as follows: Snapdragon X Elite CPU, Qualcomm Hexagon 45 TOPS NPU, 64 GB LPDDR5 RAM, 1 TB SSD, Qualcomm Adreno GPU, 13 inch Pixel Sense Corning gorilla glass 5 oled display with 2880x1920 resolution 120 Hz refresh rate, Firmware TPM 2.0, Wifi 6E 802.11ax, Bluetooth 5.3, 5G, Microsoft Pen Protocol (MPP) support, Surface Slim pen2 with charger. The hardware should be provided with flex keyboard, bag and carry case.	

Forensic Disk Imager with Hardware Write Blocker		
S. No.	**Purchaser's Requirement**	**Compliance (Y/N)**
1.	Solution should be hardware based and should be able to acquire logical images from locally attached drives and network shares	
2.	Solution should be able to collect the entire file system, manually select specific folders and files or use in-built search capabilities on the hardware solution to define a targeted search profile using pre-defined and custom criteria	
3.	Solution should leverage wildcard characters in logical image search criteria for powerful results	
4.	Solution Should save complicated and commonly used logical image searches and share across the forensic imager units by exporting/importing via the network or USB accessory ports	
5.	Solution should provide the option to set up a group of job settings and then place the forensic image in an auto mode for performing imaging operations, with any detected source media automatically getting enqueued with the pre-set settings	
6.	Solution should provide users the flexibility to manually pause any running imaging job (E01, Ex01, DD, DMG) and resume it later, even across power cycles	
7.	Solution should support the ability to resume jobs that failed due to unexpected power loss, destination full, or source/destination drive disconnected	
8.	Solution should support restoration of created image files to a full drive with original formatting and directory structure	
9.	Solution should support full forensic imaging from a wide variety of media, including PCIe, 10GbE network shares and Mac computers in target disk mode (USB-C, Thunderbolt and FireWire)	
10.	Solution should provide the ability to target a single partition, multiple partitions or custom sector range of a drive to generate a hash	
11.	Solution should support acquisition of evidence from Mac computers in target disk mode over USB-C, FireWire or Thunderbolt (with adapter)	
12.	Solution should support capture of both physical drives (HDD and SSD) configured as one Fusion Drive on iMac and Mac Mini	
13.	Solution should be able to directly acquires from both SATA and PCIe Mac removable storage media, with necessary Adapters. The necessary adapters should be provided part of the proposed solution.	
14.	Solution should support mounting of source or destination APFS volumes, enabling features like logical imaging, browsing and log export	
15.	Solution should detect the presence of APFS encryption and can pass through known credentials to unlock	
16.	Solution should detect and remove Host Protected Area (HPA) hidden partitions	

17.	Solution should detect, unlock, restore and trim Device Configuration Overlay (DCO) hidden partitions and Accessible Max Address (AMA) hidden partitions hidden partitions on newer ACS-3	
18.	Solution should automatically detect drives encrypted with the following popular encryption types: Microsoft BitLocker, BitLocker To Go, Apple	
19.	FileVault 2, Apple APFS, Linux LUKS, BestCrypt, Symantec PGP WDE, Check Point Full Disk Encryption, McAfee Drive Encryption (SafeBoot), Sophos Safeguard, WinMagic SecureDoc Full Disk Encryption, GuardianEdge Encryption and Symantec Endpoint Encryption	
20.	Solution should unlock BitLocker and APFS encryption with known credentials	
21.	Solution should Detect Opal self-encrypting drives and unlocks with known credentials	
22.	Solution should detect proprietary self- encrypting USB devices	

DeGausser and Secure Drive Eraser		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
1	Solution shall generate minimum 20,000 gauss magnetic field	
2	Solution shall support erasure of hard drives and tape drives in 30 seconds	
3	Solution shall be able to erase up to 460 (1.8 in), 360 (2.5 in) and 80 (3.5 in) drives per hour	
4	Solution shall have built in field verification system.	
5	Solution shall display the value of gauss field strength to verify the erasure, cycle count, job count and diagnostics	
6	Solution shall generate media destruction reports with date, time, user ID, serial number and verification of each cycle	
7	Solution shall be certified to UL, IEC, CSA, CE, KC and RCM Standards	
8	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution.	
Secure Drive Eraser		
1	Solution shall be a software-based solution	
2	Solution shall support secure erasure of unlimited devices	
3	Solution shall support erasure of windows, mac, Linux, Android and iOS devices	
4	Solution shall generate custom erasure reports in CSV, PDF and XML formats	
5	Solution shall support. Global erasure standards including NIST 800-88, DoD 3 & 7 Passes, HMG, NSA 130-1	
6	Solution shall support high speed erasures of multiple hard drives. The solution should provide license for unlimited erasures.	
7	Solution shall be a software-based solution	

DeGausser and Secure Drive Eraser		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
8	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution. The secure drive erasure software should also be provided in a portable USB drive for live booting from any target system.	

Malware Analysis Sandbox (from 3 different OEMs)		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
	Solution shall provide dynamic sandbox analysis environment for atleast 2 or more OS (like windows, Linux, Mac, Android, iOS). Bidder shall ensure that windows, linux, mac and android/ios support for static and dynamic analysis is covered by the offered sandbox solution from 3 different OEMs(for example: if OEM 1 supports only windows, OEM 2 supports linux + mac and OEM 3 supports only android, then the combination of these 3 OEMs can be offered as a solution).	
	Solution shall support more than 50+ file types for sandbox analysis	
	Solution shall allow user interaction with the sandbox environment during dynamic analysis	
	Solution shall support auto-extraction of indicators like files, Domains, URLs, network traffic, file activity, user activity, registry activity	
	Solution shall support AV scanning from multiple AV engines and Yara Rule matching	
	Solution shall document every single action and activity performed by the file submitted to the sandbox	
	Solution shall allow export of files or artefacts, which were created/downloaded/dropped during the execution	
	Solution shall support atleast 500 unique file submissions per day	
	Solution shall identify functions based on dynamic memory dumps	
	Solution shall detect and decode hidden payloads and malicious functionalities which is not observed during runtime	
	Solution shall detect sandbox evasion techniques employed by malwares	
	Solution shall support addition of user defined pre and post hooks to modify function parameters and return values for VBAs	
	Solution shall support interception of HTTPS traffic generated during the analysis and analyze the contents of the traffic	
	Solution shall support YARA Rules, Sigma Rules for threat detection	
	Solution shall generate supplementary data including but not limited to created files, unpacked PE files, memory dumps, PCAP of the captured network traffic (incl. decrypted HTTPS), screenshots, shellcode and strings.	
	Solution shall generate reports in XML, JSON, HTML, PDF	
	Solution shall include MITRE ATT&CK matrix mappings	

	Solution shall support API which enables file upload, analysis data download, searches, filters, alerts	
	Solution shall support playbooks/cookbooks for automated actions during file analysis	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	The Solution shall have comprehensive support for data extraction from memory, live acquisition, and analysis of computer, cloud and mobile data all within a unified platform.	
2	The Solution shall provide dedicated workflows tailored specifically for Windows, MacOS, and Linux operating systems.	
3	The Solution must provide robust support for data acquisition from Android devices, as well as logical acquisition from iOS devices, Windows Phone, Media Transfer Protocol (MTP) devices, Subscriber Identity Module (SIM) cards.	
4	The Solution shall facilitate efficient and discreet remote collections of forensic evidence from Mac, Windows, and Linux endpoints, ensuring that remotely collected data is securely written to a forensically sound container using the Advanced Forensic File Format 4(AFF4-L).	
5	The Solution shall provide a user-friendly and efficient mechanism for creating and deploying ad hoc or on-demand agents for remote acquisition.	
6	The Solution shall have an agent status dashboard that enables investigators to create a single agent and deploy it to multiple endpoints.	
7	The solution shall support multiple examiners to connect to various agents without binding the agent to a specific user.	
8	The solution shall support YARA rule processing to accelerate incident response investigations and identify malware.	
9	The solution may preferably support Dark mode to help Purchaser’s team to work long hours staring at the screen.	
10	The solution must have the ability to create a queued list of target endpoints (up to 15 endpoints) to acquire from using Targeted Locations to sequentially collect from each endpoint in the queue until the job is complete.	
11	The solution shall support forensic evidence (including full system image) acquisition from popular distributions in Linux including Ubuntu, Debian, Red Hat, Kali.	
12	Solution shall have option to save cloud acquisitions to Advanced Forensic File Format 4 (AFF4L) and Zip containers.	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
13	The tool must support different file systems including Yet Another Flash File System 2 (YAFFS2), New Technology File System (NTFS), Hierarchical File System + (HFS+), Hierarchical File System X (HFSX), Second Extended File System (EXT2), Third Extended File System (EXT3), Fourth Extended File System (EXT4), File Allocation Table 32 (FAT32), and Extensible File Allocation Table (EXFAT).	
14	The solution shall support targeted image acquisition of forensic evidence from Windows including event logs, Windows registry hives, page file, hibernation file, master file table, Update Sequence Number (USN) journal, Setup Application Programming Interface (API) logs, LNK files, user profiles, and prefetch files.	
15	The Solution shall be able to recover a wide range of system artefacts, such as user accounts, Bash history, SSH keys, scheduled tasks, log files, and recent files from Linux-based images.	
16	The solution shall support targeted acquisition of forensic evidence from Linux including home, system logs, sleep images, tamp, etc., and user and shall also have added support for recovering Bash information, including session ID, user, start date/time, end date/time, and session command history.	
17	The solution shall have support for recovering information about scheduled tasks, such as frequency, command, and paths of the directories, network interfaces information, and their DHCP leases assigned by the local Dynamic Host Configuration Protocol (DHCP) server.	
18	The solution shall have support for recovering Linux operation system installation information, Secure Socket Shell (SSH) keys information including file name/ key type/ encryption type/ Media Access Control (MAC) times, and file content, information about configured auto-run scripts that open when a Linux device starts.	
19	The solution shall have support for recovering items that a user has sent to the trash, including both deleted directories and deleted files and user account information such as the account description, username, password hash, last password change date/time, user ID, and more.	
20	The solution shall support the capture of physical memory (Random Access Memory Dump) to analyse valuable artefacts that are often only found in memory.	
21	The solution shall support capture of memory from individual running processes, providing less fragmented data and better recovery of larger data types.	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
22	The solution shall have both Graphical User Interface (GUI) and command-line options to acquire memory and individual process, reducing the footprint on the suspect system.	
23	The solution shall have a command-line utility that can quickly and non-intrusively check for encrypted volumes on a suspect computer system during incident response.	
24	The solution shall have the ability to analyse data from forensic image file formats such as E01, Ex01, L01, Lx01, AFF, AD1, DD, RAW, BIN, IMG, DMG, FLP, VFD, BIF, VMDK, VHD, VDI, XVA, ZIP and TAR.	
25	The solution shall have the ability to analyse memory dumps in the format of RAW, CRASH, VMSS, HPAK, ELF, MEM, DMP, DD, IMG, IMA, VFD, and FLP.	
26	The solution shall support full drive decryption and detect and decrypt TrueCrypt, BitLocker, McAfee, VeraCrypt, and FileVault2 with known passwords or using brute-force attacks.	
27	The solution shall provide a utility for determining and retrieving user passwords based on keywords from a case file, significantly reducing the time involved in trying to brute-force this password manually.	
28	The solution shall have multiple device queueing, allowing the automatic processing of multiple devices in a row without the need for examiner-run separate processes.	
29	The solution shall have filter stacking, allowing the layering of several dimensions of filter criteria to pinpoint specific items in a large dataset.	
30	The solution shall have the ability to view SQLite database files using a built-in SQLite viewer.	
31	The solution shall support Optical Character Recognition for the extraction of text from PDF documents (including text in scanned documents and text from pictures in PDF documents) and from picture artefacts for keyword searching.	
32	The solution shall support a search for keywords on both recovered artefact and sector level content both prior to processing the case as well as after processing the complete case with an option to select all added evidence sources or any particular evidence source.	
33	The solution shall support recovery of artefacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.	
34	The solution shall support ingesting the downloaded user data package from Facebook, Google, and Slack.	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
35	The solution shall be able to identify and categorize handwritten documents automatically.	
36	The solution shall have inbuilt support for finding similar pictures by building picture comparison for identifying any similar pictures from the extracted images or external images using CBIR (Content-Based Image Retrieval) feature.	
37	The solution shall have an advanced option to analyse media files using a dedicated Media explorer to view, sort, and filter media evidence using criteria that are specific to pictures and videos. The Media explorer shall stack copies of the same picture or video that were found in different source locations.	
38	The solution shall have option to analyse media file using dedicated Media explorer to view, sort, and filter media evidence using criteria that are specific to pictures and videos. The Media explorer shall stack copies of the same picture or video that were found in different source locations.	
39	The solution shall provide a to hover over image/video, which shall provide a larger, higher resolution preview of the image or video. Users can also zoom and pan around an image within the preview. For videos, the Purchaser shall be able to use the mouse to quickly scroll through the contents of the video.	
40	The solution Should allow the Purchaser to filter media files by Investigation leads, including attributes such as camera serial numbers, Exif created dates, camera make & model, Items with Geolocation data, deleted source, items matching social media platforms, Lens model & Serial Number, file extension, Vehicle Information & Communication System attributes, media attributes, video attributes, and file attributes. The date / time filter is also available in the Filters bar.	
41	The solution shall allow the Purchaser to sort by option to organize the evidence in ascending or descending order based on attributes such as skin tone, media size.	
42	The solution shall allow the Purchaser to filter video files with attributes such as video files within carving limit, media, duration etc.	
43	The solution shall have utility which can be installed on any number of Windows Tablet or Laptop to empower frontline officers to collect and report on fleeting digital evidence. The tool shall be capable to Maintain privacy and build trust with the public while capturing crucial but fleeting digital evidence from consenting victims and witnesses.	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
44	The Solution shall have a feature to quickly get Photo, video evidence with an external or internal camera or by connecting to the victim or witness's mobile phone, or memory card.	
45	The Solution support case dashboard that displays high level details about the case, evidence sources and summaries of processed results of multiple digital evidence in one screen.	
46	The Solution shall visualize connections between files, users, and devices. Discover the full history of a file or artefact to build case and prove intent. The Solution shall also visualize evidence from disk and memory to show where files came from, who they are connected to, and where they're stored.	
47	The solution shall support pre-processing date filters which gives the Purchaser the option of setting a date and time range for the artefacts that shall be added to a case. This feature allows to limit the artefact data being collected in order to comply with warrant restrictions around the applicable dates for the investigation.	
48	The solution shall support parse and carve and parse selected artefact option to save time on a case if carving is not necessary for investigation.	
49	The solution shall have Timeline explorer to consolidate all the timestamps from files and artefacts in a single view, with colours and tags to differentiate timestamp categorizes.	
50	The solution shall have the ability to automatically find potential chat databases along with other valuable evidence from non-chat apps that aren't yet supported in an artefact. Users can then easily create an Extensible Markup Language (XML) or Python artefact to be searched for in future cases.	
51	The solution shall have the capability for parsing unsupported database using custom artefacts or Python Scripts for popular local applications like Tally, ccleaner, FakeGPS, Linkedin, onion browser bookmarks etc.	
52	The solution shall have a Graphical User Interface/Wizard-driven utility, so no coding experience required to build custom artefacts Comma Separated Value/Delimited files (tab-separated, space-separated, or custom delimiters) and SQLite databases to bring data into the offered tool from other sources without needing to know Extensible Markup Language (XML)/Python or API.	
53	The solution shall have a platform that allows Purchaser's team to access repository of custom artefacts and option to upload custom scripts that they have built, and help their peers with their cases, or download artefacts others have built to help with their own cases.	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
54	The solution shall support addition of hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that shall specifically call out and identify known bad pictures and videos.	
55	The solution shall support enhanced searching, sorting and filtering – search, sort and filter artefact data for relevant keywords, time/date stamps, tags or comments, or layer filter criteria to pinpoint items in a powerful and intuitive, but natural interface. Support filter stacking for multiple filters.	
56	The solution shall support capturing of web pages as they are at a specific point in time for situations where the web pages need to be displayed in an environment where Internet access is not available (such as a court room).	
57	The solution shall support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view.	
58	The solution shall support to export & merge portable case and share with other stakeholders without the need for the software license or the need to install the software, the user can select different types of items to be included according to tags, comments and categories.	
59	The solution shall be capable to generate a load file that can be ingested by eDiscovery review platforms.	
60	Should Support analysis of warrant return from Google, Facebook, Instagram, Snapshot, and iCloud.	
61	The solution shall be capable to acquire evidence from the cloud, by sign into an account with the target's username and password and admin credentials or—for some platforms—an authentication token that the tool discovers during a search or creates itself.	
62	The solution shall collect data from corporate cloud storage services like Amazon Web Services and Azure in addition to communication apps like Slack and Teams. Use Admin credentials to easily acquire from Office 365, G Suite, and Box to speed up investigations.	
63	Should support cloud-based Data acquisition from popular Cloud services, including iCloud, MS Office365, Post Office Protocol (POP)/Internet Message Access Protocol (IMAP) emails, Facebook, Twitter, Google, Slack, Instagram, Box, Dropbox, Microsoft Teams, etc.	
64	Should have ability to acquire public data from Twitter and Instagram without knowing the targeted user’s credential.	
65	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution along with the laptops/PCs from well-known OEMs	

