# Request for Proposal
# For the
# Selection of Managed Service Provider for setting up
# Cyber security solutions
# for
# National Data Centres

**National Informatics Centre,**
**A Block, CGO Complex, Lodhi Road, New Delhi – 110003**

## Summary sheet

| | |
|---|---|
| Name of Organization | National Informatics Centre |
| Tender Type | Open |
| Tender Category | Goods and Services |
| Period of validity of the Bid | 180 days |
| Location (Work/Services/Items/As per tender document) | As per tender document |
| Period of Contract | Three years from the date of the acceptance of the Award of the Contract, |
| Submission of pre-Bid queries | Only queries submitted will be considered in the pre-Bid meeting. However, the formal response to any query would be that published on the said portal. |
| Number of packets | Two-packet online bid, as under:<br>Packet-1: Technical Bid<br>Packet-2: Financial Bid |
| Resubmission of Bid | Bid may be resubmitted before the last date and time for submission of the bid. |
| Address for Communication | National Informatics Centre,<br>A Block, CGO Complex, Lodhi Road, New Delhi – 110003 |

# Contents

## 1. Abbreviations

| Sr. No | Acronym | Description |
|---|---|---|
| 1. | AMC | Annual Maintenance Contract |
| 2. | API | Application Programming Interface |
| 3. | BG | Bank Guarantee |
| 4. | BoQ | Bills of Quantities |
| 5. | CA | Chartered Accountant |
| 6. | CMDB | Configuration Management Database |
| 7. | MSP | Managed Service Provider |
| 8. | CV | Curriculum Vitae |
| 9. | DC | Data Centre |
| 10. | DR | Disaster Recovery |
| 11. | DPIIT | Department for Promotion of Industry and Internal Trade |
| 12. | FAT | Final Acceptance Test |
| 13. | FEC | Financial Evaluation Committee |
| 14. | FM | Lowest GTV submitted among all the participating bidders |
| 15. | GFR | General Financial Rules |
| 16. | GST | Goods and Service Tax |
| 17. | GUI | Graphical User Interface |
| 18. | GTV | Gross Total Value |
| 19. | HA | High Availability |
| 20. | HLD | High Level Diagram |
| 21. | HQ | Head Quarters |
| 22. | INR | Indian Rupees |
| 23. | IP | Internet Protocol |
| 24. | ISO | International Organization for Standardization |
| 25. | IT | Information Technology |
| 26. | LLD | Low Level Diagram |
| 27. | LOI | Letter of Intent |
| 28. | LQx | Amount of Financial Proposal (GTV) |
| 29. | MeitY | Ministry of Electronics and Information Technology |
| 30. | NDC | National Data Centre |
| 31. | NIC | National Informatics Centre |
| 32. | NICSI | National Informatics Centre Services Inc. |
| 33. | NOC | Network Operations Centre |
| 34. | N/W | Network |
| 35. | PAN | Permanent Account Number |
| 36. | PBG | Performance Bank Guarantee |
| 37. | PC | Personal Computer |
| 38. | PCI | Peripheral Component Interconnect |
| 39. | PoC | Proof of Concept |
| 40. | PSU | Public Sector Undertaking |
| 41. | QTY | Quantity |
| 42. | RCA | Root Cause Analysis |
| 43. | RFP | Request for Proposal |
| 44. | SLA | Service Level Agreement |
| 45. | SOC | Security Operations Centre |
| 46. | SoP | Statement of Procedures/Purpose |

| Sr. No | Acronym | Description |
|---|---|---|
| 47. | | |
| 48. | STQC | Standardization Testing and Quality Certification |
| 49. | TEC | Tender Evaluation Committee |
| 50. | TPA | Third Party Auditor |
| 51. | ToT | Transfer of Technology |
| 52. | s | Second |
| 53. | m | Minutes |
| 54. | HIPS | Host based Intrusion Prevention System |
| 55. | HF | Host based Firewall |
| 56. | NDR | Network Detection and Response |

## 2. Definitions

| Sr. No | Term | Definition |
|---|---|---|
| 1. | Annual | A period of 12 Months, reckoned from the date of issuance of the Work Order and, in respect of any period constituting less than a period of 12 Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, shall include such lesser period |
| 2. | Arbitrator | Arbitrator means the person appointed by the Parties as per terms of this RFP to decide on or to settle any dispute or difference between the Parties |
| 3. | Asset | An asset refers to any valuable resource that an organization owns or controls, which is used to conduct business operations or deliver services. These assets can include tangible items such as hardware devices (computers, servers, networking equipment, security equipment etc.), software licenses, and physical infrastructure (data centers, office buildings, etc.), as well as intangible assets such as intellectual property (patents, trademarks, copyrights), digital assets (domain names, digital content), and contractual agreements |
| 4. | Audit | Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures |
| 5. | Auditor | Auditor shall mean the Statutory Auditor of a company or bidder. |
| 6. | 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 |
| 7. | Authorized 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 |
| 8. | Award of Contract | Issuance of a Letter of Intent or notification regarding the selection as the MSP |
| 9. | Biannual | A period of six Months, reckoned from the Effective Date and, in respect of any period constituting less than a period of six Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, such lesser period |
| 10. | Bidder | The person participating in the Bid process, pursuant to the RFP |
| 11. | Bid | The bidding process and the proposal submitted by the selected Bidder for this RFP, including any clarifications and amendments submitted by the Bidder in response to any request made by the Purchaser in this connection |
| 12. | Business Day | All Working Days, excluding (Saturdays and Sundays) and gazetted holidays as identified by the Purchaser. Support Centre and Operation & maintenance will be operational on 24 x 7 x 365 basis in shifts. |

| Sr. No | Term | Definition |
|---|---|---|
| | | |
| 13. | Business Hours | Business Hours of NIC is 09:00 h to 17:30 h. |
| 14. | A Day | In case of TAC support, Incident response and service request, a day shall start from time the incident or service is logged or registered. |
| 15. | Confidential Information | "Confidential Information" means any information disclosed to or by any Party to this Contract and includes any information in relation to the Parties, a third party or any information including any such information that may come to the knowledge of the Parties hereto MSP by virtue of this Contract that is by its nature confidential or by the circumstances in which it is disclosed confidential; or is designated by the disclosing Party as confidential or identified in terms connoting its confidentiality; but does not include information which is or becomes public knowledge other than by a breach of this. |
| 16. | Configuration | Configuration means the setup and customization of various hardware and software components deployed by the MSP according to the Scope of Work of the RFP |
| 17. | Contract Period | The period of subsistence of the Contract |
| 18. | Contract | The Contract issued to the Selected Bidder by the Purchaser. |
| 19. | Class-I local supplier | A Class-I local supplier is defined as a supplier or service provider whose goods, services, or works proposed for procurement contain at least 50% local content. |
| 20. | Class-II local supplier | A Class-II local supplier is defined as a supplier or service provider whose goods, services, or works proposed for procurement contain at least 20% local content. |
| 21. | Document | "Document" means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes or and databases or microfilm or computer-generated micro fiche. |
| 22. | Financial Year | The period from the first of April till the thirty-first of March of the succeeding calendar year |
| 23. | Final Acceptance Test (FAT) | Final Acceptance of solution: After completion of installation, commissioning, testing and integration all the supplied cyber security items/solutions as per scope of work. NIC security team shall issue Completion certificate. Date of completion certificate shall be treated as date of final acceptance of entire solution i.e. date of FAT-cum-Go-live. |
| 24. | Acceptance | Whenever any hardware or software is installed, configure and tested then installation report will be issued for that particular hardware, software or any cyber security solution for the purpose of release of payment only for those cyber security solutions. |
| 25. | Infrastructure as a service (IaaS) | The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include |

| Sr. No | Term | Definition |
|---|---|---|
| | | operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) |
| 26. | Letter of Acceptance | The formal acceptance submitted by the Selected Bidder to the Purchaser against the notification of the award of Contract. |
| 27. | Local Content | Local Content means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the item procured (excluding net domestic indirect taxes) minus the value of imported content in the item (including all custom duties) as a portion of the total value, in percent. |
| 28. | Managed Service Provider (MSP) | The Bidder with whom the Purchaser enters into the Contract. |
| 29. | Net worth (Consolidated) | The value computed by deducting the total liabilities from the total assets that are owned by an individual or company. |
| 30. | National Data Centre (NDC) | The data centres setup by NIC to provide data centre and cloud services, presently located at Delhi, Pune, Bhubaneswar and Hyderabad. NDC NER Guwahati is an upcoming NDC. |
| 31. | Operational phase | The phase of running the cyber security hardware or software in production. |
| 32. | Organization or User Department | One or more entities to which Purchaser provides information and communication technology (ICT) services or support, including-<br>a) a ministry, department, secretariat or office of the Central Government specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, and any other entity under the administrative purview of any such ministry, department, secretariat or office.<br>secretariats or offices of Lok Sabha, Rajya Sabha, Supreme Court of India, Delhi High Court and other Purchaser-supported Constitutional body or national level statutory body. |
| 33. | Party | Includes the MSP and the Purchaser, and the expression “Parties” shall be construed as a reference to the two taken together. |
| 34. | Platform as a service (PaaS): | The capability provided to the consumer to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |
| 35. | Promoter | Promoter(s) refers individual and his or her relatives as defined under the provisions of the Companies Act 2013 and the rules notified there under. |
| 36. | Purchaser | NIC or NICSI, including any:<br>a) of its successors;<br>b) representative authorised by it; and<br>c) assignee permitted by it |

| Sr. No | Term | Definition |
|---|---|---|
| 37. | Quarter | A period of three Months, reckoned from the date of issuance of the Work Order and, in respect of any period constituting less than a period of three Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, shall include such lesser period, and the expression “Quarterly” shall be construed accordingly. |
| 38. | Reputational Risk | Any event which may likely have the potential of negative publicity or negative public perception about the Purchaser. |
| 39. | RFP or Tender | This RFP 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 Cyber security solutions for National Data Centres ”. |
| 40. | Selected Bidder | The Bidder identified by the Purchaser for entering into the Contract. |
| 41. | Services | Services to be provided by the MSP for the discharge of its obligations under the RFP and the Contract, in a manner consistent with-<br>a) Applicable Law; and<br>b) extant policies and guidelines for—<br>i. cyber security, information security and data protection procedures and practices; and<br>ii. prevention, response and reporting of cyber incidents,<br>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 or modifications thereto as may be made from time to time. |
| 42. | Turnover | As defined in Indian Companies Act 2013 and its revisions. |
| 43. | Work Order | An order placed by the Purchaser to the MSP for providing services as per the provisions of the RFP or Contract. |
| 44. | RA | Reverse Auction |
| 45. | GeM Portal | https://gem.gov.in/ |

## 3. Objective of the RFP

3.1. India’s Data Centre (DC) industry is growing quickly due to the rising demand for digital services, cloud adoption, and the government’s focus on data localization and digital governance. Recognizing this, NIC has set up 4 National Data Centres (NDCs) in Delhi, Pune, Hyderabad, and Bhubaneswar. Currently, approx.1,141 racks are commissioned across these centres.

3.2. The NDCs were established at different times—the first in 2008 and the most recent in 2018. As a result, the equipment and software used across them vary in age, leading to differences in cyber security strength. With cyber threats evolving rapidly, it has become a top priority for NIC to strengthen security, replace outdated Cyber security solution, and ensure all NDCs maintain a uniform and modern security posture.

3.3. For this purpose, NIC is releasing RFPs to select Managed Service Providers who will:

- Replace obsolete, end-of-support, and old devices with new ones, and handle installation, configuration, commissioning, and migration of rules and policies.
- Install, configure, commission, operate, and management of newly procured security devices to enhance the overall security framework.
- Install, configure, commission, operate, and management of newly procured security solutions such as Privileged Identity and Access Management (PIM/PAM),Server Security, Patch Management, Host based Data Leak Prevention System, Web Application Firewall, Database Activity Monitoring, AAA, Vulnerability Assessment (VA）
- Manage the existing security infrastructure that remains after replacements, since some current devices are still usable and essential to maintain service continuity
- This RFP focuses on procuring and deploying security hardware to protect the perimeters of all four NDCs at Delhi, Pune, Hyderabad, and Bhubaneswar.

3.4. This initiative is a key part of NIC’s broader strategy to provide a secure digital infrastructure for government services and protect against advanced cyber security threats. It aims to modernize, strengthen, and standardize security across all National Data Centres.

## 4. Scope of work

### 4.1 Supply, Installation, Configuration, Commissioning Services, management and operation of the security solution at 4 Data Centres:

4.1.2 The MSP shall be responsible for replacement of obsolete, end-of-support, and old devices with newly procured devices through this RFP. The scope of work shall also include installation, configuration, commissioning, and migration of configuration, rules and policies from existing devices to new ones, along with management of the required security solutions.

4.1.3 The MSP shall also be responsible for operation, and management of the procured devices to enhance the security posture of all 4 National Data Centres (NDCs) under this RFP.

4.1.4 The MSP shall also be responsible to Install, configure, commission, operate, and management of newly procured security software solutions such as Privileged Identity and Access Management (PIM/PAM),Server Security, Patch Management, Host based Data Leak Prevention System, Web Application Firewall, Database Activity Monitoring (DAM) ,AAA, Vulnerability Assessment (VA)

4.1.5 The MSP shall continue to provide support in managing the existing security infrastructure deployed at the NDCs that are not being replaced, since some devices may still be operational and in use.

4.1.6 The MSP shall install and configure all cyber security solution in High Availability (HA) and redundancy mode.

4.1.7 The MSP shall ensure that any Cyber Security solution added to the NDCs does not affect the existing performance of NIC's NDCs or NGC portal, by taking necessary precautions under Purchaser's supervision.

4.1.8 MSP's plans and designs must be approved by the Purchaser before deployment to ensure comprehensive monitoring and management of all deployed solutions/tools.

4.1.9 The MSP shall manage connectivity within the rack, while inter-rack connectivity will be handled by the Purchaser.

4.1.10 The MSP shall process alerts/logs generated by security solutions, derive intelligence from them, and provide reports to NIC regularly.

4.1.11 The MSP shall provide managed services by designing a highly available, fault-tolerant, scalable (with automation), and continuously updated solution delivered as a 24x7x365 service.

4.1.12 The MSP shall provide round-the-clock managed services during the contract, including daily operations, configuration, backup, incident management, troubleshooting, and service desk support.

4.1.13 The MSP shall capture and retain all security solution logs for at least 6 months, push them in real-time to NIC's central log system, and archive them locally at each NDC SOC if required. Raw logs may also need to be shared with central agencies when requested with the approval of NIC.

4.1.14 The MSP shall set up management clusters with fault tolerance for all solutions deployed under this contract. These clusters will monitor, manage, and control both new and existing solutions. The MSP shall provision all necessary hardware, software, licenses, and components, and ensure High Availability. The MSP shall enhance management cluster capacity to meet SLA requirements if there is any service degradation without any additional work orders.

4.1.15 Minimum technical specifications for each hardware/software component are provided in Annexure: Technical Specifications of Hardware and Annexure: Technical Specifications of Software

4.1.16 MSP can provide higher-specification hardware to meet SLA requirements without any additional work order.

4.1.17 No quoted solution/item shall be End-of-Sale (EoS). OEM support must be available for 7 years. For any product nearing End-of-Service-Life (EoSL), MSP must provide an equivalent or better replacement of from the same OEM with the approval of NIC at least 3 months prior, at no extra cost to the Purchaser.

4.1.18 MSP shall ensure integration of any threat intelligence shared by Purchaser into its security ecosystem.

4.1.19 MSP shall implement a call logging system as per the work defined under Operation and maintenance at clause service request 10.1.11.5 and Operation and maintenance 4.3

4.1.20 The MSP shall use NIC's existing ITSM tool and maintain as well as update the tool on a regular basis.

4.1.21 The MSP shall be responsible for the followings

4.1.22 The MSP shall be responsible for Delivering all hardware and software to NIC sites as per the consignee list.

4.1.23 MSP shall be responsible to prepare CRD (Customer Requirement Document), HLD (High-Level Design), LLD (Low-level Design) documents, integration and migration plans, and an implementation roadmap in consultation with NIC, The HLD and LLD will include, but not limited to:

- Physical and logical topology.
- IP-Addressing and deployment strategy.
- Configuration templates.
- Security policies/rules required
- Performance optimization.
- Scalability, redundancy, and security considerations.
- Authentication, VLANs, subnet isolation, and other security features.
- Required changes to accommodate LLD.
- The MSP shall submit the proposed architecture diagram

4.1.24 Migration & Implementation Plan: Once the LLD is prepared, MSP in consultation with NIC, shall develop a migration and implementation plan. The MSP and OEM professional services team will create a structured plan, including sample configurations, a migration strategy, and an acceptance test plan.

4.1.25 The plan should ensure:

- A thorough implementation strategy.
- Adherence to aggressive deployment schedules.
- Minimal disruption to existing network security services.
- Risk mitigation for network operations.

4.1.26 It must also include:

- Sample configurations and turn-up test plans.
- Impact analysis for NIC network
- A ready-for-use plan in collaboration with OEM engineers.
- A security and infrastructure staging plan, covering:
  - Physical and logical topologies.
  - Configurations and testing scripts.
- Roll-back plan.
- Acceptance criteria.
- SOPs for each operation
- Manuals for the required services.
- Site-specific installation tasks, documentation, and checklists.

## 4.2 Product Support

4.2.1 OEM's professional services support must align with the final Low-Level Design (LLD) and Implementation Plan.

4.2.2 Data Security & Onsite Implementation

4.2.3 All tasks related to installation, commissioning, and migration must be performed within NIC premises. No NIC-specific data, including equipment distribution details, should be taken out of NIC premises or transferred over the internet.

4.2.4 The OEM professional service team must be available onsite at NIC locations (NOC/SOC/DC) during the implementation, commissioning, and migration phases.

4.2.5 The MSP shall ensure that all personal data is stored and processed in strict compliance with the Digital Personal Data Protection Act, 2023. All personal data shall be encrypted at rest and in transit, or alternatively maintained in tokenised, obfuscated, or masked form. Furthermore, access to back-end data shall be restricted to the minimum necessary set of authorised users and such access shall be secured through multi-factor authentication.

4.2.6 During the implementation and operational process, any electronics equipment like desktop, laptop etc. must be harden as per NIC security policy.

4.2.7 Integration of Critical Applications & Services

4.2.8 All security solutions must also integrate with NIC's existing or newly procured SIEM, AAA, Radius and monitoring solutions etc.

4.2.9 Any activity that may disrupt the network or critical services must be pre-approved by NIC and conducted during lean hours to minimize user impact.

4.2.10 OEM Support

i. OEM support must be available back-to-back with MSP during entire contract period.

ii. The MSP shall ensure that the entire infrastructure is supported back-to-back by OEM's professional service level. The OEMs of the solutions proposed by the MSP shall provide the following support during the below mentioned phases:

- **Implementation Phase:** Each OEM which are proposed by the MSP shall validate design, architecture, configurations, features enabled for their respective solutions proposed before installation and configuration of their solution. After completion of the deployment, OEMs shall again validate the design as per best industry practices. Each OEM shall assign single point of contact (SPOC) during the implementation phase.
- **Operational Phase:** The MSP should ensure that a robust support model is put together with OEM in such a way that the solutions and services runs with the level of availability as given in paragraphs 11. The MSP shall ensure the OEM's professional team develops a comprehensive support model for the contract period that will provide preventive, responsive and consultative support for all technological needs.

iii. One OEM engineer from major product/solution must be deployed onsite during the contract period.

iv. NIC user accounts must be created on the OEM's central services portal for direct access to support, licenses and services.

v. All OEM support, services, and licenses must be directly contracted in NIC's name.

## 4.3 Warranty

4.3.1 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.

4.3.2 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.

4.3.3 The Purchaser shall give notice to the MSP stating the nature of any such defects together with all available evidence thereof, promptly following the discovery thereof. The Purchaser shall afford all reasonable opportunity for the MSP to inspect such defects. Upon receipt of such notice, the MSP shall expeditiously repair or replace the defective Goods or parts thereof at no cost to the Purchaser.

4.3.4 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.

4.3.5 MSP shall provide comprehensive onsite warranty till the contract period from the date of Final acceptance date of all Cyber Security Solution ICT infrastructure including the software licenses provided as part of scope of work.

4.3.6 **Warranty / subscription date will be start from date of completion of Final Acceptance Testing.**

4.3.7 Acceptance of solution: After completion of installation, commissioning, testing and integration all the supplied cyber security items/solutions as per scope of work, NIC security team shall issue Completion certificate. Date of completion certificate shall be treated as date of final acceptance of entire solution i.e. date of FAT-cum-Go-live.

4.3.8 Onsite team should be deployed on before the installation and commissioning of the cyber security solutions, however billing of onsite manpower shall be start from the Final Acceptance Dat**e**.

## 4.4 Operation and maintenance

### 4.4.1.**Security Operations Monitoring** and Management

4.4.1.1 MSP shall provide monitoring and management services for all the provisioned infrastructure systems related to cyber security from the Final Acceptance Testing date.

4.4.1.2 The MSP shall be responsible for the operation and management of the entire security solutions in order to ensure confidentiality, integrity, availability and non-repudiation of the services on a 24x7x365 basis. The team will be required to provide monitoring and management of activities including but not limited to the following:-

**a. DDOS Solution**

**i. Operations & Monitoring**

- 24x7x365 monitoring of inbound/outbound traffic for volumetric, protocol, and application layer attacks.
- Real-time anomaly detection using traffic base lining and signature-based methods.
- Auto/manual mitigation of detected attacks through black holing, rate limiting, or challenge-response mechanisms.
- Escalation handling and proactive threat alerts.

**ii. Incident Management**

- Immediate response to DDoS attack events.
- Automated reporting of incident to all stakeholders including the users.
- Mitigation of false positives to ensure service continuity.
- RCA (Root Cause Analysis) and incident reports for each attack.
- Generating intel, collecting Indicators of Compromise (IOC), blocking IOCs on respective security solutions and sharing the IOCs with the purchaser.
- Support during Disaster Recovery (DR) drills or large-scale simulations.

**iii. Maintenance & Updates**

- Regular patching and firmware updates of DDoS appliances.
- Regular signature updation with intimation to all stakeholders.
- Backup and restore of configuration files.
- Health check routines and redundancy testing (failover validation).

**b. Firewall solution**

- Firewall Monitoring and Management
- Installation and maintenance of the firewall
- Firewall hardening with initial configuration
- Performance monitoring
  - ➢ Regular monitoring of the LAN errors
  - ➢ Regular monitoring of utilisation of CPU, memory of Data Plane and Control Plane and traffic levels on network interfaces
  - ➢ Firewall rule-based policy creation, implementation and changes within 30 minutes
  - ➢ Security Policy Configuration interface configuration, link aggregation.
  - ➢ Create and maintain Network Access Policy (NAP) document (the access specification) agreed between the parties from time to time. MSP shall integrate NIC's FARPS with the firewalls for implementation of Access control policies.
  - ➢ Log File review and analysis of information on traffic flow
  - ➢ Log File trend upgrade and analysis
  - ➢ Analysis of logs for
    - o If a NICNET IP is continuously attacking and traffic is being dropped by the firewall, the MSP must inform the NICNET user to clean the system.
    - o If any attacker targets the Data Centre (DC) and the firewall drops traffic, and the dropped traffic exceeds 1%, the MSP must inform the concerned NIC official to take further action.
    - o If any unusual traffic pattern is observed, the MSP must inform the NIC official to take further action.
- **Compliance Testing**
  - ➢ Design, configure, and maintain all Network Address Translation (NAT) services.
  - ➢ Manage access control through creation and upkeep of the Network Access Policy and firewall rules.
  - ➢ Implementation and maintenance of firewall solutions and configurations.
  - ➢ Network segmentation through subnetting/VLANs.
  - ➢ Regular patching and firmware updates of firewall appliances.
  - ➢ Manage secure access to firewall logs, policies, and performance statistics via protected web portals, in conjunction with monitoring tools.
  - ➢ Manage the generation and functioning of regular reports, in conjunction with monitoring tools, to provide detailed auditing of configuration history and change journals; alerts shall include critical configuration changes, potential malicious activity, and operational alarms.
- **Incident response**
  - ➢ Generating intel, collecting IOCs, blocking IOCs on respective security solutions and sharing the IOCs with the Purchaser.
  - ➢ Optimization of Firewall rules on quarterly basis. Unused rules, object, NAT etc must be removed after the approval from NIC officer.
  - ➢ Lifecycle Management of all Hardware and Software components
- **Firewall Backup**
  - ➢ Test environment implementation for firewall configuration changes to avoid impact to live environment.
  - ➢ Integration of firewall logs with a centralized SIEM system to correlate and analyse security events.
  - ➢ API Integration for comprehensive control, automation, and extended functionality of the firewall.

- Generation of regular reports summarizing firewall activity, performance metrics, and security events.
- Regular updation of firmware (OS, hotfix) to avoid any kind of outage due to known bugs.
- Implementation of high-availability configurations for firewalls to ensure minimal downtime.
- Testing of firewall failover functionality on a regular basis to ensure service continuity during emergencies.
- Ensure Minimal or No Downtime in Case of Complete Cluster Failure in a High Availability Setup.
- Ensure no downtime because of configuration changes.
- Ensure availability of logs (Traffic logs, Audit logs) on request by the NIC Team.
- Coordinate, facilitate, and ensure audit completion in case of third-party or internal audits.
- Regular stress testing of firewall infrastructure to assess its capacity to handle high-volume traffic spikes. Ensure seamless traffic flow during high-traffic events, such as CBSE results, election results, or any event etc., by proactively planning and implementing measures to handle traffic surges and bursts effectively.
- Monthly health check reports, Compliance reports, SLA adherence reports.
- Root cause analysis report for major incidents.
- Connection/session table monitoring to avoid drops.
- Trend analysis of firewall resource utilization.
- Disaster recovery drills for firewall and Periodic recovery testing from backups.
- Site-to-site VPN setup on demand.
- End-to-end troubleshooting of firewall-related issues including but not limited to connectivity, policy, VPN, performance, authentication, logging, and HA problems, ensuring timely resolution as per defined SLAs
- Ensure 24x7x365 availability for troubleshooting, configuration, firewall rule implementation.
- Ensure mandatory two-level verification for correctness of all firewall policy before final publishing on firewall.
- SNMP configuration for comprehensive monitoring which should cover CPU utilization, memory usage, physical interfaces, sub-interfaces, and VLANs. The configuration must enable granular reporting, proactive alerts, and error handling to support effective performance management and timely fault resolution.

**c. Network Intrusion Prevention System(NIPS)**

- Traffic Profiling
- Define alert levels and incident response levels
- Root cause analysis
- Technical support
- Monitor NIPS for 24*7x365 availability
- Restore NIPS availability
- Determine Intrusion occurrence
- Regularly Upgradation of intrusion signatures according to SOPs with intimation to all stakeholders
- Testing and verification of triggered signatures for false positive with OEMS.
- Fine tuning of NIPS signatures,
- Putting signatures in block mode at all NIPS.
- Creation of user defined signatures as and when required by NIC

- Provide security event correlation
- Regular patching and firmware updates of IPS appliances.
- Regular Monitoring of the attack logging rule’s logs
- Regular Monitoring of the generic deny rule’s logs
- Regular Monitoring of the attack bandwidth utilization
- Network attacks and serious attacks attempts analysis
- Assessment of uncovered new vulnerabilities
- Propose corrective and preventive actions.
- Monitoring and subscribing to external network security information in order to evaluate new attacks and propose preventive steps.
- Installation and configuration of NIPS software and hardware
- Provide maintenance and upgrade of service component software
- Provide reporting of intrusions and actions, web-based access
- Regular Reports
- Incident response
- Generating intel, collecting IOCs, blocking IOCs on respective security solutions and sharing the IOCs with the purchaser.
- Regular monitoring of alerts/incidences, traffic to detect possible compromise of internal network machines/devices and coordinating with owners/managers of such machines/devices to get them cleaned/sanitised.
- Regular monitoring of utilisation of CPU, memory of Data Plane and Control Plane and traffic levels on network interfaces
- Prevent all known network-based attacks
- Filter out IP and TCP illegal packet types
- Designing and configuring IPS services in response to Flooding limits (per source, destination and intensity)
- Technical Support desk Support
- Lifecycle Management of all Hardware and Software components and 24*7x365 Real time Monitoring and Response.
- Creation of custom signatures for newly found vulnerabilities and exploits.
- Taking daily backup of all NIPS.

**d. Web application firewall (WAF)**

- **Policy Management & Operations**

i. Putting the website behind the WAF so that all user requests first pass through the WAF for inspection and protection whenever WAF services are enabled.
ii. Necessary policy creation in consultation with the User.
iii. Deployment of all policies in learning mode.
iv. Fine tuning of all policies in consultation with user.
v. Deployment of application in protection mode in WAF and fine tuning policies as and when required.
vi. 24x7x365 monitoring of HTTP/HTTPS traffic to web applications.
vii. Continuous tuning of WAF policies based on false positive/negative feedback.
viii. IP reputation management and custom rule creation.
ix. Enforcement of rate limiting, bot protection, and CAPTCHA validation where applicable.

- **Incident Detection & Response**

i. Detection and blocking of application layer attacks (e.g., RFI, LFI, CSRF).
ii. Alert generation and analysis of blocked request logs.
iii. Incident reporting with detailed payload and attacker information.
iv. RCA and mitigation support post-incident.

v. Generating intel, collecting IOCs, blocking IOCs on respective security solutions and sharing the IOCs with the purchaser.

- **Maintenance & Security Updates**

i. Regular updates to WAF signatures and threat intelligence feeds as per SOPs with intimation to all stakeholders.
ii. Patching of WAF OS/firmware and policy engine.
iii. Backup and restore of WAF configuration and custom rules.

**e. Network Detection and Response**

i. NDR solutions inspect both raw packet data and metadata to understand normal network behaviour.
ii. Daily analysing the raw packets data and meta data to understand network behaviour. Filter the IOCs.
iii. Integrate with Firewall or other security devices to block suspicious traffic.
iv. Filter out threats like insider abuse, data exfiltration, lateral movement, and command-and-control communication that might not have a known signature.
v. Once a threat is identified, there should be an automated responses, such as isolating a compromised device or quarantining malicious traffic.