Digital Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
	having latest generation processors/GPUs and SSDs, which should remain in perfect working condition for entire contract period. The MSP shall replace the faulty, underperforming laptops/PCs with new laptops/PCs immediately during entire contract period. Latest version of MS Office suite Professional Standalone version with perpetual license shall also be provided along with each such laptops/PCs.	
66	The MSP shall provide required Forensics Hardware toolkits as part of the solution. The number and type of hardware toolkits shall be provisioned as per project requirement. Any faulty or outdated toolkit shall be replaced with a new and latest toolkit.	

Mobile Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	Solution shall support physical extraction and decoding from Android and iOS based mobile phones and tablets.	
2	Solution shall support physical extraction from phones with Chinese chipsets	
3	Solution shall support physical, system, and logical extractions of intact and deleted data, and passwords	
4	Solution shall support Logical extraction of data: Apps data, passwords, IM (instant messaging), contacts, SMS & MMS, emails, calendar, pictures, audio, videos, ringtones, call logs, phone details (IMEI/ESN), ICCID and IMSI, SIM location information (TMIS, MCC, MNC, LAC)	
5	Solution shall support forensic cloning of SIM ID to isolate the phone from network activity during analysis	
6	Solution shall provide frequent software updates to ensure compatibility with new phones or new Operating system versions as they are introduced to the market during the contract period	
7	Solution shall contain rich set of analysis features including timeline and project analytics, malware detection and watch list	
8	Solution shall support Flexible report generation and customization supporting different report formats	
9	Solution shall support device extraction via USB and RJ 45	
10	Solution shall support SIM clone and extraction	
11	Solution shall have a rich set of decoding: Apps data, passwords, emails, call history, SMS, contacts, calendar, media, location information etc.	
12	Solution shall support simultaneous operations, i.e., extraction, decoding and analysis	

Mobile Forensic Suite		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
13	Solution shall have custom boot loaders to ensure forensically sound extractions	
14	The MSP shall provide the necessary hardware, required mobile devices, software, licenses, storage, network equipment for the deployment and operations of the solution	

Memory Forensic Solution		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	Solution should provide a client-server architecture, where multiple collectors can be deployed across multiple endpoints to collect memory dumps & forensic artefacts. The Collectors should automatically forward the collected memory dump & forensic artefacts to the server for viewing, reporting and analysis	
2	Solution should support memory dump collection and analysis on various operating systems like Windows, MacOs and Linux	
3	Solution should be able to collect and analyze OS Hibernation file, crash dumps & virutal machine snapshots	
4	Solution should have in-built rules and IOCs, for detecting various threats from the collected memory dumps & other artefacts	
5	Solution should support creation of custom workflows, playbooks and visualizations	
6	Solution should support customized report generation	
7	Solution should be able to integrate with SIEM and EDR	
8	Solution should support creation of custom queries to support threat hunting and investigation of the collected samples	
9	Solution should support integration with threat intelligence feeds	
10	Solution should offer a standalone Memory dump & artefacts collector and analyzer for use in air gapped networks, where server connectivity is not available.	
11	Solution should be provided with necessary server sizing to support atleast 100 simulatenous memory and artefact acquisition from 100 unique clients.	
12	Solution should be able to retain collected memory and artefacts for atleast 12 months, necessary compute and storage sizing should be factored in as part of the proposal	
13	There should not be any licensing limitation in the number of collections or sources from where data/artefacts is being acquired and investigated	
14	Solution should be provided with a portable workstation for offline analysis, with the following minimum specifications : Snapdragon x elite 12 core processor, 32 GB RAM, 1TB SSD, 13 inch OLED display, Wifi + 5G Support,	

	magnetic keyboard with haptic touchpad, Windows 11 Pro, MS Office Latest Standalone version, OEM carry case for workstation	

Mac Forensic Suite		
S. No.	**Purchaser's Requirement**	**Compliance (Y/N)**
1	Solution should be able to forensic image and acquire forensic artefacts from latest Mac OS	
2	Solution should support acquisition of memory dump from MacOS	
3	Solution should support forensic imaging of APFS Fusion drives	
4	Solution should support decryption of file vault (where password or keychain file is available)	
5	Solution should have a feature to exclude acquisition of system files	
6	Solution should support hashing of all collected data from target systems	
7	Solution should support acquisition of active system processes, system state, print queue status etc.	
8	Solution should support analysis of data and artefacts collected from Mac OS	
9	Solution should support live triaging of Mac OS based systems	
10	Solution should provide a timeline view of activities based on the analysis of the captured image/forensic artefacts	
11	Solution should support searching and threat hunting across multiple forensic artefacts collected	
12	Solution should allow export of selected forensic artefacts, files from the acquired forensic evidence.	
13	Solution should provide a complete list of users and user activities on the mac OS	
14	Solution should be provided with a portable Workstation for offline analysis with the following minimum specifications : M4 Max 16 core CPU, 32 inch XDR monitor with stand, 128 GB RAM, 8 TB HDD, MS Office latest standalone version,	

Cloud Forensic Solution		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
	Solution should support popular cloud platforms like AWS, Azure, Google Cloud, containers, serverless & on-premise cloud	
	Solution should support importing of events, logs and other forensic artefacts from cloud, EDR/XDR, Agent/Client deployed on the host	
	Solution should provide alerts on security events, incidents	
	Solution should leverage threat intelligence for correlating multiple security events/incidents	
	Solution should support threat hunting queries	
	Solution should provide a timeline view of events	

	Solution should support acquisition of artefacts from containers, memory and disk	
	Solution should have in-built yara rules for detecting various security threats	
	Solution should support export of incidents to SIEM and SOAR platform	
	Solution should support triaging and full scale acquisition of forensic data	
	Solution should provide MITRE mapping for the events	
	Solution should support full disk acquisition across cloud platforms	
	Solution should be able to perform remediation actions including stopping, containing or isolating cloud instances to prevent damage and spread.	
	Solution should be able to automatically construct key incident details including root cause, compromised roles and assets, and more	

Steganography Solution		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
	Solution should be able to generated advanced attack payloads	
	Solution should support deployment of payloads by using steganography	
	Solution should support transformation of binary script based payloads like HTA, Jscript, Vbscript..etc to create various payloads	
	Solution should support integration of steganogarphy payloads into MS Office documents and also support VBA Macro payload creation for MS Office documents	
	Solution should be able to alter the metadata of MS Office documents	
	Solution should have an in-built C2 framework, with support for deployment of implants across Windows, Mac OS & Linux OS.	
	Solution should have in-built anti-forensic mechanism to generate payloads which can bypass Antivirus/EDR, User Account Control	
	Solution should support lateral movement through the C2 framework	
	Solution should support obfuscation techniques for hidhing malicious behaviour/code	
	Solution should support DLL Hijacking to perform local privilege escalation attacks	
	Solution should support covert interaction with target's system	
	Solution should be able to simulate various attack techniques	
	Solution should be able to identify potential blue team activities and report them	
	Solution should be able to perform a range of activities on the target system which inlcudes but not limited to the following : 1) Dump user tokens 2) Extract NTLM hashes	

eDiscovery Forensic Data Analytics Platform		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1.	Solution should support ingestion & processing of massive volumes of Electronically Stored Information (ESI) in the range of 1TB per day	
2.	Solution should support processing, investigation, analysis, review of the ingested data	
3.	Solution should be able to integrate with leading digital forensic platform for automatic forensic data ingestion	
4.	Solution should support search and retrieval of search results in less than 10 seconds for a data size of 500 TB	
5.	Solution should be able to automatically identify the type of ingested data and classify it accordingly	
6.	Solution should support quick culling, key word search and data deduplication	
7.	Solution should be able to process major file formats out of the box	
8.	Solution should be able to process all languages, character sets, metadata, and all associated, attached, embedded files, irrespective of the depth of heirarchy , compression or naming convention	
9.	Solution should be able to analyze all metadata, text and binary of documents to forensically identify relevant information, while preserving the chain of custody during the process	
10.	Solution should provide an interactive Graphical User Interface, which helps an investigator to drill down specific information, investigate, analyze or review content.	
11.	Solution should be able to automatically establish relationship between multiple data sets and simplify the understanding of the relationships	
12.	Solution should support retrieval of deleted and encrypted information	
13.	Solution should be able ot identify whether two documents are similar or same, even if file name prefix or suffix is modified	
14.	Solution should be able to identify non-english documents and provide generalized translations	
15.	Solution should have in-built AI engine for classification and analysis of ingested data	
16.	Solution should support complex keyword searches, including regular expression, wildcard, multiple wildcard, boolean, fuzzy, phrase, proximity, range and field level searches	
17.	Solution should support redaction of specific content as per the requirements of the user	
18.	Solution should support export into variety of formats including HTML, PDF, TXT, TIFF, CSV..etc.	
19.	Necessary server side infrastructure, in high availability mode, should be provided by the bidder, with a sizing to accommodate at least 500 TB of data, with high endurance Flash drive or nvme for storage	

Network Forensics		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1.	Overall Solution should be able to capture network traffic with bandwidth of 40 Gbps or more, with each single physical appliance supporting atleast 10Gbps or more	
2.	Solution should support both inline deployment and TAP mode deployment for capturing network packets	
3.	Overall Solution should be able to perform lossless packet capture with timestamping at the rate of 40 Gbps or more	
4.	Solution should have the option of capturing only metadata of the raw network traffic	
5.	Solution should support various formats including netflow v9, IPFIX, SiLK…etc.	
6.	Solution should have in-built traffic fingerprinting engine, which should be able to detect various application layer traffic and other layer traffic like email, FTP, DNS, TLS etc.	
7.	Solution should have in-built traffic analyzer, with investigation support for running custom queries on the captured traffic	
8.	Solution should be able to capture selective network traffic based on the user defined rule	
9.	Each physical appliance should have atleast 2x40 G QSFP port, with in-built storage of atleast 700 TB	
10.	Solution should deliver consistent 20 Gbps packet capture rate, with meta data analysis and 10,000 IDS inspection rules applied	
11.	Solution should support regular expression, wild card and custom key word based queries on the captured network data	
12.	Solution should allow download of whole or specific packet capture data based on the condition/rule supplied by the user	
13.	Solution should have automatic indexing capability for metadata from the captured network traffic	
14.	Solution should have in-built threat intelligence and signatures of various latest threats, attacks, exploits and malwares	
15.	Solution should support integration with Threat Intelligence Platform (TIP) for ingestion of NIC's in-house threat intelligence and subscribed intel	
16.	Solution should support reconstruction of suspicious files, web pages, emails …etc., for further investigation	
17.	Solution should support extension of storage through an external storage like SAN, with capacity to scale upto 10 petabytes	
18.	Necessary hardware for the solution should be provided by the bidder for high availability deployment, with capacity to capture and retain network traffic data of upto 1 PB on day one.	

19.	Necessary hardware and licenses for network TAPS or sensors for capturing traffic between specific source and destination should be provided by the bidder	

Data Recovery Solution		
S. No.	**Purchaser's Requirements**	**Compliance (Y/N)**
Data Recovery		
1.	The Solution shall include both hardware and software with PCI-Express Interface with minimum two native SATA ports and one IDE port	
2.	The Solution shall Support IDE (CE, CF, ZIF), SATA (MICRO SATA) interface Hard Disks	
3.	The Solution Should Support 1.8-inch, 2.5 inch, and 3.5 Hard Disks with a capacity of up to 5TB	
4.	One-click automatic HDD diagnostic repair module, for SATA disks.	
5.	The solution shall have an Efficient USB terminal that can work with Hard Disks of different OEMs	
6.	The Solution shall support Flash ROM programming unit	
7.	The Solution support the recovery of corrupted firmware in HDDs	
8.	The Solution shall support the ability to unlock and reset hard drive password (i.e., decrypt the hard drive)	
9.	The Solution shall Support data recovery and Hard Disk repair due to failed read/write heads	
10.	The Solution shall support virtual head map technology	
11.	Should Support the repair of SATA HDDs with physically-damaged sectors.	
12.	The Solution shall support disk imaging, imaging by selective head, file recovery	
13.	The Solution shall support head map editing in RAM for data recovery	
14.	The Solution shall support review of defect tables (P-list, G-list, T-list, etc.)	
15.	The solution shall be able to Load the service information access program – LDR (Loader)	
16.	The solution shall be able to hide identified defects of magnetic surface	
17.	The solution shall provide direct read and write to hard disk SA track	
18.	The solution shall be able to perform forward and reverse scan and directly recover data from bad sectors	
19.	The solution shall be able to perform Master File Table scan to recover accidentally deleted files	
20.	The solution shall support File Carving	
21.	The solution shall support File recovery from unallocated space	
22.	The solution shall support Partition recovery	
23.	The solution shall support almost all known file systems (FAT32, FAT, NTFS, EXT, APFS etc)	
24.	The solution shall provide Power backup for hardware device.	
25.	The Solution shall provide Reporting facility	

Data Recovery Solution		
S. No.	**Purchaser's Requirements**	**Compliance (Y/N)**
26.	Should be a portable form factor external device with USB 3.0 interface	
27.	The device should have the diagnostic ports for USB 3.0 (host), Port 0 (PCIe / SATA), and 2 SATA Ports	
28.	The solution should be able to connect and recover data from hard disks from different OEMs including but not limited to Seagate, Western Digital, Toshiba, Samsung, Maxtor, Hitachi, Corsair, Sandisk, G.Skill, Micron, Intel, Transcend, Patriot, Crucial, A-Data, Kingston, PNY, AMD & Quantum.	
29.	The solution should support data recovery from SATA Disks, USB 2.0 & 3.0 Disks, SAS, M.2 PCIe NVMe, mSATA, Apple MacBook SSD, Solid State Hybrid Drives (SSHD), SD/Micro SD Cards, PATA (with IDE interface)	
30.	Solution should support recovery from different file systems including but not limited to FAT, exFAT, NTFS, ReFS, APFS, EXT 2/3/4, VMFS, HFS+, ZFS, Virtual machine images.	
31.	Solution should support recovery from RAID arrays	
32.	Solution should support recovery of data from android mobile devices which are based on Mediatek, Qualcomm and Spreadtrum/UNISOC processors.	
33.	All necessary cables, interfaces, hardware and software required for fulfilling the functionality of the solution should be provided along with the solution.	
34.	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution along with the Workstations/PCs having latest generation processors and SSDs, which should remain in perfect working condition for entire contract period. The MSP shall replace the faulty, underperforming workstations with new workstations immediately during entire contract period. Latest version of MS Office suite Professional Standalone version with perpetual license shall also be provided along with each such laptop/PC.	
35.	Required Hardware Specification for portable data recovery solution: Portable Tablet form computer, with Min. Latest gen Core 19-13900H cpu with 2.6 GHz, 32 GB LPDDR5 Dual Channel RAM, Nvidia RTX 4070, 8GB GPU, 1TB NVMe M.2 SSD, Pantone validated 34.03 cm size IPS Touch display with 2560x1600,WQXGA) 165 Hz , Wifi 6E (802.11AX) Dual band, Bluetooth 5.2 card, with less than 1.5 Kg, with backlit chiclet keyboard and stylus. With licensed latest pro version of windows and standalone offline MS Office pro suite with perpetual license. All supplied laptops/tablets should be provided with the laptop/tablet bags.	
36.	Required Hardware Specification for PCIe based data recovery solution:	

Data Recovery Solution		
S. No.	**Purchaser's Requirements**	**Compliance (Y/N)**
36.a	Latest Gen Core i9, H series Processor, with 64 GB DDR5 RAM, 4 TB Nvme SSD, 10 TB SATA HDD, 34 inch QD-OLED Monitor, 2 Empty PCI-e slots, vertical ergonomic mouse, curved split keyframe keyboard .	

SOC Logistics Tools		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	4TB Portable Nvme SSD	
2	20 TB Portable SATA Hard Disk with min. 7200 rpm	
3	Faraday Bags for laptops and hard disks	
4	Portable forensic suitcase with EMF shielding to accommodate forensic laptops, hard disks, imaging/cloners, wires and other equipment	
5	256 GB USB Flash Drive with in-built hardware write blocker	
6	8 TB portable SSD drive with in-built hardware write blocker	

	Network Attached Storage (NAS)	
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1.	Total Memory (RAM) Size Installed (in GB) - At Least 32GB	
2.	Architecture Type - Processor	
3.	Number of Controller/Node/Processor - 1	
4.	Number of Controller Failure for Uninterrupted - 1	
5.	Encryption – Software based	
6.	Protocols Supported - NFS (Network File System),SMB / CIFS (Serve Messaging Block / Common Internet File System)	
7.	Backup Features - Snapshot, Replication	
8.	Type of Storage Interface – SAS SSD	
9.	Hot Swappable	
10.	Capacity Offered per SAS SSD (in GB) – 30 TB	
11.	RAID level - 5	
12.	Total Number of Ethernet Ports - 2 x 1G, 2 X 10G	
13.	Operating System Supported - Windows/Linux	
14.	Redundant Power Supply	
15.	Hot Swappable (Redundant Power Supply)	
16.	Redundant Fan	
17.	3 Years onsite Warranty	

Forensic Workstation		
S. No.	**Purchaser's Requirements**	**Compliance (Y/N)**
1.	Intel Core Ultra 9 285K CPU with 24 Core	

2.	256 GB DDR5 RAM	
3.	8 TB NvMe M.2 PCIe Gen4 SSD	
4.	Nvidia RTX 5090 32GB GDDR7 GPU	
5.	2xUSB 3.2 Gen2 Type-C (10Gbps) port with powershare	
6.	2xUSB 3.2 Gen1 Type-A (5Gbps) port	
7.	1xRJ-45 Killer E3100G 2.5 Gigabit Ethernet	
8.	2xThunderbolt 4 prots	
9.	Intel Killer Wifi 7 BE1750 (2x2 320Hz) Wireless LAN and Bluetooth 5.4	
10.	1500W Platinum rated PSU	
11.	OEM Keyboard and Mouse	
12.	Latest Windows Enterprise License	
13.	Latest MS Office Pro standalone license	
14.	34 inch OLED/QD-OLED Monitor with 4K/WQHD resolution	
Forensic Laptop		
1.	Intel Core Ultra 9 275HX with 24 Core	
2.	128 GB DDR5 RAM	
3.	4 TB NvMe M.2 PCIe Gen4 SSD	
4.	Nvidia RTX 5080 16GB GDDR7 GPU	
5.	In-built UHD camera with dual array microphone	
6.	Intel Killer Wifi 7 BE1750 (2x2 320Hz) Wireless LAN and Bluetooth 5.4	
7.	16 inch WQXGA Display	
8.	Latest Windows Enterprise License	
9.	Latest MS Office Pro standalone license	
10.	OEM Laptop Bag with shockproof and EMF shielding	
Forensic Tools		
Hackone RFOne Bundle, Flipper Zero, Proxmark3, Rubber Ducky etc. as per need for SOC operations.		