**f. Anti- Advanced Persistent Threat Solution**

- **Policy Management & Operations**

i. 24x7x365 monitoring of network, endpoint, and application-level activities for APT indicators.
ii. Continuous fine tuning of Anti-APT detection policies based on false positive/negative.
iii. Integration and correlation with threat intelligence feeds for proactive defence.
iv. Customization of detection and behavioural rules as well as policies for specific organizational assets.
v. On-demand forensic analysis of suspicious files/ packet stream

- **Incident Detection & Response**

i. Real-time detection and blocking/quarantining of malicious files, processes, and command & control (C2) communications.
ii. Alert generation and correlation with SIEM/SOC for advanced incident triage.
iii. Detailed incident reporting, including attack chain mapping, malware behaviour, and Indicators of Compromise (IoC)/Indicators of Attacks (IoA) data.
iv. Regular monitoring of alerts/incidences, traffic to detect possible compromise of internal network machines/devices and coordinating with owners/managers of such machines/devices to get them cleaned/sanitised.
v. After sandboxing any files, objects or flows and getting verdict from sandbox, details of IOCs must be collected and signatures must be created and pushed in the security solution to block the traffic related to that IOCs
vi. Root cause analysis including cyber forensics and coordinated mitigation steps post-incident.
vii. Generating intel, collecting IOCs, blocking IOCs on respective security solutions and sharing the IOCs with the purchaser

- **Maintenance & Security Updates**

i. Regular updates to Anti-APT signatures, heuristics, and sandbox analysis engines.
ii. Patching and upgrading of Anti-APT solution software, OS components, and detection engines.
iii. Backup and restore of Anti-APT configuration, custom rules, and threat detection profiles.
iv. Health checks and performance optimization to ensure continuous protection.

**g. SSL Off Loader**

- **Policy Management & Operations**
  - i. Putting the websites behind the SSL Off loader. Collect the SSL Keys from the user and deploy in the SSL Off loader. Develop a mechanism to take the SSL certificates and keys in a safe way from the user.
  - ii. Create filters/ policies in the SSL off loader as per requirement of user application.
  - iii. 24x7x365 monitoring of SSL/TLS traffic handled by the off loader to ensure secure decryption and re-encryption.
  - iv. Continuous tuning of SSL offloading policies for optimal performance and security.
  - v. Management of SSL/TLS certificate lifecycle, including procurement, installation, renewal, and revocation. Develop a mechanism to inform to user in advance in case of expiry of SSL certificates.
  - vi. Configuration and enforcement of supported cipher suites, TLS versions, and secure negotiation policies.
- **Incident Detection & Response**
  - i. Develop a mechanism to detect any malfunction of filters to stop function and the traffic flow from the device.
  - ii. Detection and alerting of SSL/TLS handshake failures, expired/invalid certificates, and insecure protocol usage.
  - iii. Logging and analysis of SSL session data (metadata only, not decrypted payloads unless permitted).
  - iv. Incident reporting for SSL-related security events, including potential downgrade or man-in-the-middle attempts.
  - v. Root cause analysis and remediation guidance for SSL configuration or performance issues.
- **Maintenance & Security Updates**
  - i. Regular updates to SSL off loader firmware/software and cryptographic libraries to patch vulnerabilities.
  - ii. Periodic review and update of SSL/TLS configuration to align with latest security best practices (e.g., disabling deprecated protocols).
  - iii. Backup and restore of SSL off loader configuration, including certificates and private keys.
  - iv. Performance optimization and resource tuning to ensure minimal latency during peak load.

**h. Privileged Access Management (PAM) / Per User**

- i. Manage onboarding and de-provisioning of user identities with role-based access control for critical infrastructure.
- ii. Regularly review and update access policies as per data centre operational roles.
- iii. Monitor session recordings and access logs for all privileged activities.
- iv. Ensure backup and periodic patching of PAM appliances or VMs.
- v. Integrate PAM with existing IDAM, SIEM, and ticketing systems.

**i. Server Security**

- i. Maintain and monitor anti-malware/EDR tools across all data centre servers.
- ii. Conduct regular integrity checks and system hardening reviews.
- iii. Respond to alerts and isolate compromised servers.
- iv. Perform OS-level patching in defined maintenance windows.
- v. Ensure compliance with organizational server security baselines.

**j. Patch Management**

- i. Implement automated and manual patch deployment cycles across physical and virtual servers.

ii. Maintain staging environments for pre-production patch testing.
iii. Document and track patch rollouts with rollback provisions.
iv. Ensure patch compliance and reporting as per defined SLAs.

k. **Host based Data Leak Prevention System**

i. Maintain and monitor the activity of Host based DLP across all data centre servers/ user Desktops
ii. Respond to alerts and isolate compromised servers.
iii. Perform OS-level patching in defined maintenance windows.
iv. Ensure compliance with organizational Data Loss Prevention Policies

**l. Web Application Firewall (WAF)**

i. Configure, maintain, and fine-tune WAF policies for hosted applications.
ii. Ensure high availability, SSL offloading, and health checks via the load balancer.
iii. Monitor throughput and manage failover configurations.
iv. Update security signatures and certificates periodically.

**m. Database Activity Monitoring**

i. Monitor database access patterns, queries, and user behaviours.
ii. Generate alerts on abnormal or unauthorized DB activities.
iii. Maintain audit logs for compliance and forensics.
iv. Ensure database monitoring solutions are updated and integrated with the SIEM.

**n. AAA (Authentication, Authorization, Accounting) – 50,000 Concurrent Users**

i. Manage AAA policies for infrastructure and application-level access control.
ii. Monitor AAA logs and track access attempts in real time.
iii. Ensure redundancy and scalability for high concurrency requirements.
iv. Periodically update configurations and perform log archiving.

**o. Vulnerability Assessment (VA)**

i. Schedule and conduct periodic VA scans across infrastructure components.
ii. Maintain VA tools, update plugins, and perform risk scoring.
iii. Submit risk reports and remediation plans based on criticality.
iv. Coordinate with patching teams to ensure timely mitigation.

## 4.5 Other Support Services

### 4.5.1. Documentation

i. MSP shall submit documentation in the format, media, and number of copies as decided by the Purchaser.
ii. Documentation shall be kept updated throughout the contract period with version control and proper change management.
iii. All documentation shall adhere to international standards (e.g., ISO/IEC 20000, ISO 27001, ITIL best practices).
iv. The MSP shall submit an overall deployment plan. The plan shall include:
- Detailed project timelines and micro-level activities with deadlines.
- High-Level Design (HLD) and Low-Level Design (LLD).
- Layout diagrams of the proposed architecture.
- Approach and methodology for deployment.
- Manpower deployment schedule.
- Test plans and acceptance criteria.

v. Indicative list of documents include:
- Configuration, operation, and maintenance manuals for each security solution
- Documents related to the configuration, operation and maintenance of each and every security solution and services provisioned by the MSP. The document should cover all the procedures, policies and necessary information for diagnosis

- The MSP shall submit the report on best security practices and further enhancement of the Cyber Security to the Purchaser.
- The MSP shall make changes to the documents as and when there is change in the Cyber Security infrastructure components or policies or as and when required by the Purchaser.
- DR/BCP documentation (backup/restore process, failover testing, escalation contacts).
- Version-controlled updates reflecting any change in Cyber Security infrastructure or policies.
- The MSP shall be responsible for creating State of Procedures (SoP) for each and every function of the proposed solutions.
- Ownership of Documentation: All documents, diagrams, manuals, and SoPs created under this contract shall be the sole property of the Purchaser.
- Documentation and reports: The MSP shall submit reports on a regular basis in a format approved by the Purchaser. The following is only an indicative list of MIS reports:

**vi. MIS Reports**

**a. Daily reports**

- Summary of issues / complaints logged at the technical support desk.
- Summary of resolved, unresolved and escalated issues / complaints.
- Logs of backup and restoration undertaken
- No of rules created on each security solutions
- Any issue related to any security devices
- Daily uptime/availability summary of critical ICT infrastructure.

**b. Weekly Reports**

- Issues / complaints analysis report for virus calls, call trend, call history, etc.
- Summary of systems rebooted.
- Summary of issues / complaints logged with the OEMs.
- Inventory of spare parts in the Data Centre
- Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, user creation, user password reset, etc.
- Major changes: configuration changes, patch upgrades, firmware updates
- Minor changes: log truncation, user creation, password resets, etc.
- Summary of Cyber-security incidents occurred and action taken to resolve the incidents.
- Health check status of key infrastructure (servers, network, storage, security devices).
- Summary of attacks blocked by each solution.

**c. Monthly Reports**

- Component wise Cyber Security solution ICT infrastructure availability and resource utilization
- SLA adherence report (as per paragraph 9).
- Summary of changes in the Data Centre
- Log of preventive / scheduled/ break fix maintenance undertaken.
- Attendance report of the manpower team

- Capacity trend analysis and forecasting report (CPU, memory, bandwidth, storage).
- Summary of attacks blocked by each solution.

d. **Quarterly Reports:**

- SLA adherence report (as per paragraph 9).
- Resource utilization trends and performance improvement recommendations.
- Cyber security posture review (based on incidents, vulnerabilities, and patches applied).
- On-Demand / Ad-hoc Reports
- Any other reports, at such periodicity, as may be required by the Purchaser, including incident-specific RCA, audit compliance reports, or regulatory submissions.
- Any other report, at such periodicity, as may be required by the Purchaser.
- Summary of attacks blocked by each solution.

## 4.6 Training

4.6.1 The MSP shall have to provide multiple training sessions on need basis.

4.6.2 **Operational training :**

4.6.2.1 The MSP shall impart offline operational training to persons designated by NIC for a minimum period of 5 business days. This training should cover a session on security awareness, practices, and configuration, management, features available in each solution, how features will be used, operations for the security solutions and services deployed by the MSP.

4.6.2.2 The standard contents of such training should be documented and made available to all the participants. Changes to the same should be updated periodically as and when required and the same should be communicated to the respective sites.

4.6.3 **Technical training**

4.6.3.1 The MSP should also provide offline OEM technical training on all equipment the persons designated by NIC for a minimum period of 3 business days. The modality and the group size of the OEM training will be mutually decided during the HLD/LLD Discussions.

4.6.3.2 The training material should be designed specific to the participants.

## 4.7 Constitution of Team

4.7.1 The MSP shall provide onsite resources at each NDCs for providing O&M

4.7.2 Role wise minimum manpower requirement are given in Annexure: C Manpower Requirement

4.7.3 These are the minimum resources envisaged by NIC. However, bidder can quote more resources to meet SLA requirements.

4.7.4 Role wise skill set & associated work

4.7.4.1 **Security Administrator:**

i. Qualifications, Skill Set & Experience required: B.E. / B. Tech. in Computer/IT / Electronics/ M.Sc. IT or M.C.A or higher from a recognized university.

ii. Certified Security Professional with one of the following valid certifications:

- Firewall OEM Certified Security administrator CCNA Security
- CEH

iii. Minimum 3 Year IT experience out of which at least 2 years in the relevant domain in any large Data Centre.

iv. Knowledge of operating systems, network devices and security devices

v. Knowledge of installation & configuration of L-2 & L3 switches, VLAN configuration etc.

vi. Knowledge of networking protocols

vii. Knowledge of troubleshooting and management of network technologies.

viii. Knowledge of configuration, operations, troubleshooting and resolution of network security appliances such as Distributed Denial of Services (DDoS), Network next-generation Firewall, SSL Off loader, Network Intrusion Prevention System (NIPS), Anti Advanced Persistent Threat (APT), Web Application Firewall (WAF), Antivirus tools, Endpoint Detection and Response (EDR), Server security solution, Vulnerability Assessment tools, Incident Handling, Forensic Analysis, Vulnerability Assessment and Penetration Testing (VAPT),SIEM, Patch Management etc.

ix. **Scope of Work:** The Security Administrator is responsible for all technical functions related to cyber security of the Data Centre. Maintain, configure, and monitor security operations and Coordinate with the core Security teams of NIC to maintain smooth security operations. Provide support in three shifts daily, however, may be called anytime (24X7) as and when required. The Security Administrator shall be performing following tasks :

- Implementation of Security Policies in the Data Centre on the security devices, servers and client systems
- Security administration of the security solutions, such as, Distributed Denial of Services (DDoS), Network next-generation Firewall, SSL Off loader, Network Intrusion Prevention System (NIPS), Anti Advanced Persistent Threat (APT), Web Application Firewall (WAF), Antivirus tools, Endpoint Detection and Response (EDR), Server security solution, Vulnerability Assessment tools, Incident Handling, Forensic Analysis, Vulnerability Assessment and Penetration Testing (VAPT),SIEM, Patch Management, Server OS hardening, application scanning tools, switch security
- Ensure proper implementation and maintenance of security architecture
- Administration of the Data Centre Security Operations Centre
- Analysis of security logs pertaining to the Data Centre to find out attack pattern
- Investigate network security incidents and resolve the same
- Provide periodic reports on cyber security activities to NIC core security team
- Conduct internal security compliance review of the Data Centre
- Keep abreast of the latest security vulnerabilities and implement appropriate mitigation measures
- Preparation of Manual and SOPS.
- Designing of Security Architecture.
- Provide support for Data Centre security operations

4.7.4.2 **Senior Security Administrator:**

i. **Qualifications, Skill Set & Experience required**: B.E. / B. Tech. in Computer/IT / Electronics/ M. Sc IT or M.C.A or higher from a recognized university.

ii. Certified Security Professional with one of the following valid certifications:

- Firewall OEM Certified Security administrator

- CCNP Security
- CEH

iii. Minimum 5 Year IT experience out of which at least 3 years as a Security Administrator in large Data Centre.

iv. Knowledge of operating systems, network devices and security devices

v. Knowledge of installation & configuration of L-2 & L3 switches, VLAN configuration etc.

vi. Knowledge of Networking protocols

vii. Knowledge of troubleshooting and management of network technologies.

viii. Knowledge of installation, configuration, operations, troubleshooting and resolution of network security appliances such as Distributed Denial of Services (DDoS), Network next-generation Firewall, SSL Off loader, Network Intrusion Prevention System (NIPS), Anti Advanced Persistent Threat (APT), Web Application Firewall (WAF), Antivirus tools, Endpoint Detection and Response (EDR), Server security solution, Vulnerability Assessment tools, Incident Handling, Forensic Analysis, Vulnerability Assessment and Penetration Testing (VAPT),SIEM, Patch Management etc.