SOC Logistics Tools		
S. No	**Purchaser's Requirement**	**Compliance (Y/N)**
1	4TB Portable Nvme SSD	
2	20 TB Portable SATA Hard Disk with min. 7200 rpm	
3	Faraday Bags for laptops and hard disks	
4	Portable forensic suitcase with EMF shielding to accommodate forensic laptops, hard disks, imaging/cloners, wires and other equipment	
5	256 GB USB Flash Drive with in-built hardware write blocker	
6	8 TB portable SSD drive with in-built hardware write blocker	

Governance Risk & Compliance Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
1	The Solution shall be capable of integrating via APIs with other tools including provide built in as well as customizable workflows to track, IT compliance Risk issues, third party risk management, Cyber threats, vulnerabilities, Vulnerability Assessment Penetration Testing Findings,	

Governance Risk & Compliance Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
	Audit Findings, Compliance findings, internal/external audits, critical incidents etc. Shall support role-based access.	
2	The Solution shall support advanced workflow capabilities such that multiple simultaneous paths/tasks and return back to earlier steps, phases or stages. The workflow configuration shall be driven via a graphical user interface.	
3	The Solution shall provide the ability to document, track, and monitor sign-off / approvals for any issues or actions.	
4	The Solution shall have option to store Content (policies, controls, report templates, reference documentation)	
5	The Solution shall allow users to view policies and search by criteria such as policy type, geography, role, etc.	
6	The Solution shall allow users to perform keyword searches to quickly find specific information among various IT / Accounts / Cyber Security and other policies as desired by the Purchaser.	
7	The Solution shall document the IT and Cybersecurity infrastructure including overview of business products/services, business processes. information assets, facilities and personnel and hierarchy of the Department.	
8	The system shall have surveys and questionnaires and automatically generate findings for incorrect responses.	
9	The Solution shall be able to manage the lifecycle of remediation plans, and it shall also have the remediation action.	
10	The Solution shall be able to track and monitor control implementation status	
11	The Solution shall have capability to use external data by having an Application Programming Interface (API) connection or any alternate connection/ upload method with the data source.	
12	The Solution shall have predefined assessment templates for global standards and allow and customizable assessment template as per Purchaser’s policies, standards, and other requirements.	
13	The Solution shall have pre-mapped controls for global standards and frameworks which include, ISO 27001/27002/27005/27032, Centre for Internet Security Benchmarks, Control Objectives for Information Technologies (COBIT), National Institute of Standards and Technology, IT Amendment Act 2008, Payment Card Industry Data Security Standard, Information Technology Infrastructure Library (ITIL) v4.0.	
14	The Solution shall have the ability to document and maintain external benchmarks, frameworks, laws, and regulations identified for meeting the corporate objectives.	

Governance Risk & Compliance Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
15	The Solution shall offer a library of technical baseline configuration procedures mapped to various regulatory standards / technologies. Along with implementation guidelines	
16	The Solution shall provide top-down or bottom-up approaches to developing key control procedures aligned with the compliance requirements as desired by the Purchaser	
17	The Solution shall facilitate that Compliance requirements can be mapped to a business function	
18	The Solution shall have capability to record the non-compliance instances by capturing related information.	
19	The Solution shall have the ability to provide built-in assessments, Control Self Assessments (CSA) and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing	
20	The Solution shall support applying weight to questions and responses	
21	The Solution shall be able to collect and store the Management responses	
22	The system shall have the ability to track outstanding issues and assigned task.	
23	The Solution shall have capability to perform gap analysis	
24	The Solution shall support risk assessments for both inherent and residual risk	
25	The Solution shall have the ability to document control activities and capture details like control owners, testing requirements, mapping with compliance, risk, business unit etc.	
26	The Solution shall be able to capture robust details about each risk item including objectives, products and services, business processes, risks, threats, vulnerability, impact, like hood controls, physical facilities, technology assets, policies, and procedures.	
27	Risk assessments must have both qualitative and quantitative approaches.	
28	The Solution shall calculate, display, and report risk scores. Risk calculations must be transparent to users.	
29	The Solution shall give users full control over risk calculation parameters, weightings	
30	The Solution shall allow for aggregation of risks across the organisation	
31	The solution must keep the History of last 5 years risk	
32	The Solution shall have the ability to capture and document risk response procedures as well as mitigating controls	

Governance Risk & Compliance Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
33		
34	The Solution shall have the ability to link, and map identified risk to Authoritative Sources, departments, asset, and divisions	
35	The Solution shall be enabled to manage exceptions with appropriate risk sign-off/acceptance	
36	The Solution shall provide the capability to document and capture details of stakeholders identified like asset owner, risk owner, control owners etc	
37	The Solution shall provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.	
38	The Solution shall have capabilities to perform risk assessments as per risk category and/or threat category	
39	The solution shall have capability to perform third-part risk assessment and shall have ability to capture contracts and master services agreement associated with third party	
40	The Solution shall have capability to define and automate the frequency of conducting the IT and Cyber Security risk assessment and automatically generating reports across various levels such as business unit head / manager, asset owner as well as board and management levels.	
41	The Solution shall include multiple impact categories to evaluate criticality of the business process	
42	The Solution shall capture recovery time objective (RTO) and recovery point objective (RPO) for business processes and calculate the result as overall business criticality rating for the asset and/or process.	
43	The Solution shall include workflow for multiple participants (Approx. 10-15) in the BIA (Business Impact Analysis) process, including the business process owner and others that may need to provide input, as well as review by another level and the relevant teams.	
44	To support the Business Impact Analysis, the Solution shall enable mapping of business processes to their supporting IT Service, Process, Third Party, and Personnel.	
45	The Solution shall be able to generate report of ISO 27001 statement of applicability based on controls already existing or controls which are planned to be implemented.	
46	The Solution shall be able to generate report on control effectiveness metrics for continual improvement of Information Security Management System (ISMS).	

Governance Risk & Compliance Platform		
S. No	**Purchaser's Requirements**	**Compliance (Y/N)**
47	The Solution shall provide the ability to create a risk summary report that describes key risks, how they are being managed and monitored, remediation of key issues and accountability.	
48	The Solution shall be able to generate report on Risk levels on risk assessment and risk treatment to showcase mitigation status	
49	The Solution shall be able to generate risk treatment plan implementation progress report	
50	The Solution shall be able to demonstrate open risk status with implementation progress, control gaps and assets affected	
51	The Solution shall show dashboard including current audit findings, remediation, and responsibility.	
52	The Solution shall be able to generate reports on audit findings, remediation, and responsibility	
53	The Solution shall have options to display all the asset, risk, audit, action items and training related metrics in one single dashboard	
54	The Solution shall provide a variety of layout options enabling business user to alter the user interface/dashboard	
55	The Solution shall have capability to enable separate interface wherein MSP can login and provide response and upload artefacts	
56	The Solution shall provide Enterprise risk management system and Enterprise Audit Management	
57	The MSP shall provide the necessary hardware, software, licenses, storage, network equipment for the deployment and operations of the solution	
58	The solution should support upto 50 users with 10 concurrent users.	

Note :

1. Bidder has to ensure that the quoted solutions comply with the all technical specifications
2. Bidder shall ensure appropriate evidences to prove the compliance are made available to the Purchaser
3. At any point of time, Purchaser may request the Bidder to provide the proof of compliance and a live demonstration of the solution to verify the compliance.

16. Operational Manpower Skillset

16.1 High Level Skill Set of Operational Manpower

Qualification: Minimum qualification for all the manpower resources required to be deployed at SOC (Except Office Assistants) should be BE/B.Tech/MCA from a Government recognised university/college. The experience and required skillset should be as given in Table 17 below:

TABLE 17: HIGH LEVEL SKILL SET OF OPERATIONAL MANPOWER

S. No	Resource Type	Skill Sets	Location of Deployment & Minimum Qty of Manpower and Shift Requirement.
1	Project Manager	Should have at least 10 years of experience in handling similar large projects in the area of technology transformation, program governance, cybersecurity implementations, SOC, extended location, log management etc.	Refer Annex 16
2	Administrators for SIEM, SOAR, TIP and Ticketing platforms	Hands on experience and expertise in installation, configuration, troubleshooting, operating and managing the respective components including but not limited to network, security, and storage. Hands on experience in operations of the respective paltforms.	Refer Annex 16
3	**Security Breach Investigation Specialist, to work on :** Attack Simulation Platform, Security Testing Platform & Application Security, SAST/DAST, PIM/PAM, Digital Forensic Suite/ Digital Incident response tool, Data and Password Recovery, Mobile Forensics Tools and Forensic Disk Imager with Hardware write blocker and Magnetic Media Degausser & Secure Drive Eraser	•Expertise in Malware Reverse Engineering, Exploit Development, •Security Breach Investigation & Threat Hunting. • Experience in binary diffing/patch analysis. • Strong Hands on expertise in PE32/PE64 files analysis, x86 and x86- 64 assembler, Windows, Linux & Android OS internals - Kernel, memory, threads, processes, API, etc. • Strong Hands On expertise in disassemblers and debuggers (IDA Pro, HIew, WinDbg, OllyDbg, etc.) • Knowledge and understanding of file formats and network protocols • Experience with network traffic analysis tools (like Wireshark, Fiddler) • Strong hands-on expertise in detecting, investigating security incidents and breaches.	Refer Annex 16

		• Analysis and reversing of source codes compiled in different programming languages • Cyber Forensics • Should have worked as a part of security breach investigation team for at least 5 years. • Should have hands-on expertise and deep understanding of OS internals of Linux, MAC and Windows environments.	
4	Malware Analysis Expert:	Expertise in Malware Reverse Engineering, Exploit Development, Security Breach Investigation & Threat Hunting. • Experience in binary diffing/patch analysis. • Strong Hands-on expertise in PE32/PE64 files analysis, x86 and x86-64 assembler, Windows, Linux & Android OS internals - Kernel, memory, threads, processes, API, etc. • Strong Hands-On expertise in disassemblers and debuggers (IDA Pro, HIew, WinDbg, OllyDbg, etc.) • Knowledge and understanding of file formats and network protocols • Experience with network traffic analysis tools (Wireshark, Fiddler) • Analysis and reversing of source codes compiled in different programming languages •Strong Programming experience in C/C++, Python, Javascript, Bash & Powershell Scripting • Cyber Forensics	Refer Annex 16

5	Platform Security Expert and System Administrators (Windows, Linux, Mac OS, Virtualisation etc.)	Strong understanding and expertise along with relevant experience of at least 5 years in Linux/MAC/Windows environments. **Linux Security:** • In-depth knowledge of Linux Kernel • Expertise in Scripting languages - bash/shell • Linux internals, Linux packaging, • Expertise in GPG signature/checksum validation of binary components • Debugging and investigation of running services, processes • Linux OS Security Hardening • Expertise in Linux OS Breach Investigation • Hands on Expertise in open source webservers, proxy servers, IP tables • Expertise in analysing kernel dumps, tcp dumps, linux logs • Expertise in Linux OS Security Audit **Windows Security:** • In-depth knowledge in windows server and desktop operating system internals • Hands on expertise in Active Directory, Windows Clustering, IIS, Hyper-V • Expertise in Powershell scripting, batch scripting • In-depth knowledge of Windows Registry • Hands on expertise in Windows log analysis • Expertise in Windows OS breach investigation • Expertise in analysing OS crash dumps, tcp dumps, process dumps • Expertise in Windows OS Security Hardening	Refer Annex 16

		• Expertise in Windows OS Security Audit **Mac OS Security:** • Hands on expertise on MacOS – Kernel, file system, administration, and security architecture • Expertise in reverse engineering MAC OS binaries and firmware components like Mach-O, dyld and KEXTs. • Experience and expertise in MacOS Security breach investigation • Hands on expertise in analyzing Mac OS kernel dumps, memory dumps and process dumps. • Hands on scripting knowledge on shell scripts, Zsh Script and Apple Script. **Database Expert:** • Hands on expertise in RDBMS & No SQL Databases • Expertise in Re-creating, analysing, troubleshooting, and diagnosing incidents • Determines root cause of incidents (configuration vs. defect) • Expertise in Database log analysis, transaction log analysis • Expertise in Database replication, backup, business continuity & Disaster Recovery • In-depth knowledge in Database configuration, Clustering, query analysis • Expertise in Database breach investigation • Expertise in Database Security Audit	
6	ISO 20000 Expert	ISO 20000 Lead Implementer certified resource, with hands on experience in ISO 20000 implementation for more than 3 years	For Implementation of and training on ISO 20000 as per requirement under this RFP