**ix. Scope of Work:**

- Senior Security Administrator (SSA) will manage the security services of Data Centre. The SSA will be the interface between NIC Cyber Security Group, NIC DC management team and its Facility Management Staff. He will facilitate the DC management with his services through proper management system and job distribution system. He will be responsible for monitoring and managing the complete service delivery module during the time frame of this contract.
- The SSA will act as a centre point for escalation and management of day-to-day issues that may arise from the management and operations prospect of the security solutions.
  - The SSA's roles & responsibilities are:
  - ➢ Overall responsible for Cyber Security operations and smooth functioning.
  - ➢ Interface between NIC Cyber & Information Security Group, DC staff and deployed FMS team.
  - ➢ Provide technical solutions and strategic recommendations to enhance productivity and its services. He should have thorough knowledge of working environment within the above-mentioned services.
  - ➢ Manage and coordinate according to requirements defined by NIC-DC team.
  - ➢ Provide company escalation matrix to DC management team as and when required.
  - ➢ Senior Security Administrator will be the interface to provide all periodic reports as and when required by the NIC Cyber & Information Security Group, DC team, configuring, maintaining and smooth running of all management software. Ensuring the call logging and its tracking is done through proper surveillance & guidance.
  - ➢ Responsible for all sort of periodic reporting regarding the security operations mentioned above.
  - ➢ Shall undertake the training on security operations, help desk to their staff and prepare run book for the same.

- ➢ The Senior Security Administrator has to ensure the compliance of security policies governed by NIC. He will have to train team members on security policies.
- ➢ Able to develop IPS and WAF signatures.
- ➢ Preparation of Manual and SOPS.
- ➢ Designing of Security Architecture.

4.7.4.3 **Security Operator / Security operations**

i. **Qualifications, Skill Set & Experience required:** B.E. / B. Tech. in Computer/IT / Electronics/ M.Sc. IT or M.C.A or higher from a recognized university.

ii. Minimum 1 year of experience

iii. Knowledge of operating systems, network devices and security devices

iv. Knowledge of networking protocols

v. Scope of Work: The Security Operator is responsible for the cybersecurity of a Data Centre, their role expands beyond basic security monitoring to include ensuring the operational integrity, availability, and protection of critical infrastructure. The Security Operator shall be performing following tasks –

- Real-Time Monitoring: Continuously monitor of the security solutions, such as, Distributed Denial of Services (DDoS), Network next generation Firewall, SSL Off loader, Network Intrusion Prevention System (NIPS), Anti Advanced Persistent Threat (APT), Web Application Firewall (WAF), Antivirus tools, Endpoint Detection and Response (EDR), Server security solution, Vulnerability Assessment tools, Incident Handling, Forensic Analysis, Vulnerability Assessment and Penetration Testing (VAPT),SIEM, Patch Management, Server OS hardening, application scanning tools, switch security
- Scanning for Vulnerabilities: Regularly run vulnerability scans across the Data Centre’s systems to detect weaknesses.
- Communication and Coordination: Maintain constant communication with different teams of NIC.
- Monitoring of Attacks: Monitoring of logs on security devices to detect any real time attacks and same report to next level

4.7.4.4 **Lead Security Administrator**

i. **Qualifications, Skill Set & Experience required:** B.E. / B. Tech. in Computer/IT / Electronics/ M. Sc IT or M.C.A or higher from a recognized university.

ii. Certified Security Professional with any two of the following valid certifications:
    - Firewall OEM Certified Security administrator
    - WAF Certifications
    - CCNP Security
    - CEH

iii. Minimum 8 Year IT experience out of which at least 3 years as a Senior Security Administrator in large Data Centre.

iv. Knowledge of operating systems, network devices and security devices

v. Knowledge of installation & configuration of L-2 & L3 switches, VLAN configuration etc.

vi. Knowledge of Networking protocols

vii. Knowledge of troubleshooting and management of network technologies.

viii. Knowledge of installation, configuration, operations, troubleshooting and resolution of network security appliances such as Distributed Denial of Services (DDoS), Network next-generation Firewall, SSL Off loader, Network Intrusion

Prevention System (NIPS), Anti Advanced Persistent Threat (APT), Web Application Firewall (WAF), Antivirus tools, Endpoint Detection and Response (EDR), Server security solution, Vulnerability Assessment tools, Incident Handling, Forensic Analysis, Vulnerability Assessment and Penetration Testing (VAPT),SIEM, Patch Management etc.

ix. **Scope of Work:** The Lead Security Administrator (LSA) is a critical leadership role responsible for developing, implementing, and managing the NIC Data Centre's cyber security strategy across all NDCs in India. They ensure the security infrastructure is resilient, compliant, and up to date while leading a team of security professionals. This role involves technical expertise, strategic planning, compliance oversight, and close collaboration with other teams to protect the organization from evolving cyber threats. The Lead Security Administrator also plays a crucial part in incident response, risk management, and continuously improving the security posture of the organization. The LSA's roles & responsibilities are:

- Design and Implement Security Policies: Develop, implement, and enforce security policies and procedures that align with industry standards.
- Policy Review and Updates: Regularly review and update security policies to address evolving security threats, compliance requirements, and changes in NIC infrastructure across all NDCs.
- Manage Security Team: Lead and supervise a team of security administrators, analysts, and engineers. Provide mentorship and guidance to all team members.
- Resource Allocation: Allocate resources effectively, ensuring that security solutions, staff, and processes are used efficiently and appropriately to meet security objectives.
- Training and Development: Organize and facilitate security training programs for the team to ensure they stay up to date with the latest cyber security trends, technologies, and best practices.
- Manage Security Tools and Technologies: Oversee the management and configuration of security infrastructure, including DDoS, firewalls, WAF, intrusion detection/prevention systems (IPS), APT, and endpoint protection solutions.
- System Monitoring and Optimization: Ensure that all security tools are properly configured, maintained, and optimized for performance to detect and mitigate cyber security threats.
- Lead Incident Response: Lead the response to security incidents, including breaches, malware infections, DDoS attacks, and data leaks. Coordinate with internal teams (e.g., IT, network, and compliance) and external vendors when necessary.
- Risk Analysis: Perform regular risk assessments to identify security threats, weaknesses, and vulnerabilities within the NIC's infrastructure. Develop and implement strategies to mitigate these risks.
- Threat Intelligence Integration: Integrate threat intelligence into the NIC's security posture by staying informed about emerging threats and vulnerabilities, adjusting defences accordingly.

### 4.7.4.5 Project Manager

i. **Qualifications, Skill Set & Experience required:** Postgraduate or higher from a recognized university.

ii. Certified Professional with any of following valid certifications:

    - PMP
    - CompTIA Project+ / CompTIA Security
    - CISM

iii. Minimum 10 Year of experience as project coordinator or assistant

iv. Knowledge of operating systems, network devices and security devices

v. Knowledge of following:

vi. Risk Management: Identifying, assessing, and mitigating security risks in projects.

- Agile and Scrum Methodologies: Delivering iterative solutions, especially in software or application security.
- Stakeholder Management: Communicating with technical teams, executives, and external vendors.
- Strategic Planning: Aligning cyber security initiatives with organizational goals.

**vii. Scope of Work:**

- The Project Manager is essential to the success of any cyber security project, ensuring that security initiatives are planned, executed, and delivered effectively. They must coordinate multiple teams, manage resources, ensure compliance with standards, and deliver security solutions on time and within budget. They must also navigate the challenges of changing security landscapes and emerging cyber threats, making sure the organization remains protected while meeting business objectives.
- The roles & responsibilities of Project Manager are:
    - ➢ Define Project Scope and Objectives: Work with stakeholders (e.g., security teams, NIC Ministries and departments) to define the scope, goals, and objectives of cyber security projects. This includes determining the necessary resources, timelines, and deliverables.
    - ➢ Develop Project Plans: Create detailed project plans that include task breakdowns, timelines, milestones, resource allocation, and risk management strategies. Ensure alignment with organizational priorities and security objectives.
    - ➢ Clear Communication: Provide regular status updates to senior management and key stakeholders. This includes presenting progress, addressing any issues, and providing solutions or recommendations.
    - ➢ Team Coordination: Lead and coordinate the project team, including internal security experts, IT professionals, and external contractors or vendors, ensuring they understand their roles and responsibilities in the project.
    - ➢ Ensure Compliance and Security Standards: Ensure that all project activities comply with regulatory requirements and security best practices (e.g., NIST, ISO 27001). This includes setting up processes for audits, certifications, or assessments as required.
    - ➢ Handle Changes and Issues: Manage changes to the project scope, timelines, or resources, ensuring that any adjustments do not compromise the overall security goals. Address any project delays or issues that arise, ensuring minimal disruption to the security goals.
    - ➢ Quality Assurance: Ensure that the implemented security measures meet organizational security standards and deliver the expected outcomes. This could involve performing quality checks, vulnerability testing, or security reviews of the project outputs.

- Security Strategy Integration: Ensure that the cyber security solutions being implemented align with the organization's overall security strategy, including risk management and business continuity plans.

4.7.1. Employee Training: Ensure that training programs are developed and delivered to employees to raise awareness of the security measures implemented as part of the project. This may include training on new systems, processes, or security protocols. The MSP shall have to factor the onsite manpower to be deployed at each NDC.

4.7.5 The manpower should be comprising of Project Manager, Security Lead, Senior Security Administrator Security Administrator and Security Operations Staff to meet 24X7x365 operational efficiency. The team shall be deployed at distinct places i.e. NDC Pune, NDC Hyderabad, NDC Bhubaneswar and NDC Delhi.

4.7.6 The Purchaser in consultation with the MSP may increase the number of resources during the lifecycle of the contract period within the discovered rates.

4.7.7 Prior to Project Start, the MSP shall carry out background checks of the human resources identified to work on this project and submit the background check reports, along with copies of any of the officially valid documents under the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, in respect of each such resource. The same process shall be followed post Project Start/Go-live in respect of any resource who may be replaced or added, prior to his/her deployment. 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 Government-designated agency as the Purchaser may communicate in writing. If the Purchaser, at any point of time, communicates in writing the fact that a resource having been identified as unsuitable by the Government-designated agency as aforesaid, the MSP shall take action to remove such resource promptly, and in any case not later than 24 hours of receipt of such communication, and shall stop forthwith the access (both in-person and virtually) of such human resource.

4.7.8 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, maternity benefits, employee and disability benefits and the like, and shall be the responsibility of the MSP, subject to Applicable Law.

4.7.9 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 penalties shall be applicable as specified in paragraph 9.3

4.7.10 NDC's operates 24x7x365 without any service interruptions. The deployed resources will have to work on 24x7x365 basis in shifts. Each resource will have to work for minimum five days per week including holidays. However, compensatory leave would be given for National holidays as per convenience of Data Centre operations. In case of absence/leave of deployed manpower, the agency will have to ensure suitable substitute is present on site.

4.7.11 The deployed manpower working for 5 days per week will be entitled for 12 days of casual leaves per year on pro-rata basis and in case of 6 working days, the deployed manpower will be entitled to 15 days casual leave per year on pro-rata basis. Beyond specified leaves as applicable, leave will be treated as Leave without Pay (LWP) for which necessary deduction will be made by the Purchaser in the billed amount, on pro-rata basis, if no replacement is provided.

4.7.12 If the deployed resources does not 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 15 days of receiving such an intimation from the Purchaser. Further, the outgoing resource shall have to provide knowledge transfer of minimum 15 days to the new resource. The resources are expected to work in a 24x7 x365 security operations environment.

4.7.13 If a resource is not available at the place of duty for more than 3 consecutive days due to unauthorized absence, 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

4.7.14 The MSP shall be required to provide the documentary proof of the qualifications and experience of the manpower being provided to the Purchaser before the deployment of that resource.

4.7.15 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.

4.7.16 The Purchaser may have an interaction with the proposed manpower, deployed by the MSP, if its required before the actual deployment.

4.7.17 All the resources shall log their attendance daily in the Biometric attendance system or AEBAS at the Purchaser’s premises. The MSP shall also maintain a database of attendance of the resources deployed. The attendance database should have facilities to track attendance and draw out MIS reports, as and when required by the Purchaser.

4.7.18 The laptops and other essential equipment/ software to resources will be provided by the MSP and the Purchaser will provide the hardened image for the same laptops. The data residing in such devices will be owned by the Purchaser.

4.7.19 The MSP shall provide dedicated laptops with at least 8 Core latest gen 2.4 GHz CPU, 16 GB RAM and 1 TB SSD standalone MS Office professional (latest version) with perpetual license to the deployed resources. The laptops shall not have any 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. The resources shall not connect these dedicated laptops anywhere outside Purchaser’s network, without an explicit written permission from the Purchaser.

4.7.20 The MSP shall replace the laptop within 7 days, if laptop is faulty. After 7 days, the resource without a functioning laptop will be marked as absent.

## 4.8 Responsibilities of Purchaser

4.8.1 Purchaser shall provide all the basic (non-IT) infrastructure such as power, cooling, DG and rack space etc.

4.8.2 Purchaser shall provide Public IP pool and private IP pool to the MSP as per requirement.

4.8.3 Purchaser shall provide approvals and signoffs to the deliverables within the stipulated time.

4.8.4 Purchaser shall direct and monitor the activities performed by the MSP as per the tender document and in turn validate the service levels attained as per the SLA defined.

### 4.9 Ownership of assets

4.9.1 All the Cyber Security ICT infrastructure supplied and supporting infrastructure deployed by the MSP through this project shall be under the ownership of the purchaser.

## 5. Bidding Process

### 5.1 Overview

**5.1.1** Bidder shall adhere to the timelines as mentioned in the paragraph 1: Summary Sheet. No Bids shall be accepted post the last date of submission of Bid. Bids submitted online, shall only be considered for the Tender opening process and further evaluation. Incomplete Bids may be rejected.

### 5.2 Online Bid Submission

5.2.1 The Tender document is available at Gem website.

5.2.2 Prospective Bidders desirous of participating in this Tender may view and download the Tender document or corrigendum as a revised RFP document free of cost from the above-mentioned website.

5.2.3 The Bidders are expected to examine all instructions, forms, terms, scope of work and other information in the RFP or corrigendum or revised RFP as a corrigendum document.

5.2.4 Online bidding can be done through Gem website latest by the time and date mentioned in the paragraph 1: Summary Sheet. Online Bids shall be submitted as per the below:

**Table 3: Document to be uploaded**

| Packet Number | Documents to be uploaded | Packet File Format |
|---|---|---|
| Packet-1<br>(Technical Bid)<br>*(As per online provision)* | The file should be saved and uploaded in a PDF format only as “Packet 1_<Bidder Name>”.pdf<br>(a) Scanned copy of **Original Power of Attorney letter** in a Non-Judicial Stamp Paper of at-least Rs.100/-<br>Or<br>Board Resolution in Letter Head in original in case of Registered Limited Companies<br>Or<br>Original Authorization in Letter Head in case of Partnership Firm<br>Or<br>**Original Self Certificate in Letter Head** in case of Proprietorship naming/indicating the person authorised to sign the Bid (PDF).<br>(b) Scanned copy of duly filled signed and stamped Pre-qualification Evaluation (as **per paragraph 6.1.7)** and all the supporting or mandated documents and Annex(s) required for eligibility criteria. | PDF |

| Packet Number | Documents to be uploaded | Packet File Format |
|---|---|---|
| | (c) Scanned copy of Bidder’s Profile as per Annexure: Bidder’s Profile duly filled in, signed and stamped along with all supporting documents.<br>(d) All the supporting documents as per paragraph 6.2 Technical Evaluation Criteria<br>(e) Scanned copy of Annexure: Un-priced BOQ and<br>(f) Scanned Copy of Annexure: Covering Letter<br>(g) Scanned copy of duly filled signed and stamped for Pre-qualification Evaluation (as **per paragraph 6.1.7)** and 12 Annexure: Technical Specifications of Hardware and 13 Annexure: Technical Specifications of Software<br>(h) Annexure: 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<br>(i) Duly filled signed and stamped copy of MAF and undertaking form from respective OEMs as per Annexure: Manufacturing Authorization Form (MAF) and Annexure: Undertaking to be submitted by OEM.<br>(j) A copy of Malicious Code Free Certificate as per Annexure: Format for Malicious Code Free Certificate duly filled signed and stamped by the Bidder and respective OEM for all the supplied components shall be submitted.<br>(k) Scanned copy of Annexure: Undertaking to be submitted by the OEM<br>(l) A signed copy of the Integrity Pact as per the format given at Annexure: Format for Integrity Pact.<br>***Note:***<br>*The PDF file not containing above documents or **containing the financial Bid in the explicit or implicit form** may lead to rejection of the Bid.*<br>*Provide other document(s), as asked or mentioned anywhere in the RFP to be submitted along with technical Bid.* | |
| Packet-2 (Financial Bid) | | |

| Packet Number | Documents to be uploaded | Packet File Format |
|---|---|---|
| *(As per online provision)* | Financial Bid to be uploaded as per Annexure: Detailed Financial Bid Annexure 18: Format for Gross Total Value and Annexure 17: Detailed Financial Bid. | .zip or .rar or .pdf or .xls or .xlsx |

### 5.2.1. Instructions for Packet-1

(a) All the Bid documents duly signed by the Authorised Signatory of the Bidder and stamped with Bidder's seal.