7	ISO 27001 Expert	ISO 27001 Lead Implementer certified resource, with hands on experience in ISO 27001 implementation for more than 3 years	For Implementation of and training on ISO 27001 as per requirement under this RFP
8	Log Analysis/Data analytics and Threat Hunting Professional:	1 Having more than 5 years of experience. 2 Search for vulnerabilities and risk factors in data and systems. 3 Stay up to date on the latest innovation in cybersecurity. 4 Study trends in cybercrime around threat actors' behaviors, tactics and goals. 5 Analyze collected data to find potential anomalies in the security environment. 6 Eliminate any risks and vulnerabilities. 7 Search and track hidden threats. 8 Assist IT teams in using the appropriate methods, tools, and techniques to detect and mitigate cyber threats 9 Search for security gaps by performing risk assessment, penetration testing, and identifying internal risks	Refer Annex 16
9	SOC Analyst	1 Having more than 3 years of experience. 2 Identifying and resolving incidents in a timely manner 3 Keeping relevant parties updated on the status of incidents 4 Developing and implementing processes and procedures for incident management 5 Overseeing the work of incident response teams 6 Follow escalation matrix and escalate incidents as needed 7 Reporting on incidents and trends 8 Strong analytical and problem-solving skills	Refer Annex 16

		9 Excellent communication and interpersonal skills 10 Ability to work well under pressure and meet deadlines	
10	Windows, Linux, MacOS, Memory, Android, IoS, Forensics expert.	Strong understanding and expertise along with relevant experience of at least 5 years in Linux/MAC/Windows environments. Linux Security : • In-depth knowledge of Linux Kernel • Expertise in Scripting languages - bash/shell • Linux internals, Linux packaging, • Expertise in GPG signature/checksum validation of binary components • Debugging and investigation of running services, processes • Linux OS Security Hardening • Expertise in Linux OS Breach Investigation • Hands on Expertise in open source webservers, proxy servers, IP tables • Expertise in analysing kernel dumps, tcp dumps,linux memory dumps, linux logs • Expertise in Linux OS Security Audit **Windows Security:** • In-depth knowledge in windows server and desktop operating system internals • Hands on expertise in Active Directory, Windows Clustering, IIS, Hyper-V • Expertise in Powershell scripting, batch scripting • In-depth knowledge of Windows Registry	Refer Annex 16

		• Hands on expertise in Windows log analysis • Expertise in Windows OS breach investigation • Expertise in analysing OS crash dumps, tcp dumps, windows memory dumps, process dumps • Expertise in Windows OS Security Hardening • Expertise in Windows OS Security Audit **Mac OS Security:** • Hands on expertise on MacOS – Kernel, file system, administration, and security architecture • Expertise in reverse engineering MAC OS binaries and firmware components like Mach-O, dyld and KEXTs. • Experience and expertise in MacOS Security breach investigation • Hands on expertise in analyzing Mac OS kernel dumps, memory dumps and process dumps. • Hands on scripting knowledge on shell scripts, Zsh Script and Apple Script. **Android Security:** • Hands expertise on Android OS kernel and security architecture • Knowledge of Android security basics: root , SELinux, APK signing, screen locks (including FaceID/fingerprint/PIN/password bypass), OTA updates, etc. • Familiarity with common vulnerability principles: experience in successful vulnerability mining/exploitation of heap overflow, UAF (Use-	

		After-Free), process injection, privilege escalation, etc. • Strong knowledge of Android operating system principles, understanding of ARM architecture • Expertise in Java/C/C++ development, knowledgeable about packaging, decompiling, and cracking processes • Expertise in shell unpacking, obfuscation countermeasures; experienced in Ollvm obfuscation and practical counter-strategy; • Knowledge in Android device fingerprinting and environmental analysis countermeasures. • Expertise in exploitation techniques, including but not limited to cross-cache attacks, heap groom, file/process injection, GPU vulnerability exploitation, mitigation bypass, etc. • Strong knowledge of cryptography, security protocols, reverse engineering, fuzzing. **iOS Security:** • Hands expertise on iOS kernel and security architecture • Strong understanding of current bug classes and patterns. • Expertise on iOS memory management, application sandboxing, Mach and XPC-based IPC, and Apple's code signing mechanisms. • Knowledge on techniques and packages used for jailbreaking and rooting. • Hands-on experience with hooking and instrumentation frameworks used in iOS	

		• Expertise in manual analysis of iOS Apps, reverse engineering.	
11	AI Engineer	• Strong programming knowledge on Python, Java, C, C++ and R • Expertise in TensorFlow, PyTorch, Scikit-learn, and Pandas. • Strong understanding of machine learning algorithms, deep learning architectures (e.g., CNNs, RNNs, Transformers), and data structures. • Expertise in Large Language Models and Generative AI. • Expertise to Design, train, and evaluate machine learning and deep learning models for a variety of tasks, including but not limited to, predictive analytics, image recognition, and natural language understanding • Implement and manage the end-to-end machine learning operations (MLOps) pipeline, from data ingestion to model deployment and monitoring. • Continuously monitor and optimize the performance of deployed models, ensuring efficiency and accuracy	Refer Annex 16
12	Full Stack developer	• Strong knowledge in java script • React/ angular proficiency • Back end hands on in node/ springboot/ APIs • Handling of large volume datasets	Refer Annex 16
13	GRC Experts	• GRC Professional certification along with over 5 years' experience in implementation of GRC in a large enterprise.	Refer Annex 16

Annexures

Annex 1 – Arrangement with Sub-contractors / Service Providers

The MSP is required to provide the details of the activities that it proposes to subcontract (if required) to third parties. The above arrangements shall be supported with relevant documentary evidence.

Table-1: Subcontracting Details

Name of service	Description of Service (Installation / Cabling / Maintenance / Others)	Proposed party for subcontracting
Audit	Manpower for ISO	
Installation , Commissioning and integration	Cabling and installation of other passive components as part of integration and commissioning	
Training and Support	Operational training	
Documentation	Preparation of user manuals, reports etc.	
Any Others*		

* For others, please mention the component and provide the necessary details

Annex 2 – Instructions to fill the Bill of Material

a) Bidder shall provide all prices as per the prescribed format under this Annexure. Bidder shall not leave any field blank. In case the field is not applicable, Bidder shall indicate "0" (Zero) in all such fields. Quoting of zero (0) as rate for a specific item shall imply that there shall be no charges on any level of usage of that particular item during the Contract Period including the extension. However, quoting of NIL value/no/dash (-) for any item, as listed in the detailed financial Bid shall imply that the Bidder has quoted zero (0) as rate for a specific item. Purchaser in such case reserves the right to seek clarification/ undertaking from the Bidder. If the Bidder fails to agree or provide undertaking for the clarification, Purchaser reserves the right to consider rejecting the Bid of the Bidder.

b) All the prices (even for taxes) are to be entered in Indian Rupees ONLY **(%age values are not allowed)**

c) It is mandatory to provide breakup of all Taxes, US Dollar component, Duties and Levies wherever applicable and/or payable while submitting the financial Bid (refer **Annex 5— Bill of Material**).

d) The rate revision due to dollar fluctuation shall be considered when the average monthly fluctuation is ±10% of the above reference value. The revised rate shall become the reference value for any further rate revision and so on. If the fluctuation is upwards/downwards, the Purchaser, on the request of the MSP shall initiate the process for increasing or reducing the rate by following the same procedure. The documents in support of claims for such variations shall be submitted by the MSP.

e) Purchaser reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.

f) In case any line item is already in support, or no support is available, the same shall be marked as "0" (zero) and highlighted separately.

Annex 3 – Abridged Financial Bid

Abridged Financial Bid for Submission of Grand Total Value
Prices shall be quoted in Indian Rupees (inclusive of all taxes) and indicated both in figures and words. **Price in words shall be considered for evaluation, in the event of any mismatch**.

Table-1: Grand Total Value

Grand Total Value (GTV) i.e., value of **Annex – 4** (Detailed Financial Bid, in figures)	
(Rupees_____) in words	

Note: The Bidder shall ensure that the Grand Total Value given in **Annex 3** (Grand Total Value) must match the Grand Total Value given in **Annex 4** (Detailed Financial Bid).

Place:
Date: **Authorised Signatory Name:**

Annex 4- Detailed Financial Bid

Bidder Name: .....

Prices in the Financial Bid (Inclusive of all Taxes) shall be quoted in the following format. All prices shall be quoted in Indian Rupees and indicated both in figures and words. Figures in words shall prevail.

Grand Total Value (GTV)

The grand total value shall be derived as below:

Grand Total Value (GTV) = shall be the sum total of the following components, inclusive of all taxes:

Table-1: Grand Total Value

S. No	Component Name (A)	Amount (in INR) (B)
1.	Grand Total of Table for Platform and Components (Refer Annex 5, Table - 1) - **B1**	
2.	Total one-time cost for Installation, commissioning of all S/W. (Refer Annex 5, Table - 2) - **B2**	
3.	Cost for comprehensive security Audit of entire supplied and deployed components (Refer Annex 5, Table - 4) – **B3**	
4.	Cost incurred for Training & Support requirements (Refer Annex 5, Table - 5) – **B4**	
5.	Total Cost of Manpower (Refer Annex 5, Table - 6) – **B5**	
6.	Any Other Miscellaneous Expenses – (Refer Annex 5, Table - 7) **B6**	
7.	Cost for Forensic Investigation (Refer Annex 5, Table - 8) – **B7**	
	GTV (B1+B2+B3+B4+B5+B6+B7) in figures	
	GTV (B1+B2+B3+B4+B5+B6+B7) in words	

Place:
Date:

Authorised Signatory Name:

Annex 5 – Bill of Materials (BoM)

Bidder Name: .....

5(A) Table for Platforms and Components

Table–1: Cost of software platforms and components

S. No.	Item	Make and model of the item	Unit Cost (in INR)	GST on Unit Cost (in INR)	Unit Cost Incl. GST (in INR)	Qty	Total Cost (in INR)	AMC cost 2nd Year (Incl. GST)	AMC cost 3rd Year (Incl. GST)	Grand Total Cost for 3 years (in INR)
1	**Security Incident Event Management (SIEM)**									
1a	SIEM (Unlimited License with at least 7 Lakh EPS)									
1b	Software with licences for additional 1 Lakh EPS									
2	**Security Orchestration Automation Response (SOAR)**									
2a	SOAR (Unlimited License with at least 50 users)									
2b	SOAR (Additional 10 users)									
3	**Information Technology Service Management (ITSM)**									
3a	Software with licences for 500 users and 250 concurrent users									
3b	Software with licences for additional 100 users and additional 50 concurrent users									
4	**Threat Intelligence Platform (TIP)**									

5	**Attack Surface Management Platform (Unlimited cloud-based license)**									
5a	Software with licences for 10000 FQDNs, /16 network segments (2 Nos) /20 Network segments (1 No.)									
5b	Software with licences for additional 1000 FQDNs)									
6	**Attack Simulation Platform**									
7	**Security Testing Platform**									
8	**Dynamic Application Security Testing (DAST) Tools.**									
9	**Threat Intelligence (IP & Web Reputation Feeds)**									
10	**Threat Intelligence (IOC Feeds)**									
11	**Threat Intelligence (Deep Web, Dark Web, Social-media & OSINT Feeds)**									
12	**Incident Response Retainer service from a security OEM**									
13	**Digital Forensic Incident Response Tool**									
14	**Portable Log Analyzer**									
15	**Forensic Disk Imager with hardware write blocker along with required forensic hardware toolkits.**									
16	**Magnetic Media Degausser and Secure Drive Eraser**									
17	**Static & Dynamic Analysis Sandbox from 3 OEMs**									
18	**Digital Forensic Suite**									
19	**Mobile Forensic Suite**									
20	**Memory Forensic Suite**									

21	**MAC Forensic Suite**									
22	**Cloud Forensic Solution**									
23	**Steganography Forensic Solution**									
24	**eDiscovery Forensic Data Analytics Platform**									
25	**Network Forensics**									
26	**MacOS Data Recovery**									
27	**SOC Logistics Tools and standalone storage systems for system Image storage.**									
28	**Forensics work stations**									
29	**Forensic Laptops**									
30	**SOC workstations**									
31	**SOC Laptops**									
32	**Forensic Logistics Tools (Hackone RFOne Bundle, Flipper Zero, Proxmark3, Rubber Ducky etc.)**									
32a										
32b										
32c										
32d										
32e										
32f										
33	**Laying of Inter building fiber cable between adjacent buildings for connecting the GSOC with NICNET/NKN**									
33a										
33b										
33c										
33d										
33e										
33f										