(b) 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 Evaluation, Annexure Technical Specifications of Hardware and Annexure: Technical Specifications of Software No relevant information or document should be left, whether listed above or not.

(c) Bidder must provide all documents mandated for Bidder's profile, eligibility criteria, etc.

(d) The document should have a table of contents indicating page number where supporting document are placed. All pages in the Bid document should be sequentially numbered, stamped and signed by the Authorised Signatory of the Bidder.

(e) Provide other document(s), as asked or mentioned anywhere in the RFP or corrigendum as a revised RFP document to be submitted along with technical Bid.

(f) Technical Bid should not contain financial details.

### 5.2.2. **Instructions for Packet-2**

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

(b) The Bidder must strictly follow the prescribed format as specified in the detailed Financial Bids.

(c) During financial opening, only the Grand Total Value quoted by the Bidder after the RA on GeM portal shall be considered for determining the LQ1 Bidder

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

## 5.3 General Instructions for Bid Submission

5.3.1 The Purchaser shall not be responsible for any delay on the part of the Bidder in submission of the Bid. The Bids submitted by Fax or E-mail etc. shall not be considered. No correspondence shall be entertained on this matter.

5.3.2 Conditional Bids or any form of deviations from the RFP shall not be accepted on any ground and may be rejected. (A Bid is conditional when Bidder submits its Bid with his own conditions and stipulations extraneous to the terms and conditions specified in this RFP) If any clarification is required, the same should be obtained before submission of the Bids i.e., during pre-Bid meeting.

5.3.3 No Bids shall be accepted after the expiry of the deadline as stated in the paragraph 1: Summary Sheet.

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

5.3.5 All pages of the Bid being submitted must be signed by the Authorized Signatory, stamped and sequentially numbered by the Bidder irrespective of the nature of content of the documents.

5.3.6 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 RFP by publishing a corrigendum or revised RFP as a corrigendum document. The corrigendum or revised RFP as a corrigendum document shall be notified on the portal https://gem.gov.in/ and should be taken into consideration by the Bidders while preparing their Bids. It is the responsibility of the Bidder to check website for any such notice or changes and submit its Bid accordingly.

5.3.7 In order to give Bidders reasonable time to take the amendment into account in preparing their Bids, the 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.

5.3.8 In case any terms and conditions of the RFP is or are not acceptable to the Bidder, or the Bid is submitted with any deviation, the Bid may be rejected.

5.3.9 Ambiguous or Incomplete or Illegible Bids may be out rightly rejected. Bid in which the financial value is not quoted shall be consider as non-responsive and shall be rejected.

5.3.10 Bidder(s) are advised to study the RFP document carefully. Submission of the Bid shall be deemed to have been done after careful study and examination of all instructions, eligibility norms, Prequalification Criteria, terms and condition and required specifications in the RFP with full understanding of its implications. Bids not complying with all the given provisions in this RFP shall be rejected. Failure to furnish all information required in the RFP or submission of a Bid not responsive to the RFP in all respects shall be at the Bidder’s risk and may result in the rejection of the Bid.

5.3.11 RFP process shall be over after the issuance of contract to the Selected Bidder(s).

5.3.12 Submission of false or forged documents shall lead to execution of Bid Securing Declaration and blacklisting of the Bidder for a minimum period of 3 years from participating in NIC Tenders.

5.3.13 Information relating to the evaluation of Bids and recommendation of Contract award, shall not be disclosed to Bidders or any other persons not officially concerned with such process until information on Contract award is communicated to all Bidders

### 5.4 Bid Validity

5.4.1 Bid must be valid for a period of 180 calendar days from the last date of Bid submission. If necessary, the Purchaser may seek an extension in the Bid validity period. The Bidders, not agreeing for such extensions shall be allowed to withdraw their Bids.

### 5.5 Earnest Money deposit

5.5.1 The EMD shall be accepted in the form of Account Payee Demand Draft, Fixed Deposit Receipt or Bank Guarantee from any commercial bank in favor of National Informatics Centre, New Delhi 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, EMD shall remain valid until the Security Deposit is furnished by MSP and accepted by the Purchaser. In such case, the MSP shall extend the validity of the EMD for a period till the Security Deposit is submitted and accepted by the Purchaser.

5.5.2 In case the EMD is submitted in the form of Bank Guarantee, the MSP shall submit the same in the format as given in Annex 12.

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

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

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

5.5.6 The Bidder shall deposit the envelope containing the EMD at Tender Process Section, NIC Headquarter within 7 days from the Bid submission date.

5.5.7 EMD of the unsuccessful Bidders shall be returned to the respective Bidders 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

### 5.6 Assistance to Bidders

5.6.1 Any queries relating to the tender document and the terms and conditions contained therein shall be addressed to the relevant contact person indicated in the tender.

5.6.2 Any queries relating to the process of online Bid submission or queries relating to https://gem.gov.in/ in general may be directed to GeM portal helpdesk.

5.6.3 Financial Prices shall not be indicated in the Technical Bid, not adhering to which shall lead to disqualification of the Bid.

### 5.7 Correspondence Address of the Bidder

5.7.1 The Bidder shall designate the official mailing address, place, email, phone, and fax number to which all correspondence shall be sent by the Purchaser.

### 5.8 Period of Validity of Contract or Agreement

5.8.1 The period of validity of the contract shall be three years from the date of Award of the Contract

5.8.2 If it is considered necessary for the continuance of operation by the Purchaser, the MSP shall be required to continue delivering services as required under this project, on the same rate and terms and conditions or additional mutually agreeable conditions, even beyond contract period till an alternate arrangement is made by the Purchaser to manage the operations.

### 5.9 Cost of Bid

5.9.1 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 any costs, regardless of the conduct or outcome of the Tendering process.

### 5.10 Influencing the Purchaser

5.10.1 Any effort by a the Bidder to influence any activities related to Tender such as Bid evaluation, Bid comparison or Contract award decisions may result in the rejection of the Bidder’s Bid.

### 5.11 Purchaser Clarification

5.11.1 When deemed necessary, as part of Technical and Financial Evaluation, during the tendering process, the Purchaser may seek clarifications or ask the Bidders to make presentations or clarifications on any aspect from any or all the Bidders.

### 5.12 Bidder’s Clarification on Tender Document

5.12.1 Bidders requiring any clarification on the Tender Document may submit their queries, on https://gem.gov.in/ portal. The queries must be submitted on the GeM portal only to be considered for clarification. Queries submitted by other means i.e mail, phone, by letter may not be considered.

5.12.2 The Purchaser shall not respond to any queries not adhering to the above-mentioned format. Bidders are responsible for duly checking the website for any clarifications.

### 5.13 Amendment of Tender Document

5.13.1 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.

5.13.2 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.

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

### 5.14 Revelation of Prices

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

### 5.15 Bid Opening

5.15.1 The Purchaser shall download the Technical Bid (Packet-1) from the portal at first. Bidder’s representatives can remain present during the Bids download process.

5.15.2 For Technical evaluation, these technical Bids shall be passed on to a duly constituted Technical Evaluation Committee (TEC).

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

5.15.4 Financial Bids, original and revised (if any) for the technically qualified bidders only, shall be opened.

5.15.5 After opening the financial bid L1 Bidder will be displaced in the GeM portal and RA will be open for further processing.

5.15.6 Final Financial RA bid will be opened, Bidder’s representatives can remain present during the Financial RA Bids opening process.

5.15.7 The Financial Bids shall be evaluated by the duly constituted Financial Evaluation Committee (FEC).

## 6. Evaluation Process

### 6.1 Pre-qualification Evaluation

6.1.1. Purchaser shall validate the “EMD”.

6.1.2. If the EMD is as per requirements as per given paragraph 5.5. the Purchaser shall evaluate the documents. In case the bidder does not meet any one of the conditions, the bidder will be disqualified

6.1.3. Documentary evidence for compliance to each of the eligibility criteria must be enclosed along with the bid, together with references as required.

6.1.4. Relevant portions, in the documents submitted in pursuance of Prequalification Criteria mentioned above, shall be highlighted.

6.1.5. Undertaking for subsequent submission of any of the documents will not be entertained under any circumstances. However, the Purchaser reserves the right to seek required or additional documents (in case the bidder finds any issue, with due justification, in submitting the documents) and/or seek clarifications on the already submitted documents.

6.1.6. All documents should be submitted electronically in PDF format.

6.1.7. **Prequalification Criteria**

| Sr. No. | Parameter | Clause | Documents Required | Compliance (Yes or No or NA) | Page No. |
|---|---|---|---|---|---|
| **1.** | Legal Entity | The bidder should be an established Information Technology company registered under the Companies Act, 1956/2013 or LLP firm or Partnership firm under Partnership Act 1932 and in operation for at least 5 years as on last date of bid submission and should have their registered offices in India.<br>The company must be registered with appropriate authorities for all applicable statutory duties or taxes | Valid documentary proof of:<br>• Certificate of incorporation/ Certificate of Commencement<br>• Certificate consequent to change of name if applicable<br>• Copy of Memorandum of Association (if applicable<br>• Valid documentary proof of:<br>• GST Registration certificate- Certificate of GST registration<br>• PAN Details- Copy of PAN / TAN / Income tax number. | | |
| **2.** | Eligibility Declarations | Bidder should meet the eligibility criteria as of the date of his bid submission and should continue to meet these till the award of the contract. Bidder shall be required to declare the same. | Bidder should submit as per enclosed Eligibility Criteria in Form 1.2 (Eligibility Declarations) | | |

| Sr. No. | Parameter | Clause | Documents Required | Compliance<br>(Yes or No or NA) | Page No. |
|---|---|---|---|---|---|
| **3.** | Annual Turnover | The bidder's average annual turnover for the last 3 financial years should be INR 600 Cr. | Audited sheet with CA/CA Certificate with registration number | | |
| **4.** | Relevant Experience in Cyber Security | The bidder must have successfully implemented 5 similar Cyber security related work in India during the last three (3) financial years up to 31.03.2025, and the cumulative value of a maximum of five (5) such completed projects shall be not less than INR 320 Crore, | Copies of relevant Work Orders with value and client completion certificate. In case of NDA, A masked Work Order and CA certificate and completion certificate depicting the value of the component of Cyber security or Managed Services.<br>NIC may ask the relevant tender also.<br>Note: Value of Work Order will be considered as inclusive of all taxes. | | |
| **5.** | Resources or Manpower Strength of MSP | The bidder's technically qualified manpower strength (on the bidder's payroll as on the bid submission date) in the domains of Cyber Security should be more than 100 resources.<br>Eligible professionals must be engaged in any of the following areas:<br>a. Cyber security solution Configuration, management troubleshooting and operation<br>b. Cyber Security solution Architecture<br>c. Integration and automation of Cyber security solution<br>d. Any other activity related to Cyber security<br>Note 1: Manpower from subsidiary companies shall not be considered for this criterion | Certificate from bidder's HR Department for the number of Technically Qualified professionals employed by the company. Certificate should capture employee's details in the following format with all mandatory columns. Please note that the bidder which will submit the employee list as per format will be evaluated only. The list with Incomplete information will not be evaluated. | | |

<table>
<tr><th>Sr. No.</th><th>Parameter</th><th>Clause</th><th>Documents Required</th><th>Compliance (Yes or No or NA)</th><th>Page No.</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td>Employee name</td><td></td></tr><tr><td>Qualification:</td><td></td></tr><tr><td>Years of Experience</td><td></td></tr><tr><td>Designation or Domain of expertise</td><td></td></tr><tr><td>Certification</td><td></td></tr><tr><td>PF No</td><td></td></tr></table></td><td></td><td></td></tr>
<tr><td><b>6.</b></td><td>Certification</td><td>The bidder must have the following certifications<br>1. ISO 27001:2015 or higher<br>or<br>ISO 20000-1:2018. Or higher<br>2. SOC 2 Type 2 audit or latest version<br>3. CMMI Level 3 or 5 certificate</td><td>Valid Copy of the Certification stating the location and the scope of the certification</td><td></td><td></td></tr>
<tr><td><b>7.</b></td><td>Financial Net Worth</td><td>The Bidder must have positive net worth during the last three financial years (i.e., 2022-23, 2023-24 and 2024-25) and also the net worth of the bidder should not have been eroded by more than 30% (thirty percent) in the last three financial years, ending on 31st March 2025.<br>Note: The net worth of the parent company OR collective net-worth of group companies* shall not be considered</td><td>Certificate with CA’s Registration Number and Seal.<br>Audited Balance Sheets for the three consecutive financial years: (2022-23, 2023-24 and 2024-25) where financial turnover is segregated.<br>Every sheet shall be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for the three financial years.</td><td></td><td></td></tr>
<tr><td><b>8.</b></td><td>OEM MAF</td><td>The bidder should submit valid letter from all the OEMs confirming the following:<br>○ Authorization for bidder to confirm that the products quoted are not “end of life or end of sale products”.<br>Undertake that the support including, patches, signatures,</td><td>Documentary evidence’s such as Manufacturers Authorization Form (MAF) from all OEMs whose products are being quoted.</td><td></td><td></td></tr>
</table>

| Sr. No. | Parameter | Clause | Documents Required | Compliance (Yes or No or NA) | Page No. |
|---|---|---|---|---|---|
| | | hotfixes, firmware update for the quoted products shall be available for next 7 years. | | | |
| **9.** | Point of Contact | The bidder shall be the single point of contact for Purchaser and shall be solely responsible for all warranties and upgrades etc. | Self-certification duly signed by authorized signatory** on company letter head. | | |
| **10.** | IT Act | The bidder must comply with IT Act 2000 and all latest amendments. | Self-certification duly signed by authorized signatory** on company letter head. | | |
| **11.** | Restriction under Rule 144(xi) of the GFR | The bidder must comply with the Govt. notifications provided under Rule 144 (xi) of the General Financial Rules 2017 | Self-declaration as attached in Annexure: Format of Restriction under Rule 144(xi) of the GFR | | |
| **12.** | Malicious Code Free Certificate | Duly filled signed and stamped Malicious Code Free Certificate shall be submitted by the Bidder and respective OEM(s) for all the supplied components. | Copy of Malicious Code Free Certificate as per Annexure: Format for “Malicious Code Free” Certificate | | |
| **13.** | Back to back support | Bidder shall provide back-to-back Enterprise support from OEM for a period of 3 years from the date of.(FAT) | Copy of Undertaking to be submitted by the OEM is attached at Annexure: Undertaking to be submitted by the OEM | | |
| **14.** | Integrity Pact | Bidder shall provide duly signed Integrity Pact | Copy of Integrity Pact as per Annexure: Format for Integrity Pact | | |

Note:

- In case the latest audited financials are not ready, provisional balance sheet may be submitted.
- Value of Work Order will be considered as inclusive of all taxes.
- For the technical evaluation, in respect of the work orders submitted by the bidder, in respect of any ongoing projects if any extension orders have been placed upon the bidder then all set of orders within that project shall be considered as single workorder.

## 6.2 Technical Evaluation

6.2.1. Technical Bids If any bidder found eligible in pre-qualification criteria after scrutinizing the submitted documents then bidder shall be eligible for evaluation of Annexure: Technical Specifications. Bidder must be met the compliances of each and every point mentioned in the specification.

6.2.2. Technical Evaluation Committee (TEC), 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).

6.2.3. The Technical presentation or demonstration shall be a part of the process for evaluation of the Bids.

6.2.4. Bidders shall submit the technical specification compliance sheet as a part of technical bid as given in Annexure: Technical Specification.

6.2.5. Bidder shall submit reference to the relevant document or datasheet or white paper or publically available information or screenshot of the dashboard of the proposed solution for each technical compliance wherever required. Purchaser has right to reject the technical bid if any reference document is not submitted as mentioned here.

6.2.6. The technical specifications of all proposed cyber security solutions must be complete, accurate, and in strict conformity with the requirements specified in the RFP. If, at any stage during the contract period, it is found that:

- Any offered solution does not comply with the technical specification requirements of the RFP; or
- The submitted documents are false, misleading, or inaccurate; or

6.2.7. The MSP has falsely marked compliance as “Yes” against any requirement, then the following actions shall apply:

- The contract with the Managed Service Provider (MSP) shall be liable for immediate termination.
- The MSP shall be blacklisted from participating in future tenders of NIC.
- The entire contract value already paid, along with any additional losses incurred by NIC due to such non-compliance, shall be recoverable from the MSP.
- Purchaser reserves the right to award the contract to another eligible agency at the risk and cost of the defaulting MSP, without prejudice to any other remedies available under applicable law.

6.2.8. The Purchaser reserves the right to call upon the Bidder and its prospective OEM(s) to conduct a Proof of Concept (PoC) and/or demonstration of each proposed solution as part of the technical evaluation process, if required. The bidders/OEM must bring their quoted product in a High Availability (HA) setup, along with all necessary infrastructure required for the PoC. This includes a traffic simulator, interconnecting switches, cables, and any other essential equipment. NIC will provide only the physical space and a ~230V power supply. The bidder/OEM must complete the PoC within the stipulated timeframe set by NIC. Failure to arrange all the required items within 15 days, may result in the rejection of the bidder’s BID. Additionally, bidders will be required to leave the demo appliances at NIC premises until the completion of the bidding process.

6.2.9. All the Bidder qualifying or not qualifying for Technical Evaluation will be notified via Gem portal or e-mail.

6.2.10. MSP must quote the make and model of each security solution in the bid.MSP shall be responsible to deliver those make and model security solution which is quoted in the bid and technical evaluated by the TEC committee. Any other make and model will not be accepted in delivery.

6.2.11. The bidder must qualify in pre-qualification and Technical qualification compliance as per Annexure Technical Specification to be eligible for evaluation of the Financial Bid. Only the Financial Bids of technically qualified bidders will be opened

### 6.3 Financial Bid Opening

6.3.1. Financial bid of only those bidders who Pre-qualification criteria and The bidders who will qualify technical evaluation stage will be considered for Financial Evaluation.

**6.3.2.** First the Financial Bid GTV of all shortlisted bidders shall be opened electronically 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).

### 6.4 Total Bid Evaluation

6.4.1. Initially, L1 bidder will be declared based on the lowest quoted Gross Total Value (GTV) among all the bidders.

6.4.2. The Purchaser may decide to call for reverse auction process, same will be followed as per the GeM terms and conditions. Subsequently, L1 bidder (with lowest GTV after completion of RA called RAL1) will be declared post completion of reverse auction process. There could be change in GTV after RA. The detail financial bid of only L1 bidder (after RA) shall be opened.

Further, in the event of mismatch in the RAL1 value:

**i.** When **RAL1 value is** greater than the Total Value **of Annexure: Detailed Financial Bid**. The Total value given **of the Annexure: Detailed Financial Bid shall** be taken as the Grand Total value for Annexure: Format for Gross Total Value.

**ii.** When **RAL1 value** is less than the **Total Value of Annexure: Detailed Financial Bid**. The value given in **Annexure: Detailed Financial Bid** shall be replaced with the **RAL1 value** and the item-wise value for each item in **Annexure: Detailed Financial Bid** shall be reduced on Pro-Rata basis and consequently unit values shall be worked out.

**6.4.3.** If only single Bid or two bid are submitted, Purchaser reserves the right to process with the evaluation of the Bid.

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

### 6.5 Consideration of Abnormally Low Bids

6.5.1. An Abnormally Low Bid is one in which the GTV, or any of its components including manpower, appears so low that it raises substantive concerns as to the Bidder's capability to perform the contract at the offered price.

6.5.2. The Purchaser may in such cases seek written clarifications 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.

6.5.3. If, after evaluating the price analyses, 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 or proposal, Reasonability of Prices Received

### 6.6 Reasonability of Prices Received

6.6.1. The Purchaser shall evaluate whether the GTV, and/or any of its components mentioned in Annexure: Detailed Financial Bid, 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 3.5 or reject any or all Bids, or abandon or cancel the Tender process and issue another tender for identical or similar Services.

## 7. Contract

### 7.1 Contract Process

7.1.1 The MSP has to agree for honouring all tender conditions, SLAs and adherence to all RFP terms and conditions in executing the Work Orders placed by Purchaser.

7.1.2 Purchaser reserves the right to cancel this tender or modify the requirement, at any stage of Tender process cycle.

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

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

## 7.2 Placing of Work Order

7.2.1 Purchaser has the right to choose any subset of the tendered items for placement of the Work Order or Contract. Through this contract the purchaser reserves the right to place multiple work orders.

7.2.2 Purchaser can place the order of AMC in pro rata basis for less than 1 year.

7.2.3 For procurement of Cyber Security solution , Purchase order will be placed on the selected bidder in hardcopy format or in softcopy mode either through e-mail containing the scanned copy of the Work Order or an alert through e-mail for downloading the Work Order from Purchaser or e-procure.gov.in.

7.2.4 Objection, if any, to the Work order must be reported to Purchase department by the bidder within three (3) working days counted from the Date of Work Order for modifications, otherwise it is assumed that the bidder has accepted the Work Order in totality. This is applicable in case of electronic publishing or delivery of Work Order also.

7.2.5 On the receipt of the Work Orders, the bidder shall obtain all the necessary documents for the State Entry Permit in respective States wherever required by them, for complete, safe and timely delivery of the ordered products.

## 7.3 Performance Bank Guarantee

7.3.1 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 Annexure 24: Format for Performance Bank Guarantee. PBG must be furnished within 15 days of issuance of the Contract/ Work Order to the MSP or as informed by the Purchaser. In the event of default or 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 Work order Value per day delay or default with a maximum penalty capping of 10% of Work order value.

7.3.2 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.

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

7.3.4 Performance Bank Guarantee would be returned only after successful completion of tasks assigned to MSP only after adjusting or recovering any dues recoverable or payable from or by the MSP on any account under the contract.

7.3.5 The PBG shall be released (without any accrued interest) after the completion of all tasks (deliverables) of the Contract.

7.3.6 During the Contract period, the Purchaser shall review the total Contract value considering the total orders issued by the Purchaser. The MSP shall be required to deposit additional PBG, as required by the Purchaser, to keep the aggregate PBG value to minimum 5% of the total Contract value, in accordance with the instructions or directions of ministry of finance, Government of India or any other ministry

## 8. Implementation of the Contract

### 8.1 Timelines

8.1.1 MSP shall adhere to the below timelines for the Cyber Security Solutions being procured by the Purchaser through this RFP as per Annexure: A Hardware unpriced BoQ and Annexure: B Software unpriced BoQ. In case of any delay, Penalty shall be applicable as per Section Penalty Terms.

| Sr. No | Milestone | Timeline |
|---|---|---|
| 1. | Placement of Work order | T0 |
| 2. | Delivery of Cyber Security Items/Solution | T1=T0+ 12 weeks |
| 3. | Deployment of Manpower for Operation and Maintenance | T2=T1 |
| 4. | Completion of Installation, Configuration testing commissioning and operationalized of all supplied Cyber Security Items/ solution) | T3=T2+8 weeks |
| | **Total Timeline** | **T0+20 Weeks** |

**Note** Final Acceptance of solution: After completion of installation, commissioning, testing and integration all the supplied cyber security items/solutions as per scope of work. NIC security team shall issue Completion certificate. Date of completion certificate shall be treated as date of final acceptance of entire solution i.e. date of FAT-cum-Go-live.

### 8.2 Validity of Rates

**8.2.1** The finalised L1 rates after RA shall remain valid during the Contract Period. The Purchaser reserves the right to use these rates for placing additional Work Orders, subjected to 40% of the finalised L1 value for other NDCs, including Delhi, Pune, Hyderabad, Bhubaneswar and Guwahati. The MSP shall accept all such subsequent Work Orders.

## 9. Payment Terms

### 9.1. Overview

**9.1.1** A pre-received invoices (Three copies) shall be submitted in the name of "NATIONAL INFORMATICS CENTRE" at NIC, New Delhi.

**9.1.2** Invoices shall be genuine and accurate in all respects.

**9.1.3** The invoices raised by the MSP to the Purchaser shall be inclusive of duties, fees, levies, charges, commissions and tax as applicable under Applicable Laws.

**9.1.4** After receiving the detailed invoices for the quarterly payments, each invoice payment shall undergo scrutiny for breach of SLA requirements and other factors and payment shall be released to the MSP after deducting the penalty amount, if any, and tax deduction at source as per Applicable Laws.

**9.1.5** Payments shall be made by the Purchaser to the MSP in accordance with the scope of work as given in paragraph 5, SLA requirements as given in paragraph 10 and other terms and conditions of this RFP or Contract.

**9.1.6** Payment shall be made using ECS, NEFT or RTGS.

**9.1.7** Payment shall be made in Indian Rupees (INR).

**9.1.8** The Purchaser shall release the payment, subject to the condition that the invoice and all supporting documents produced are in order.

**9.1.9** 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.

**9.1.10**In respect of any claim where the same is raised but the invoice with requisite details is not made available in time for the Purchaser to be in position to claim input tax credit under the Applicable Laws governing taxation or the documents necessary for making such claim are not made available in time for the Purchaser to make such claim, the MSP shall not be entitled to payment of such input tax credit amount as the Purchaser would not be in position to claim.

**9.1.11**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.

**9.1.12**Payment will be done after deduction of all applicable penalties, for the defaults like delay in delivery, delay in completing the installation of all the ordered items, adherence to SLA as defined in Section 10.

### 9.2. Payment Schedule

| Sr. No | Payment Milestone | Payment % |
|---|---|---|
| 1 | On Delivery of Cyber Security hardware. | 70% of the cost of the delivered product/solution in good condition. |
| 2 | Installation, Configuration testing commissioning and operationalized of Cyber Security Items/ solution (Acceptance Date) of Cyber Security hardware. | Remaining 30% of the cost of the delivered product/solution |
| 3 | On Delivery of licences of Cyber Security software solutions. | 70 % of the cost of the software of the 1st Year |
| 4 | Installation, Configuration testing commissioning and operationalized of Cyber Security software Licences (Acceptance date) | 30 % of the cost of the software of the 1st Year |
| 5 | Renewals of licences of software at sr. no 3, for 2nd year and 3rd year | Yearly advanced payment at the start of each year on submission of Licence installation certificate. |
| 6 | AMC of hardware for 2nd, 3rd year | Quarterly in arrears |
| 7 | Manpower deployment | Quarterly in arrears |

## 10. Penalty Terms

### 10.1. Penalty for delay

**10.1.1** All activities outlined under paragraph no. 9.1 – Timelines shall be completed strictly within the stipulated timelines. In the event of any delay in completion of these activities, the Managed Service Provider (MSP) shall be liable to pay penalties as specified in the RFP.

| Sr. No | Project Activities | Penalty |
|---|---|---|
| 1. | Delivery of Security solution | 1. 0.5 % of cost of the delayed item value will be applied for each week beyond the specified timeline. In case of delayed items/solutions |

| Sr. No | Project Activities | Penalty |
|---|---|---|
| | | would not impact to other services or solutions functioning.<br>2. 0.5 % of cost of the delayed item value and all items/solutions value which are impacted by these delayed items/solutions will be applied penalty for all those items each week beyond the specified time line. |
| **2.** | Installation, Configuration testing commissioning and operationalized of Cyber Security Items/ solution | 1. 0.1 % of cost of the delayed item value will be applied for each week beyond the specified timeline. In case of delayed items/solutions would not impact to other services or solutions functioning.<br>2. 0.1 %  of cost of the delayed item value and all  items/solutions  value which are impacted by these delayed items/solutions  will be applied penalty for  all those items each week beyond the specified time line |
| The overall penalty is capped at 10% of the respective work order value. | | |

Note:

Delay exemptions due to ‘site not ready’ shall be considered only upon submission of the Annexure – Site Not Ready Certificate, duly issued by the nominated Site In-Charge of NIC.

## 11. Service Level Agreement

### 11.1Overview

11.1.1 The MSP shall render the services strictly adhering to the SLAs mentioned in this section. Any delay on the part of the MSP in the performance shall attract penalty. Post that Purchaser shall have the option of getting the work done through alternate sources at the cost and risk of the MSP, which will be realized from applicable payments of the MSP, or from the Performance Bank Guarantee or by raising claims.

11.1.2 MSP shall maintain spare units of the required Cyber Security Solutions at appropriate locations to meet the Service Level Agreement (SLA) requirements.

11.1.3 MSP must choose best of the breed security solution to achieve the SLA requirement.

11.1.4 Any recovery of penalty shall not relieve the MSP in any way, from any of its obligations to complete the works or services or from any other obligations and liabilities under the SLAs of RFP.

11.1.5 Purchaser reserves the right to levy or waive off penalty considering various circumstances at any point in time.

11.1.6 If at any time during performance of the work order, the MSP encounter conditions impeding timely execution of the ordered services, the MSP shall promptly notify Purchaser in writing of the fact of the delay, it’s likely duration and its cause(s).