34	**Supply and installation of Active LAN components (Router, switches, access points etc.) for Approx. 1200 nodes at GSOC LAN.**									
34a										
34b										
.										
.										
.										
.										
.										
.										
..										
.										
34n										
35	**NGFW**									
36	**IPS**									
37	**WAF**									
38	**Server Load Balancer**									
39	**SSL Off Loader, proxy, etc**									
40	**Governance Risk & Compliance Solution**									
Grand Total of Table for Platforms and Components (B1a) in figures										

Note:-

1. IP and Web Reputation and Classification Database from single OEM is to be filled at Sr. No. 9
2. IOC feeds to be filled at Sr. No. 10 should be from one different OEM other than OEM of 9
3. Deep Web, Dark Web, Social Media, OSINT Feeds to be filled at Sr. No. 11, should also be from one different OEM from OEMs of 9 and 10

Table–1a: Cost of other Hardware required for software platforms and components

S. No.	Hardware Item	Make and model of the item	Unit Cost (in INR)	GST on Unit Cost (in INR)	Unit Cost Incl. GST (in INR)	Qty	Total Cost (in INR)	Software cost 2nd Year (Incl. GST)	Software cost 3rd Year (Incl. GST)	Grand Total Cost for 3 years (in INR)
1	Hardware Component 1									
1a	Incremental component for Hardware component 1									
2	Hardware Component 2									
2a	Incremental component for Hardware component 2									
.										
.										
.										
N	Hardware Component n									
Na	Incremental component for Hardware component n									
Grant Total of Hardware components – B1b (in Figures)										

Grand Total of Software and Hardware components (B1): B1a+ B1b (In Figures) =

a) The Bidder has to quote the price of each and every hardware component having financial impact in the proposed solution.
b) The bill of material in the table above shall include all the components required for installation and commissioning of platforms specified in paragraph 14.1 for achieving the scope of work as defined in the RFP.
c) The pieces of hardware to support the requirements/solution as part of the bill of Material shall be with one-year warranty.
d) The year-wise AMC value of hardware components shall be in rupees as numerical value of unit cost of item/ sub item. The AMC value quoted for an item in any year shall, at the minimum be 8% of the numerical value of the corresponding item. If quoted less than 8% for any item, Purchaser reserves the right to distribute the AMC value as per their terms and conditions through FEC as deemed appropriate.
e) In case of extension of the contract beyond Three years, the AMC cost of hardware shall not be more than 8% of the Total cost of the respective component in subsequent years.
f) At the time of initial deployment as per work order of Implementation phase, the MSP shall size the solution (including any hardware, system software like enterprise operating system, hypervisor, database, automation etc. collectively called as infrastructure here) with 25% additional capacity of the minimum infrastructure required with 24X7 support. This is applicable to both Primary and DR sites.
g) Any additional hardware, system software like enterprise operating system, hypervisor, database, automation etc. required to run the solution without any performance degradation as per the work order issued shall be factored by the bidder with 24X7 support, back lined with respective OEMs at no additional cost to the Purchaser. This is applicable to both Primary and DR sites.
h) The warranty of the platform and components shall be effective from the date of Go-Live, for a period of one year.
i) If a Bidder quotes less than the minimum BoQ specified in Table 14.1, the Bid may be rejected.
j) The unpriced BOM shall not deviate from the one submitted in the financial Bid, or it may lead to rejection of the Bid. Bidder to ensure that unpriced BOM submitted as part of the technical Bid does not include any pricing or financial details.
k) All software/licenses should be having enterprise class licenses.
l) The software licenses shall be delivered with the initial one-year cost and annual subscription cost for subsequent years to be included in the BOM for each year. The cost of all software subscription license in subsequent years of the 3 years contract period shall not be more than the initial one year cost.
m) The cost of all software subscription license in subsequent years beyond the 3 years contract period (if any) shall not exceed by more than 8% of the average yearly subscription cost of first three years.

5(B) Table for One Time cost for Installation, commissioning of all H/W & S/W (Inclusive of all taxes)

Table-2: One Time cost for Installation, commissioning of all H/W & S/W (As per work order of Implementation phase)

S No.	Item	Cost (in INR)	GST on Cost (in INR)	Total Cost (in INR)
A	**B**	**C**	**D**	**E=C+D**
1.	One Time cost for Installation, commissioning of all H/W, S/W licenses for the UAT period + Cost for the manpower which is deployed between T3 till date of Go-Live as per Table 3 (For a maximum period of 5 week)			
2.	Any other one-time cost till Go-Live			
	Total (B2) in figures			

Note:

1. Any deviation or changes made to the BOM, may lead to rejection of the Bid
2. All amounts to be filled in INR
3. The Bidder shall not leave any field blank. In case the field is not applicable, Bidder shall indicate “0” (Zero) in all such fields. Any blank field shall be considered as "0” Zero.

5(C) Table for Import (Dollar) Component Percentage in SOC Items

Table-3: Import (US Dollar) Component Percentage

S. No.	Item	OEM	Model/Version	% Import (US Dollar) Component in Basic Cost	% Import (US Dollar) Component in AMC

5(D) Cost for comprehensive Security Audit of the entire supplied and deployed components as defined in paragraph 5.8: Project Delivery Timelines and cost of recurring security audits as defined in Section 5: Scope of Work

Table-4: comprehensive Security Audit of the entire supplied and deployed components

(a)	Overall cost (inclusive of all taxes) for Security Audit (Annually) (in INR)	
(b)	Overall cost (inclusive of all taxes) for Security Audit (Three years) (in INR) = 3 * (a) in figures **B3**	

5(E) Cost incurred for Training and Support requirements as defined in para 5.10 of Scope of Work

Table-5: Cost incurred for Training and Support requirements

(a)	Overall Cost (inclusive of all taxes) for Training & Support (in INR) **B4**	

5(F) Table for Manpower

Table-6: Cost of Manpower (Year 1 will commence from date of Go-Live)

S. No.	Designations	Resource Type	No. of proposed Resources	Monthly cost of resource in the 1st year (Incl. GST) (in INR)	Monthly cost of resource in the 2nd year (Incl. GST) (in INR)	Monthly cost of resource in the 3rd year (Incl. GST) (in INR)	Grand Total for 3 Years (Incl. GST) (E+F+G) *D*12 ((in INR)
A	B	C	D	E	F	G	H
1	Project Manager						
2	SOC Analyst						
3	Malware Analyst						
4	Security Breach Investigation Specialist						
5	Log Analysis & Threat Hunting Specialist						
6	SIEM Administrator						
7	SOAR Administrator						
8	Ticketing Platform Administrator						
9	Linux Expert						
10	Windows Expert						
11	MacOS Expert						
12	Office Assistant						
13	Windows Forensic Expert						
14	Linux Forensic Expert						
15	MacOS Forensic Expert						
16	Memory Forensic Expert						
17	Android Forensic Expert						
18	iOS Forensic Expert						

19	Data Analytics Expert						
20	AI Engineer						
21	ISO 20000,27001, SOC CMM experts						
22	Full stack developers						
23	GRC Experts						
	Total Yearly Cost for 1st, 2nd and 3rd years respectively (B5)						

Note:

(a) Per man month cost given above shall include all applicable taxes.

(b) In the table above, the bidders have to add manpower cost for all Three years period after Go-Live.

(c) The Bidder may add additional roles and designations that may be required for execution of the contract.

(d) The Bidder may increase the number of resources above the minimum indicative resources specified in Annex 16.

(e) If a Bidder quotes less than the minimum location wise Manpower deployment specified in Annex 16, the Bid may be rejected.

(f) In case of extension of the contract beyond three years on the existing terms and conditions, the manpower cost shall be considered with **10% year-on-year** increase of the manpower cost of the 3rd year.

5(G) Any Other Miscellaneous Expenses for the Operational phase of the Contract

Table-7: Other miscellaneous expenses (Inclusive of all Taxes)

S. No.	Item Name	Unit Cost	GST on Unit Cost	Unit Cost Incl. GST (C+D)	Qty	1st Year Total Cost (E*F)	2nd Year (Incl. GST)	3rd Year (Incl. GST)			Grand Total Cost (G+H+I)
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	
1	<Item Name>										
2	<Item Name>										
3	<Item Name>										
4	<Item Name>										
5	<Item Name>										
6	<Item Name>										
7	<Item Name>										
8	<Item Name>										
…	…										
Grand Total Miscellaneous Expenditure in figures **B6**											

Table-8: Forensic Investigation

(a)	Overall cost (inclusive of all taxes) for Forensic Investigation (Annually) (in INR)	
(b)	Overall cost (inclusive of all taxes) for Forensic Investigation (Three years) (in INR) = 3 * (a) in figures **B7**	

Annex 6 – Proforma for Bank Guarantee for Contract Performance (PBG)

Ref: _____ Date: _____

BG Number: _____ Bid Number: _____

To,

Tender Processing Section
National Informatics Centre
A Block, CGO Complex, Lodhi Road, New Delhi – 110 003

1. Against contract vide Advance Acceptance of the Tender- No._____ dated _____Covering (hereinafter called the said "Contract") entered into between the NIC (hereinafter called "the Purchaser") and _____ (hereinafter called the "MSP") this is to certify that at the request of the MSP, we _____Bank Ltd., are holding intrust in favour of the Purchaser, the amount of _____(Write the sum here in words) to indemnify and keep indemnified the Purchaser against any loss or damage that may be caused to or suffered by the Purchaser by reason of any breach by the MSP of any of the terms and conditions of the said contract and/or in the performance thereof. We agree that the decision of the Purchaser, whether any breach of any of the terms and conditions of the said contract and/or in the performance thereof has been committed by the MSP and the amount of loss or damage that has been caused or suffered by the Purchaser shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to the Purchaser.
2. We _____Bank Ltd, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfilment in all respects of the said contract by the MSP i.e. till_____hereinafter called the said date and that if any claim accrues or arises against us, _____Bank Ltd, by virtue of this guarantee before the said date, the same shall be enforceable against us_____ Bank Ltd, notwithstanding the fact that the same is enforced within six months after the said date, provided that notice of any such claim has been given to us, _____Bank Ltd, by the Purchaser before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from the Purchaser.
3. It is fully understood that this guarantee is effective from the date of the said contract and that we _____Bank Ltd, undertake not to revoke this guarantee during its currency without the consent in writing of the Purchaser.
4. We undertake to pay to the Purchaser any money so demanded notwithstanding any dispute or disputes raised by the MSP in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present bond being absolute and unequivocal.

The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the MSP shall have no claim against us for making such payment.

5. We _____Bank Ltd, further agree that the Purchaser shall have the fullest liberty,

without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the Tendered from time to time or to postpone for any time of from time to time any of the powers exercisable by the Purchaser against the said MSP and to forebear or enforce any of the terms and conditions relating to the said contract and we, _____Bank Ltd, shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said MSP or for any forbearance by the Purchaser to the said MSP or for any forbearance and or omission on the part of the Purchaser or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.

6. This guarantee shall not be discharged due to the change in the constitution of the Bank or the MSP.

Date _____

Place _____ Signature _____

Witness_____ Printed name_____

(Bank's common seal)

Annex 8 – Manufacturing Authorization Form (MAF)

<This form needs to be filled by all OEMs.>

Date: _____

Bid Number: _____

To,

Tender Processing Section
National Informatics Centre
A Block, CGO Complex
Lodhi Road, New Delhi – 110 003

(a) We, <OEM Name> having our registered office at <OEM address>, hereinafter referred to as OEM are an established manufacturer of the following items quoted by <Bidder Name> having their registered office at <Bidder address>, hereinafter referred to as Bidder.

(b) We <OEM Name> authorise <Bidder's name> to quote our product for above specified tender as our Authorised Indian Agent.

(c) We confirm that we have understood the delivery & installation timelines defined in the tender. We confirm that we have worked out all necessary logistics and pricing agreement with <Bidder name>, and there won't be any delay in delivery, installation and support due to any delay from our side. Our full support as per pre-purchased support contract is extended in all respects for supply, warranty and maintenance of our products. We also ensure to provide the required spares and service support as pre-purchased for the supplied equipment for a period of contract and any extensions thereof as provided for in the contract, not exceeding a maximum period of 8 years from date of Go-Live. In case of any difficulties in logging complaint at Bidder end, user shall have option to log complaint at our call support centre.

(d) We also undertake that in case of default in execution of this tender by Bidder, we shall provide necessary support to Purchaser in identifying another authorised partner with similar certifications/capabilities and extend support to the new partner in accordance with OEM's agreement with the new partner. In case Bidder is unable to fulfil the obligations given under this tender, OEM shall be responsible to replace the Bidder with an alternate Indian Authorised agent to facilitate Purchaser to get the requisite work done as per the same terms and conditions of the RFP. OEM shall also ensure that the alternate Indian Authorised Agent in this case shall abide by all the terms and conditions laid down under this tender and during the contract of the Bidder for the quoted OEM products.

(e) If any product is declared end of sale, we shall proactively ensure that a suitable equivalent or higher roll over product is offered through the existing Bidder to National Informatics Centre, for due approval, contract and order executions thereafter. The licenses supplied if any as a part of this solution shall include upgrades & updates as a part of the deployment for the entire contract period and any extensions thereof.

(f) We understand that any false information/commitment provided here may result in <OEM's Name> getting debarred from doing business with National Informatics Centre.

For <OEM Name>

Name of Authorised Signatory:

Designation:

Email:

Phone Number (Office):

Signature

Seal

NOTE:

a) *The letter shall be submitted on the letter head of the manufacturer / OEM and shall be signed by the authorised signatory.*

b) *A copy of the MAF shall be uploaded on GeM portal along with the Bid. The date of the uploaded MAF should be before the date of the bid submission but not older than 30 days from the date of bid submission.*

Annex 9 – Covering Letter

<To be submitted on the letter head of the Bidder>

<Place>
<Date>

To
Tender Processing Section
National Informatics Centre
A Block, CGO Complex
Lodhi Road, New Delhi – 110003

Subject: **Submission of Bid for Selection of Managed Service Provider for Setting up, Operating and Managing the Cyber Security Operation Centre for Purchaser (Tender ID: _____)**

Dear Madam/Sir,

This is to notify that our company is submitting technical Bid in response to Tender No. Purchaser/… for Selection of Managed Service Provider for Setting up, Operating and Managing the Cyber Security Operation Centre for Purchaser.

Primary & Secondary contact for our company are as follows:

<M/s Company Name>	**Primary Contact**	**Secondary Contact**
Name		
Title		
Address		
Phone		
Mobile		
Fax		
E-mail		

1. We are responsible for communicating to the Purchaser in case of any change in the Primary or/and Secondary contact information specified above. We shall not hold Purchaser responsible for any non-receipt of Bid process communication in case such change of information is not communicated and confirmed with NIC on time.
2. We are submitting our Bid for Selection of Managed Service Provider for Setting up, Operating and Managing the Cyber Security Operation Centre for Purchaser as per the scope and requirements of the tender document:
3. By submitting the proposal, we acknowledge that we have carefully read all the sections and clauses of this tender document including all forms, schedules and appendices hereto, and are fully informed

to all existing conditions and limitations. We also acknowledge that the company is in agreement with terms and conditions of the tender and the procedure for bidding and evaluation. We also understand that any decision taken by NIC, or the evaluation committee shall be final and binding on the Bidder.

4. We have enclosed the earnest money deposit as per the tender Conditions. It is liable to be forfeited in accordance with the provisions of tender document.

5. Deviations:

We declare that all the services shall be performed strictly in compliance with the Tender Document. Further, we agree additional conditions, if any, found in the Bid documents, other than those stated in the tender document, shall not be given effect to.

6. Bid Pricing:

We do hereby confirm that:

(a) Our Bid prices for all platforms and components are exclusive of all taxes, as applicable on the last date of submission of Bid.

(b) Our Bid prices for one-time cost for Installation, commissioning of all H/W & S/W, Cost for comprehensive security Audit of entire supplied and deployed components, Cost incurred for Training & Support requirements, Cost of Manpower and cost of Other Miscellaneous Expenses are inclusive of all taxes, as applicable on the last date of submission of Bid.

(c) We further declare that the prices stated in our proposal are in accordance with your terms & conditions in the bidding document.

7. Qualifying Data:

We solemnly declare that we (including our affiliates or subsidiaries or constituents):

(a) are not insolvent, in receivership, bankrupt or being wound up, not have our affairs administered by a court or a judicial officer, not have our business activities suspended and are not the subject of legal proceedings for any of these reasons; including our Contractors/ subcontractors for any part of the contract):

i. Do not stand declared ineligible/ blacklisted/ banned/ debarred by the Procuring Organization or its Ministry/ Department from participation in its Tender Processes; and/ or

ii. Are not convicted (within three years preceding the last date of bid submission) or stand declared ineligible/ suspended/ blacklisted/ banned/ debarred by appropriate agencies of Government of India from participation in Tender Processes of all of its entities, for offences mentioned in Tender Document in this regard. We have neither changed our name nor created a new “Allied Firm”, consequent to the above disqualifications.

(b) Do not have any association (as bidder/ partner/ Director/ employee in any capacity) with any serving or retired public official of the Purchaser or near relations of such officials.

(c) We certify that we fulfil any other additional eligibility condition if prescribed in Tender Document.

(d) We have no conflict of interest, which substantially affects fair competition. The prices quoted are competitive and without adopting any unfair/ unethical/ anti-competitive means. No

attempt has been made or shall be made by us to induce any other bidder to submit or not to submit an offer to restrict competition.

8. **Restrictions on procurement from bidders from a country or countries, or a class of countries under Rule 144 (xi) of the General Financial Rules 2017:**

   (a) **"**We have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries, and solemnly certify that we fulfil all requirements in this regard and are eligible to be considered. We certify that:

      i. we are not from such a country or, if from such a country, we are registered with the Competent Authority (copy enclosed) and;

      ii. we shall not subcontract any work to a contractor from such countries unless such contractor is registered with the Competent Authority

   (b) We confirm having submitted in qualifying data as required by you in your tender document. In case you require any further information/documentary proof in this regard before evaluation of Bid, we agree to furnish the same in time to your satisfaction.

   (c) We confirm that information contained in this response or any part thereof, including documents and instruments delivered or to be delivered to Purchaser are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part misled Purchaser in its evaluation process.

   (d) We fully understand and agree that on verification, if any of the information provided here is found to be misleading the evaluation process or result in unduly favours to our company in evaluation process, we are liable to be dismissed from the selection process or termination of the contract during the contract with Purchaser.

   (e) We understand that you are not bound to accept the lowest or any Bid you may receive.

   (f) It is hereby confirmed that I/We are entitled to act on behalf of our corporation/ company/firm/organisation and empowered to sign this document as well as such other documents, which may be required in this connection.

Yours sincerely,
On behalf of [Bidder's name]
Authorised Signature [In full and initials]:
Name & Title of signatory:

Name of Firm:
Address:

Seal/Stamp of Bidder:

Place:
Date:

Annex 10 - Indicative list of minimum platforms and components as part of the work order for Implementation phase

TABLE 14: BOQ - PLATFORMS AND COMPONENTS

S. No.	Description	Total Quantity (H/W + S/W) to be supplied
1	ITSM	1 +1 (Active,Passive)
2	SIEM	1+1 (Active,Passive)
3	SOAR	1+1 (Active,Passive)
4	Threat Intelligence Platform (TIP)	1+1 (Active,Passive)
5	Attack Surface Management Platform	1
6	Incident Response Retainer service from a security OEM	1
7	MIS Solutions and its components (To be developed inhouse by the MSP)	1
8	Hardware appliances / solutions: (a) NGFW (b) WAF (c) Server Load Balancer (d) SSL Off Loader (SSLO) (e) Proxy	To be provisioned by the MSO as per design and architecture proposed by it keeping in view the cyber security requirements of the proposed solution.
9	Threat Intelligence (IOC Feeds, Deep Web, Dark Web, Social Media, IP and Web reputation feed, OSINT Feeds)	1 each
10	Digital Forensic Incident Response Tool	1
11	Portable Log Analyzer	8
12	Magnetic Media Degausser& Secure Drive Eraser	8
13	Attack Simulation Platform	1
14	Security Testing Platform	3
15	Dynamic Application Security Testing (DAST) Tools.	60
16	Laying of Inter building fiber cable between adjacent buildings for connecting GSOC with NICNET/NKN	1
17	Supply and installation of Active LAN components (Router, switches, access points etc.) for Approx. 1200 nodes at GSOC LAN.	Router (2) L3 Switches (2) L2 Switches (30) Access Points (15)
Forensic Solutions		
1	Digital Forensic Suite	3
2	Mobile Forensic Suite	3

3	Forensic Disk Imager with hardware write blocker along with required forensic hardware toolkits.	12
4	Memory Forensic Solution	3
5	Mac Forensics Suite	3
6	Cloud Forensic Solution	3
7	Steganography Forensic Solution	3
8	eDiscovery Forensic Data Analytics Platform	3
9	Network Forensics	3
10	MacOS Data Recovery	4
11	Forensic Workstations & Laptops etc.	18
13	Forensic Tools (Hackone RFOne Bundle, Flipper Zero, Proxmark3, Rubber Ducky etc.)	6
14	Static & Dynamic Analysis Sandbox from 3 OEMs	1
15	SOC Logistics Tools and accessories	As per Annex-17

Note: The associated hardware, system software for UAT and manpower and services required for the components and platforms mentioned above shall also be part of the work order for Implementation phase.

Annex 11 – Undertaking to be submitted by OEM

OEM UNDERTAKING

This is to certify that:

(a) The vulnerability details of the supplied products (OEM to mention the product name) shall be shared with the Purchaser prior to public disclosure. The information shall be shared within seven days of such vulnerability details of the supplied products are known to the OEM.

(b) The OEM shall also provide the Purchaser with the necessary information for mitigating any unpatched vulnerabilities identified in their products at no additional cost to the Purchaser.

(c) An NDA may be signed between the OEM and the Purchaser, for such sharing of vulnerability details of the supplied products with third parties.

(d) The overall solution architecture (enclosed herewith) including the unpriced bill of materials (enclosed herewith), architecture, sizing, security and deployment of hardware, software, network, security, storage and other relevant components, which are submitted as a part of the technical solution by _M/s._____ (Name of Bidder) conforms to the best practices and satisfies all the technical and SLA compliance requirements as per the RFP _____ (name of RFP for which the solution is being quoted) and international best practices, including the OEM's best practice guidelines. The following solutions have been supplied as part of the Bid:

1._____
2._____
3._____

We undertake full responsibility for the solution architecture, design, sizing proposed by the Bidder M.s/_____ in their technical Bid submitted for the RFP _____ (Name of the RFP).

We hereby confirm that all the solutions/ appliances supplied for which MAF has been submitted as part of this Bid shall not be End of life and End of support and OEM shall provide premium support for Three years and any extension thereof on same terms and conditions of this RFP, from the date of delivery to the Purchaser.

Submitted on behalf OEM Name:

Name of Authorised Signatory:

Designation of Authorised Signatory:

Signature & Seal of the OEM Authorised person:

Place:
Date:

Annex 12 - Format for Integrity Pact

This pre-contract agreement (hereinafter called the "Integrity Pact" or "Pact") is made on <<day>> of

<<month, year>>, between, on one hand, National Informatics Center (hereinafter called the "Purchaser", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part

AND

M/s <<bidder's legal entity >> represented by <<name and designation>> (hereinafter called the "BIDDER/MSP", which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the PURCHASER proposes to engage the Managed Service Provider (MSP) for implementation and operations management of the Project and the BIDDER is willing to offer/has offered the services and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the PURCHASER is a Ministry/Department/Attached Office of the Government of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:-

Enabling the PURCHASER to obtain the desired services at a competitive price in conformity with the defined specification by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the PURCHASER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

Commitments of the PURCHASER

1.1 The PURCHASER undertakes that no official of the PURCHASER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organisation or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The PURCHASER will, during the pre-contract stage, treat all the BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

1.3 All the officials of the PURCHASER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the

PURCHASER with full and verifiable facts and the same is prima facie found to be correct by the PURCHASER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the PURCHASER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the PURCHASER the proceedings under the contract would not be stalled.

Commitments of the BIDDER

3. The BIDDER commits itself to take all the measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

    3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour or any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PURCHASER, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

    3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PURCHASER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or dis-favour to any person in relation to the contract or any other contract with the Government.

    3.3 BIDDER shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

    3.4 The BIDDER further confirms and declares to the PURCHASER that the BIDDER has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the PURCHASER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

    3.5 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the PURCHASER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

    3.6 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation contracting and implementation of the contract.