11.1.7 For non-execution of work orders for reasons attributable to the MSP, Purchaser would be free to use MSP Performance Bank Guarantee received against the affected work order and/or termination of the Contract, provided agency fails to remedy such default in spite of 30 days written notice from Purchaser to cure such default.

11.1.8 All SLA calculations will be done on Monthly basis.

11.1.9 Non-Adherence to any of the parameters of the SLA caused wholly by any act of the Purchaser or omission of anything required to be done by the Purchaser shall not be taken into account for the purpose of calculating penalty on the MSP, subject to production of supporting evidence by the MSP.

11.1.10 Any incident to the extent the same is caused wholly on account of any system component both provided and maintained exclusively by the Purchaser shall not be taken into account for the purpose of calculating the penalty on the MSP, subject to production of supporting evidence by the MSP.

11.1.11 The general terms w.r.t the SLA is defined as mentioned below.

11.1.11.1. **Uptime:** Shall mean the time period for the specified services or components with the specified technical service standards are available to the users. Uptime, in percentage, of any component can be calculated as:

**Uptime = {1- [(Downtime) / (Total Time – Scheduled Maintenance Time)]} * 100**

11.1.11.2. **Downtime**: Shall mean the time period for which the specified services or components with specified technical and service standards are not available to the user department and excludes Downtime owing to Force Majeure and Reasons beyond control of the MSP

11.1.11.3. **Scheduled Maintenance Time:** The time that the System is not in service due to a scheduled activity as defined in this SLA. Further, scheduled maintenance time is planned Downtime taken after the permission of the Purchaser.

11.1.11.4. **Incident:** An Incident is an event that results in loss of the confidentiality, integrity or availability of information that Purchaser’s IT system processes and/or stores and/or transmits or a violation of Government security policies or procedures or guidelines or regulations.

11.1.11.5. **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:

- Request to create or delete or modify an Administrator account.
- Request to integrate an asset with the Ticketing Management – Service Desk Platform.
- Request to add/modify /delete the assets details in the Ticketing Management – Service Desk Platform.
- Request to put any incident in the Ticketing Management – Service Desk Platform.
- Request to do entry of follow-up of the incident/ticket in the Ticketing Management – Service Desk Platform.
- Request to investigate or analyse a system for potential security threats or compromise.
- Request to review configuration, design, architecture, deployment of an application or Hardware or software services etc. from the cyber security perspective.
- Request to collect forensic evidence from an asset suspected or confirmed to be infected or compromised related to cyber security infrastructure including its management infrastructure.
- Request to provide the cyber security alerts logs to user/ investigation agencies if required
- Request to analyse logs for a specific anomaly or attack or compromise related to cyber security perspective.
- Request to conduct a security breach assessment related to cyber security perspective.
- Firewall port opening
- Creating policy on security devices.

- Patching of the cyber security infrastructure
- Installation/ de-installation of agents of cyber security solutions in the user VMs, Servers, containers.
- Vulnerability scanning
- Signatures installations at different cyber security solutions.
- Server security agent installation/ de-installation
- Putting the website behind the WAF
- any other request related to cyber security

11.1.12 The proposed solution shall have its own comprehensive monitoring solution. MSP shall use the same tool to do an integrated monitoring of the entire Cyber security infrastructure at Data Centre, DR site, network, and other office equipment. The monitoring tool should provide automated status issues at each layer of Purchaser infrastructure, network, and applications. Dashboard customization and reporting shall be done in consultation with Purchaser.

11.1.13 Note :

11.1.13.1. MSP shall ensure compliance to uptime and performance requirements of project as indicated in the Service Level tables. Any upgrades or major changes to the setup shall be accordingly planned by MSP to ensure the SLA requirements.

- Submit a monthly MIS report covering all key details of compliance with the Service Levels and KPIs.
- Create other reports, trend analysis and such other information as Purchaser may reasonably request to verify MSP's performance and compliance against the Service Levels and KPIs.

11.1.13.2. Within five (5) Business Days of the end of each month, MSP shall provide Purchaser with a written (paper or electronic) monthly report detailing the actual levels of performance of the solution, the Operations and Maintenance Services, and the Services against the Service Levels and KPIs in such month, together with:

- Details of the monitoring which has been performed by MSP in accordance with scope of work section to this schedule during the relevant month together with a summary of the performance-related issues identified by such monitoring.
- A summary (and each RCA) of all service failures that occurred during the relevant month.
- The service failures which remain unresolved, including an assessment as to how long they will remain unresolved.
- A statement of the applicable penalty in respect of service failures which occurred during the relevant month together with supporting calculations.
- A total number of service failures that have occurred and the amount of applicable penalty that have been incurred by MSP over the past twelve (12) months.
- Relevant particulars of any aspects of MSP's performance which fail to meet the requirements of the Agreement; and
- Such other detail as customer may reasonably require to be included in the monthly report from time to time.
- MSP shall provide the reports referred to the scope of work for MSP's performance against the Service Levels and KPIs on a monthly basis.
- MSP shall, throughout the contract period and as set out in scope of work section, evaluate all data generated as part of the process of monitoring its performance against the Service Levels and KPIs.
- MSP shall present customer with regular proposals (no less than quarterly) on ways in which MSP shall optimize the performance of the Cyber Security solutions and the Services to which each Service Level relates.

- MSP shall ensure that suitably qualified MSP Personnel attend and participate in regular Service Level evaluation meetings with Customer at such times, places and for such purposes as Customer requires.

11.1.13.3. MSP acknowledges and agrees that all data created, handled and/or collected by it in connection with the performance of its obligations under this is deemed to be Purchaser's Confidential Information

### 11.2 SLA for Availability

10.2.1 Penalty for Service and Hardware Failure (for the Data Center security infrastructure components supplied and installed under this contract as well as existing security infrastructure) shall be calculated on the basis of total service failure and individual Hardware/part. In case when both (total service failure and individual Hardware/part failure) are applicable, the higher one shall be considered. Penalty for service and equipment failure shall be deducted from the Performance Bank Guarantee/ quarterly payment applicable.

10.2.2 The downtime shall be the time from the point the respective Cyber Security solution becomes unavailable (due to any reason attributable to the Bidder) till the time the same becomes fully available for carrying out intended operations (including reinstallation, configuration, restoration, boot-up time, etc.) OR till the time a standby Cyber Security Solution is made available for carrying out intended operations (including installation, configuration, restoration, boot-up time, etc.)