    3.7 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

    3.8 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the PURCHASER as part of the business relationship,

regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.9 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.10 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.11 If the BIDDER who is involved in the bid process or any employee of such BIDDER or any person acting on behalf of such BIDDER, either directly or indirectly, is a relative of any of the officers of the PURCHASER, or alternatively, if any relative of an officer of PURCHASER who is involved in the bid process has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender.

3.12 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the PURCHASER.

3.13 For the purposes of clauses 3.11 & 3.12, the listed words shall have the ascribed meanings as follows:

i. "employee of such BIDDER or any person acting on behalf of such BIDDER" means only those persons acting on behalf of such Bidder who are involved in the bid process / Project.

ii. "officers/employee of the PURCHASER", means only those persons who are involved in the bid process / Project.

iii. "financial interest/stake in the BIDDER's firm" excludes investment in securities of listed companies".

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5. Earnest Money (EMD)

5.1 The Bidder's EMD of Rs. 6.5 Crore deposited along with the bid shall remain valid till the submission of performance guarantee by the BIDDER.

5.2 In case of the successful BIDDER, a clause would also be incorporated in the Performance Bank Guarantee that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the PURCHASER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.3 Within 15 days of the receipt of notification of award from the employer, the successful Bidder shall furnish the performance security/PBG equal to 5 per cent of the value of contract from a commercial bank in accordance with the conditions of the Agreement, in the proforma prescribed at Annex 6 of the RFP.

5.4 Performance security should remain valid from date of execution of Contract to the expiry of 90 days after the date of completion of all contractual obligations including warranty obligations.

5.5 No interest shall be payable by the PURCHASER to the BIDDER on Earnest Money/ Performance Security/PBG for the period of its currency.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the PURCHASER to take all or any one of the following actions, wherever required:

(i) To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Performance Security/PBG (after the contract is signed) shall stand forfeited either fully or partially, as decided by the PURCHASER and the PURCHASER shall not be require to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

(iv) To recover all sums already paid by the PURCHASER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing prime lending rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the PURCHASER in connection with any other contract for any other stores, such outstanding payment could also be utilised to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the PURCHASER, along with interest.

(vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the PURCHASER resulting from such cancellation/rescission and the PURCHASER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

(vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the PURCHASER.

(viii) To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the PURCHASER with the BIDDER, the same shall not be opened.

(x) Forfeiture of Performance Bond in case of a decision by the PURCHASER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The PURCHASER will be entitled to take all or any of the actions mentioned at para 6.1 (i) to (x) of this Pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the PURCHASER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fall Clause

7.1 The BIDDER undertakes that under similar buying conditions, it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or subsystems was so supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the PURCHASER, if the contract has already been concluded.

8. Independent Monitors

8.1 Shri <Name> has been appointed as Independent External Monitor (hereinafter referred to as Monitor) for overseeing and implementation of the Pre-Contract Integrity Pact for procurement of services in NIC. His contact details are as under:

<Name>

<Address>

<Contact details>

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the PURCHASER.

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the PURCHASER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

8.7 The PURCHASER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of PURCHASER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the PURCHASER/BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the

PURCHASER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is New Delhi.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend upto ___ years or the complete execution of the contract to the satisfaction of both the PURCHASER and the BIDDER, including warranty period, whichever is later. In case Bidder is unsuccessful, this Integrity Pact shall expire after six months from the date of signing of the contract.

12.2 Should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The parties hereby sign this Integrity Pact at on

PURCHASER	BIDDER
Name of Officer	CHIEF EXECUTIVE OFFICER
Designation	
Dept/Ministry/PSU	

WITNESS	WITNESS
1.	1.
2.	2.

Note:- Provisions of these clauses would need to be amended / deleted in line with the policy of the PURCHASER in regard to involvement of Indian agents for foreign suppliers.

Annex 13 – Format for Malicious Code Certificate

Format for Bidder

(To be provided on Bidder letter head)

Tender Ref. No.: _____ & Date: _____

To,
Tender Processing Section
National Informatics Centre
A Block, CGO Complex
Lodhi Road, New Delhi – 110003

(a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code/ malware or torjan that would activate procedures to:
i. Inhibit the desires and designed function of the equipment.
ii. Cause physical damage to the user or equipment during the exploitation.
iii. Tap information resident or transient in the equipment/network.

(b) The firm shall be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

Date:
Place:

Authorised Signatory:
Name of the Person:
Designation:
Firm Name & Seal:

Format for OEM

(To be provided on OEM letter head)

Tender Ref. No.: _____ & Date: _____

To,
Tender Processing Section
National Informatics Centre
A Block, CGO Complex
Lodhi Road, New Delhi – 110003

(a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code/ malware or torjan that would activate procedures to:
i. Inhibit the desires and designed function of the equipment.
ii. Cause physical damage to the user or equipment during the exploitation.
iii. Tap information resident or transient in the equipment/network.

(b) The firm shall be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

Date:
Place:

Authorised Signatory:
Name of the Person:
Designation:
Firm Name & Seal:

Annex 14 - Guidelines for Cybersecurity audit

1. Comprehensive security audit

1.1 Comprehensive audit should be done at least once in a year and should cover the entire application, including the following:

(a) web application (both thick client and thin client);
(b) mobile apps;
(c) APIs (including API whitelisting);
(d) databases;
(e) hosting infrastructure and obsolescence;
(f) cloud hosting platform and network infrastructure; and
(g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

1.2 The scope of the comprehensive audit should include, *inter alia,* the following:

(a) source code assessment;
(b) application security assessment (both Black Box and Grey Box testing), including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;
(c) network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs);
(d) penetration testing;
(e) network and device configuration review;
(f) application hosting configuration review;
(g) database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication);
(h) user access controls (including privilege access management) and access reconciliation review;
(i) identity and access management controls review;
(j) data protection controls review (*inter alia,* with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]");
(k) security operations and monitoring review (including maintenance of security logs, correlation and analysis);
(l) review of logs, backup and archival data for access to personal data (including whether personal data not in use / functionally required is available online rather than archived offline; and whether

logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); and

(m) review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website).

1.3 The auditor should be CERT-In-empanelled and, in case of application hosted on cloud, the auditor and should have the capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website.

2. Limited audit

2.1 Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is—

(a) modification in application functionality; or
(b) addition/modification of APIs; or
(c) migration to new infrastructure platform or cloud service; or
(d) change in configuration of application hosting, servers, network components and security devices; or
(e) change in access control policy.

2.2 The scope of limited audit should include, *inter alia,* the following:

(a) *In all cases:* Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;
(b) *In case limited audit is after six months of comprehensive audit:* In addition to (a) above, user access controls (including privilege access management) and access reconciliation review; identity and access management controls review;
(c) *In case limited audit is done earlier:* In addition to (a) and (b) above,—
    (i) *For audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change in configuration of application hosting, servers, network components and security devices:* Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs); network and device configuration review; application hosting configuration review; database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorised users and are protected with multi-factor authentication); data protection controls review (*inter alia,* with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration

with security monitoring solutions, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); review of logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

(ii) *For audit on change in access control policy:* Review of logs and integration with security monitoring solutions.

2.3 Auditor should be a CERT-In-empanelled auditor who is other than the auditor who has done the last comprehensive audit. Further, in case the application is hosted on cloud, the auditor should have capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website.

2.4 Alternatively, in case there is an information security audit vertical of the organisation hosting and/or managing the application which—

(a) satisfies the baseline requirements specified for CERT-In empanelment in CERT-In's Guidelines for applying to CERT-In for Empanelment of IT Security Auditing Organisations; and

(b) is independent of the ICT vertical, with the head of such vertical having direct reporting line to the head of the organisation,

such information security audit vertical may perform internal audit.

3. Role of the application owner

3.1 The application owner (Ministry/Department/organisation concerned, as applicable) should—

(a) appoint the auditor and initiate the audit process as required;

(b) extend necessary support and access for the audit;

(c) meet the cost of audit; and

(d) ensure requisite follow-up for closure of audit findings, including in terms of securing requisite approvals and resources and coordinating among the application developer, application manager, hosting service provider, Web Information Manager / Chief Information Officer and CISO.

Annex 15 - Format for Change Control Note

<table>
<tr><td colspan="6">Please attach any paper required to support this Change Request</td></tr>
<tr><td>RFP Reference</td><td colspan="5"></td></tr>
<tr><td>Subject</td><td colspan="5"></td></tr>
<tr><td>Change No.</td><td>Change Requested By</td><td colspan="2">Request Date</td><td>Required by Date</td><td>Proposed Implementation Date</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="5">Justification</td><td colspan="5">Type of Change</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">Requested Change</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">Reason for Change</td></tr>
<tr><td colspan="6">CR Classification</td></tr>
<tr><td rowspan="4">Priority: (Choose P1 TO P3)</td><td>Severity</td><td colspan="4">Component name:</td></tr>
<tr><td>High</td><td colspan="4"></td></tr>
<tr><td>Medium</td><td colspan="4">Details (if any):</td></tr>
<tr><td>Low</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Area</td><td colspan="5">Impact of Proposed Change</td></tr>
<tr><td colspan="5">Note: If possible, provide details of impact in terms of days/INR</td></tr>
<tr><td rowspan="4">Impact</td><td>Impact on Cost (Estimated cost for each component and justification for the same)</td><td colspan="4"></td></tr>
<tr><td>Impact on SOC operations including risks & issues</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Impact on Schedule</td><td colspan="2">Schedule Date</td><td colspan="2">Proposed New Date</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="6">Conclusion for consideration of NIC:</td></tr>
</table>

Annex 16 - Location wise minimum Manpower deployment details from commencement of Operational Manpower deployment timeline (i.e. T3 of paragraph 5.8)

Sr No.	Resource Type/Resource Profile				
		DEL(24X7)	CHEN (16X6)	HYD (16x6)	Total
1	Project Manager	1	0	0	1
2	SOC Analyst	12	4	0	16
3	Malware Analyst	9	3	0	12
4	Security Breach Investigation Specialist	9	3	0	12
5	Log Analysis & Threat Hunting Specialist	15	5	0	20
6	SIEM Administrator	8	0	3	11
7	SOAR Administrator	3	0	3	6
8	Ticketing Platform Administrator	3	0	3	6
9	Linux Expert	6	1	1	8
10	Windows Expert	6	1	1	8
11	MacOS Expert	5	1	1	7
12	Office Assistant	6	1	1	8
13	Windows Forensic Expert	2	1	0	3
14	Linux Forensic Expert	2	1	0	3
15	MacOS Forensic Expert	2	1	0	3
16	Memory Forensic Expert	2	1	0	3
17	Android Forensic Expert	2	1	0	3
18	iOS Forensic Expert	2	1	0	3
19	Data Analytics Expert	2	1	0	3
20	AI Engineer	1	1	0	2

21	ISO 20000, 27001, SOC CMM experts	3	0	0	3
22	Full stack lead developer	2	0	0	2
23	Governance, Risk & Compliance Expert	4	0	2	0
	Total	**107**	**27**	**15**	**149**

Annex- 17 - Indicative List of Accessories

Sr. No	Purchaser's Requirement
1	SATA Cables (power and data) - 10 Nos
2	USB 2.0 to USB Type-C and USB Type-C to lightning cable- 10 Nos
3	USB Type C to USB Type-C Power delivery cable - 10 Nos
4	HDMI 2.1 Male to Male with 8k support -10 Nos
5	USB Hard Disk Docking Station with support for 2 nos 3.5 inch SATA Drives - 5 Nos
6	USB Internet Dongle with 5G Internet connection - 2 Nos
7	Bluetooth 5.0 adapter - 2 Nos
8	USB Wifi adapter - 2 Nos
9	Portable DVD Writer - 2 Nos
10	Blank DVDs (4.7G) - 50 Nos
11	55inch PolyCarbonate Shell based Trolley bag with Anti-theft zipper, suspension ball-bearing wheels, antimicrobial treated fabric - 2 Nos
12	Silica Gel 5gm pouches -1000 Nos
13	Microfiber Cloth - 20 Nos
14	USB Type -C Hub - with ports for USB 3.1, 4K HDMI, Power Delivery, VGA, RJ 45, 3.5mm audio, SD & Micro SD Card Reader
15	Isopropyl Alcohol 99% - 5 Nos

----------**End of the Document**----------