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **1.** | DDoS Solution services | >=99.99%<br>Measurement window-24x7, calendar month (excluding approved maintenance) | <=4m and 23s Downtime per month | No Penalty (Complaint) |
| **2.** | | < 99.99% to >=99.98%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 4m and 23s to <=8m and 46s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to **1% of the Purchase Order (PO) value of the respective DDoS solution** for the respective period |
| **3.** | | <99.98% to >=99.95%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 8m 46s to <=21m 55s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to **2% of the Purchase Order (PO) value of the** |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | **respective DDoS solution** for the respective period |
| **4.** | | <99.95% to >=99.90%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 21m 55s to <= 43m 50s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to **5% of the Purchase Order (PO) value of the respective DDoS solution** for the respective period |
| **5.** | | <99.90%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 43m 50 s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to **10% of the Purchase Order (PO) value of the respective DDoS solution** for the respective period plus SLA breach notice; recurring breaches may lead to contract termination |
| **6.** | Perimeter Firewall | >=99.99%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | <=4m and 23s Downtime per month | No Penalty (Complaint) |
| **7.** | | < 99.99% to >=99.98% | > 4m and 23s to <=8m and 46s Downtime per month | The Managed Service Provider |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | Measurement window -24x7, calendar month (excluding approved maintenance) | | (MSP) shall be liable to pay a penalty equivalent to **1% of the Purchase Order (PO) value of the respective Perimeter Firewall solution** for the respective period |
| **8.** | | <99.98% to >=99.95%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 8m 46s to <=21m 55s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to **2% of the Purchase Order (PO) value of the respective Perimeter Firewall solution** for the respective period |
| **9.** | | <99.95% to >=99.90%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 21m 55s to <= 43m 50s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to **5% of the Purchase Order (PO) value of the respective Perimeter Firewall solution** for the respective period. |
| **10.** | | <99.90%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 43m 50 s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | **10% of the Purchase Order (PO) value of the respective Perimeter Firewall solution** for the respective period plus SLA breach notice; recurring breaches may lead to contract termination |
| **11.** | WAF Services | >=99.99%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | <= 4m 23s Downtime per month | No Penalty (Complaint) |
| **12.** | | <99.99% to >=99.97%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | >4m 23s to <=13m 8.9s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty of **0.1% of the Purchase Order (PO) value of the respective WAF solution** for the respective period. |
| **13.** | | <99.97%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | >13m 8.9s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty of **0.3% of the Purchase Order (PO) value of the respective WAF solution** for the respective period plus SLA breach notice; recurring breaches may lead to contract termination |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **14.** | 1. IPS Service (Type-1, Type-2 and Type-3)<br>2. POD Firewall<br>3. SSL off loader Services (Type-1 and Type-2)<br>4. Anti APT Servic<br>5. NDD (Network Detection and Response) including sensors, collectors, and management consoles | >=99.99%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | <= 4m 23s Downtime per month | No Penalty |
| **15.** | | <99.99% to >=99.97%<br>Measurement window-, calendar month (excluding approved maintenance) | >4m 23s to <=13m 8.9s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to 0.03**% of the Purchase Order (PO) value of *respective Cyber Security device*** for the respective period.. |
| 1 | | < 99.97% to >= 99.95<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 13m 9s to ≤ 21m 55s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to 0.05**% of the Purchase Order (PO) value of *respective Cyber Security device*** for the respective period. |
| **17.** | | < 99.95% to >= 99.90<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 21m 55s to ≤ 43m 49s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to 0.10 **% of the Purchase Order (PO) value of *respective Cyber Security device*** for the respective period |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **18.** | | < 99.90%<br>Measurement window -24x7, calendar month (excluding approved maintenance) | > 43m 49s Downtime per month | The Managed Service Provider (MSP) shall be liable to pay a penalty equivalent to 0.20 **% of the Purchase Order (PO) value of *respective Cyber Security device*** for the respective period + NIC reserves the right to invoke PBG / terminate the contract |
| **19.** | Availability of ICT Infrastructure of Software Solution | >=99.98% (Measured Uptime (per quarter)<br>(excluding approved maintenance) | <= 8 minutes 46 seconds (Measured down time per quarter) | No Penalty (Compliant) |
| **20.** | | <99.98% to >=99.95% Measured Uptime (per quarter)<br>(excluding approved maintenance) | > 8 minutes 46 seconds to <=21m 55s (Measured down time per quarter) | The Service Provider shall be liable to a penalty of **0.03% of the quarterly payment value of the respective affected Software Solution.** |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **21.** | | < 99.95% to ≥ 99.90% Measured Uptime (per quarter)<br>(excluding approved maintenance) | > 21 minutes 55 seconds to ≤ 43 minutes 49 seconds<br>(Measured down time per quarter) | The Service Provider shall be liable to a penalty of **0.05% of the quarterly payment value of the respective affected Software Solution.** plus SLA breach notice; recurring breaches may lead to contract termination |
| **22.** | | < 99.90%<br>Measured Uptime (per quarter)<br>(excluding approved maintenance) | > 43 minutes 49 seconds in a quarter<br>(Measured down time per quarter) | The Service Provider shall be liable to a penalty of **0.10% of the quarterly payment value of the respective affected Software Solution.** plus SLA breach notice; recurring breaches may lead to contract termination |
| **23.** | RMA (Return Merchandise Authorization)Delivery (Replacement Hardware) | | Replacement hardware must be delivered **by the Next Business Day (NBD)** from the time of reporting/approval. | No Penalty (Complaint) |
| **24.** | | | 1–5 days<br>Delivery | **0.05% of PO value** of the respective hardware solution per day |
| **25.** | | | 6–10 days<br>Delivery | **0.10% of PO value** of the respective hardware solution per day |
| **26.** | | | > 10 days<br>Delivery | **0.20% of PO value** of the respective hardware |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | solution per day, plus SLA breach notice |
| **27.** | | | > 15 days<br>Delivery | The Managed Service Provider (MSP) shall be liable to a penalty of **0.50% of PO value** of the respective hardware solution per day, plus SLA breach notice and NIC may procure replacement at the **risk & cost of MSP** |
| **28.** | After RMA, the faulty device must be configured and fully operational, including restoring the configuration, | | Device must be configured, restored with the latest backup, and made fully operational within **12 hours** of delivery | No Penalty (Compliant |
| **29.** | | | Device not operational beyond 12 hours of receipt. | The Managed Service Provider (MSP) shall be liable to a penalty of **0.05% of PO value of the respective hardware solution per day of delay** until acceptance by NIC |
| **30.** | Any Feature Modification Request (FMR) submitted by NIC | | **≤ 3 months** (from date of submission or unless mutually agreed otherwise in writing) FMR delivery by MSP/OEM | No penalty (Compliant) |
| **31.** | | | > 3 months to ≤ 6 months.<br>Delay beyond SLA but within 3 additional months | The Managed Service Provider (MSP) shall be liable to a penalty of 0.05% of PO value of the respective solution per month of delay |
| **32.** | | | > 6 months to ≤ 9 months<br>Prolonged delay despite SLA extension | The Managed Service Provider |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | (MSP) shall be liable to a penalty of **0.10% of PO value of the respective solution per month of delay**, plus SLA breach notice |
| **33.** | | | > 9 months<br>Excessive non-compliance | The Managed Service Provider (MSP) shall be liable to a penalty of 1% **of PO value of the respective solution per month of delay**, plus SLA breach notice and NIC reserves the right to **terminate the contract / procure alternatives at risk and cost of MSP** |
| **34.** | Detection by Network Detection and Response (NDR) Solution | | **Detection:-Critical Alerts (e.g., malware, lateral movement, command & control)** must be generated within **5 minutes** of network traffic observation.<br>Continuous monitoring Measurement Window | The Managed Service Provider (MSP) shall be liable to a penalty of<br>For each violation, **0.05% of the PO value of NDR solution.** |
| **35.** | Response by Network Detection and Response (NDR) Solution | | Response **Incidents** *Acknowledgment*: Within **24 hour**<br>Measurement Window - 24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of<br>Delay beyond SLA timelines will attract **0.05% of PO** |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | **value per incident.** |
| **36.** | Response by Network Detection and Response (NDR) Solution | | Reporting & Compliance<br>• Daily **Alerts Summary**: Delivered within **24 hours**.<br>• Weekly **Threat Report**: Shared every **Monday**.<br>• Monthly **Compliance Report**: SLA adherence, false positives/negatives, and performance benchmarks.<br>Measurement Window - Agreed timeline | The Managed Service Provider (MSP) shall be liable to a penalty of Non-submission or delayed submission beyond 3 working days **0.02% of PO value per instance**. |
| **37.** | False Positive/ Nagative Detection by NDR | | • False positive rate must be ≤ 5%. monthly average<br>• False negative rate must be ≤ 2% monthly average | The Managed Service Provider (MSP) shall be liable to a penalty If thresholds are breached for two consecutive months, **0.5% of PO value per instance** will be deducted. |
| **38.** | For any security incident involving the devices, the vendor must provide a Root Cause Analysis (RCA) | | Within 7 working days | No Penalty (Complaint) |
| **39.** | | | Beyond the 7 working days | The Managed Service Provider (MSP) shall be liable to a penalty of 0.05% of the PO value of the solution per day |
| **40.** | Perimeter and POD Firewall | | Firewall should process traffic at committed throughput (as per technical specs with 64-byte packet size) | No penalty (Compliant) |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | Throughput & Performance | | Measurement window: Continuous monitoring | |
| **41.** | | | For degradation > 5% from committed throughput: | The Managed Service Provider (MSP) shall be liable to a penalty of 0.05% of PO Value per instance |
| **42.** | Threat Detection & Prevention Efficiency by Network IPS solution | | IPS must detect and block ≥ 99% of known exploits, malware traffic, and protocol violations as per signature database<br>Measurement window Continuous monitoring & validation tests | The Managed Service Provider (MSP) shall be liable to a penalty of For detection rate falling below threshold: 0.05% of PO value per instance |
| **43.** | Latency/Performance Impact by Network IPS solution | | IPS should introduce latency ≤ 150 microseconds in inline mode at committed throughput.<br>Measurement window- Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of For degradation >10% from committed throughput or latency SLA violation: 0.05% of PO value per instance. |
| **44.** | Zero-Day/Custom signature Deployment in network IPS solution. | | IPS custom signatures for emerging threats must be created and implemented within 3 days of request<br>Measurement window 24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond SLA: 0.05% of PO value per violation. |
| **45.** | False positive/False Negative of | | False Positive Rate ≤ 5% False Negative Rate ≤ 2%<br>Measurement window- Monthly | The Managed Service Provider (MSP) shall be liable to a penalty of |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | signatures | | | Breach for 2 consecutive months → 0.5% deduction of PO value per violation. |
| **46.** | Time-to-Detect (TTD) by DDoS solution | | Detect volumetric and protocol attacks within ≤ 30 seconds.<br>Measurement window-Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond SLA: 0.05% of PO value per incident. |
| **47.** | Time-to-Mitigate (TTM) by DDoS solution | | Mitigate volumetric/protocol/ application-layer attack within ≤ 30 seconds after detection.<br>Measurement window- 24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond SLA: 0.1% of PO value per incident |
| **48.** | Traffic Handling Capacity by DDoS solution | | Should handle committed bandwidth as per technical specification.<br>Measurement window- Continuous | The Managed Service Provider (MSP) shall be liable to a penalty of For degradation > 5% of committed capacity: 0.05% of PO value per instance. |
| **49.** | False Positive Rate of DDoS solution | | ≤ 5% of clean traffic should be wrongly blocked<br>Measurement window- Monthly | The Managed Service Provider (MSP) shall be liable to a penalty of Breach for 2 consecutive months: 0.5% deduction of PO value. |
| **50.** | False Negative Rate for DDoS solution | | ≤ 2% of malicious traffic should bypass mitigation.<br>Measurement window- Monthly | The Managed Service Provider (MSP) shall be liable to a penalty of |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | Breach for 2 consecutive months: 0.5% deduction of PO value. |
| **51.** | Threat Detection & Blocking Efficiency of WAF | | Detect & block ≥ 99% of OWASP Top-10 threats (SQLi, XSS, CSRF, RFI, etc.)<br>Measurement window -Continuous monitoring & validation | The Managed Service Provider (MSP) shall be liable to a penalty of Failure to block per test case: 0.05% of PO value per violation. |
| **52.** | Latency/Performance Impact of WAF | | Additional latency ≤ 200 ms at committed throughput.<br>Measurement window -Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of For SLA breach >10% latency overhead: 0.05% of PO value. |
| **53.** | Signature & Policy Updates in WAF | | OEM signatures to be updated within 24 hrs of release; Custom rules applied within 4 hrs of request.<br>Measurement window- 24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay: 0.05% of PO value per violation. |
| **54.** | Zero-Day Protection in WAF | | Virtual patching within 4 hours of disclosure/request.<br>Measurement window -24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond SLA: 0.05% of PO value per incident. |
| **55.** | False Positives / False Negatives in WAF | | False Positive (Genuine traffic wrongly blocked Rate ≤ 5% ;<br>False Negative( Malicious traffic by pass) Rate ≤ 2%<br>Measurement window -Monthly | The Managed Service Provider (MSP) shall be liable to a penalty of Breach for 2 consecutive |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | months → 0.5% deduction of PO value per violation. |
| **56.** | SSL/TLS Throughput Performance in SSL Offloader | | Should support committed SSL/TLS sessions per second and throughput (as per technical specification)<br>Measurement window -Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of For degradation >5% from committed throughput: 0.05% of PO value per instance |
| **57.** | Latency Overhead in SSL Offloader | | Additional latency ≤ 100 ms for SSL termination.<br>Measurement window- Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of Breach of latency SLA: 0.05% of PO value. |
| **58.** | Detection Efficiency of Anti-APT | | Must detect and analyze ≥ 99% of known APT behaviors (malware, C2 communication, lateral movement, data exfiltration)<br>Measurement window -Continuous monitoring, test validations | The Managed Service Provider (MSP) shall be liable to a penalty of Failure per instance: 0.05% of PO value. |
| **59.** | Time-to-Detect (TTD) in Anti APT | | Detect advanced malware/APT activity within ≤ 10 minutes of traffic/file observation.<br>Measurement window -Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond SLA: 0.05% of PO value per incident |
| **60.** | Time-to-Respond (TTR) in Anti-APT | | Automated containment/blocking within ≤ 30 minutes of detection<br>Measurement window -24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | SLA: 0.05% of PO value per incident. |
| **61.** | Threat Intelligence Updates in Anti-APT | | OEM threat feeds & sandbox signatures updated within 24 hrs of release.<br>Measurement window 24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay: 0.02% of PO value per violation. |
| **62.** | Custom IOC/Rule Deployment in Anti APT | | Deployment of custom IoCs/rules within 4 hrs of request.<br>Measurement window 24x7 | The Managed Service Provider (MSP) shall be liable to a penalty of Delay beyond SLA: 0.05% of PO value per violation |
| **63.** | False Positive/ Negative Rates in Anti APT | | False Positive ≤ 5%,<br>False Negative ≤ 2%<br>Measurement window -Monthly | The Managed Service Provider (MSP) shall be liable to a penalty of Breach for 2 consecutive months → 0.5% deduction of PO value. |
| **64.** | Signatures for DDoS | | Provide signatures within 12 hours from the requested time | No penalty (Compliant) |
| **65.** | | | Beyond 12 hours | The Managed Service Provider (MSP) shall be liable to a penalty of Rs.10,000 per hour |
| **66.** | Signatures for IPS | | Deployment of signatures within 12 hours after release. | No penalty (Compliant) |
| **67.** | | | Beyond 12 hours | The Managed Service Provider (MSP) shall be liable to a penalty of Rs.10,000 per hour |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **68.** | Custom signatures for IPS, WAF and Anti APT | | Must be created by OEM within 1 working days | No penalty (Compliant) |
| **69.** | | | Beyond the 1 working days | The Managed Service Provider (MSP) shall be liable to a penalty of Rs.10,000 Per day. |
| **70.** | Updation of N-1 firmware update. | | Updated within 7 days from the release of a new firmware update. | No penalty (Compliant) |
| **71.** | | | Beyond the 7 days | The Managed Service Provider (MSP) shall be liable to a penalty of Rs. 10,000 per day |
| **72.** | If any bugs hits in security solution, then developing hotfix from the OEM | | Developing hotfix from the OEM within 24 hours. | No penalty (Compliant) |
| **73.** | | | Beyond the 24 hours | The Managed Service Provider (MSP) shall be liable to a penalty of Rs. 50,000 per hour. |
| **74.** | NIC cannot provide a snapshot backup of security devices to the TAC team for replicating unknown technical issues. Instead, the vendor must offer an alternate solution, such as | | The on-site environment must be established within 2 days of the request to replicate production issues. | No penalty (Compliant) |
| **75.** | | | Beyond the 2 days | The Managed Service Provider (MSP) shall be liable to a penalty of Rs. 10000 Per day. |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | setting up an on-site test environment. | | | |
| **76.** | For security solutions, if vulnerabilities are discovered in a new firmware release, | | The MSP must intimate and provide an update/patch within 3 days. | No penalty (Compliant) |
| **77.** | | | Beyond the 3 days | The Managed Service Provider (MSP) shall be liable to a penalty of Rs. 25,000 per day. |
| **78.** | Security patches for known vulnerabilities must be provided | | Within 7 days of their release. | No Penalty |
| **79.** | | | Beyond the 7 days | The Managed Service Provider (MSP) shall be liable to a penalty of Rs, 50,000 per day. |
| **80.** | If a product fails at least 3 times in 3 months, indicating chronic system design, manufacturing defects, or quality control issues. | | The MSP must replace the product at their cost and risk within 30 days of the third failure. | No penalty (Compliant) |
| **81.** | | | Beyond the 30 days. | The Managed Service Provider (MSP) shall be liable to a penalty of 0.05% of the PO value of the cyber security Hardware per week |
| **82.** | Applications protected by security devices should not stop, misbehave, or slow down due | | No such instance | No penalty (Compliant) |
| **83.** | | | If arise any instance | The Managed Service Provider (MSP) shall be liable to a penalty of 0.05% of the PO value of the cyber security |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | to device misconfiguration like false positives of device signatures, geo-location, hotfix, patch updates etc. | | | Hardware per instance. |
| **84.** | For critical issues such as security breaches like if NIC get to know that some data is breaches continuously | | If breaches due to inability of the cyber security solution | The Managed Service Provider (MSP) shall be liable to a penalty of 0.1% of the PO value of the cyber security solution per breach |
| **85.** | The incidents like performance degradation, | | Must be resolved within 48 hours | No penalty (Compliant) |
| **86.** | | | Beyond 48 hours | The Managed Service Provider (MSP) shall be liable to a penalty of 0.1% of the PO value of the cyber security solution per day. |
| **87.** | HIPS Detection & Prevention in Server security | | Detect & block ≥ 99% of known exploits, malware traffic, privilege escalation attempts<br>Measurement window-Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty For detection efficiency <99%: 0.05% of PO value per violation |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **88.** | Application Control in Server security | | Unauthorized application execution blocked within 5 minutes of detection Measurement window -24x7 | The Managed Service Provider (MSP) shall be liable to a penalty if Delay beyond SLA: 0.05% of PO value per violation |
| **89.** | Host-based Firewall in Server security | | Policy enforcement & changes applied within 4 hours of request.<br>Measurement window-Business hours (24x7 for critical changes) | The Managed Service Provider (MSP) shall be liable to a penalty if Delay: 0.05% of PO value per violation. |
| **90.** | Zero-Day / IOC Deployment in Server Security | | Custom signatures / IoCs deployed within 4 hours of request<br>Measurement window -24x7 | The Managed Service Provider (MSP) shall be liable to a penalty if Delay beyond SLA: 0.05% of PO value per violation |
| **91.** | Performance Impact in server security | | Security agents must not exceed 5% CPU or 10% memory utilization on protected servers<br>Measurement window -Monthly performance audit | The Managed Service Provider (MSP) shall be liable to a penalty for Breach: 0.05% of PO value per violation |
| **92.** | False Positive/ Negative Rates in server security | | False Positive ≤ 5%,<br>False Negative ≤ 2%<br>Measurement window -Monthly | The Managed Service Provider (MSP) shall be liable to a penalty for Breach for 2 consecutive months → 0.5% deduction of PO value |
| **93.** | Critical Security Patch availability (Vendor | | Must be available all patches of all vendors all os and software's within ≤ 72 hours of vendor release. | The Managed Service Provider (MSP) shall be liable to a penalty if Delay |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | Released) in Patch management | | Measurement window -Continuous monitoring | per system: 0.05% of PO value per violation |
| **94.** | Zero-Day / Emergency Patch availability | | Emergency security patches (zero-day) must be available within ≤ 24 hours of release/advisory<br>Measurement window -24x7 | The Managed Service Provider (MSP) shall be liable to a penalty if Delay: 0.05% of PO value per violation |
| **95.** | Integration with Vulnerability Management in Patch management | | Patch solution must integrate with vulnerability assessment tool and remediate detected vulnerabilities within SLA<br>Measurement window -Month | The Managed Service Provider (MSP) shall be liable to a penalty for Failure to remediate within SLA: 0.1% of PO value per month. |
| **96.** | Real-Time Monitoring in DAM | | Capture & analyze 100% of database transactions (queries, DML, DDL, privileged actions) in real time.<br>Measurement window-Continuous | The Managed Service Provider (MSP) shall be liable to a penalty for Failure per instance: 0.05% of PO value. |
| **97.** | Policy Enforcement in DAM | | Database security policies (blocking, alerting, masking) must be applied within ≤ 4 hours of request<br>Measurement window -Business hours (24x7 for critical changes) | The Managed Service Provider (MSP) shall be liable to a penalty if Delay: 0.05% of PO value per violation |
| **98.** | Detection Efficiency in DAM | | Must detect ≥ 99% of suspicious DB activities (SQL injection, privilege escalation, unauthorized access, data exfiltration)<br>Measurement window -Continuous | The Managed Service Provider (MSP) shall be liable to a penalty if Detection <99%: 0.05% of PO value per violation |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **99.** | Latency Impact in DAM | | Monitoring should not add > 2% query response overhead.<br>Measurement window- Continuous | The Managed Service Provider (MSP) shall be liable to a penalty for SLA breach: 0.05% of PO value |
| **100.** | Audit Log Integrity in DAM | | Audit logs must be tamper-proof & retained for ≥ 6 months<br>Measurement window -Quarterly verification | The Managed Service Provider (MSP) shall be liable to a penalty if Failure: 0.05% of PO value per violation. |
| **101.** | False Positive / Negative Rates in DAM | | False Positive ≤ 5%,<br>False Negative ≤ 2%<br>Measurement window -Monthly | The Managed Service Provider (MSP) shall be liable to a penalty for Breach for 2 consecutive months → 0.5% deduction of PO value. |
| **102.** | Policy Enforcement in DLP | | DLP policies (blocking, alerting, encryption, quarantine) applied within ≤ 4 hours of request.<br>Measurement window -Business hours (24x7 for critical changes) | The Managed Service Provider (MSP) shall be liable to a penalty if Delay: 0.05% of PO value per violation |
| **103.** | Detection Efficiency in DLP | | ≥ 99% detection of sensitive data types (PII, PCI, HIPAA, classified docs, etc.) across endpoints, email, web & cloud<br>Measurement window -Continuous monitoring | The Managed Service Provider (MSP) shall be liable to a penalty of The Managed Service Provider (MSP) shall be liable to a penalty if Detection <99% → 0.05% of PO value per violation |
| **104.** | False Positive / | | False Positive ≤ 5%,<br>False Negative ≤ 2% | The Managed Service Provider |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
|  | False Negative Rates in DLP |  | Measurement window -Monthly | (MSP) shall be liable to a penalty for Breach for 2 consecutive months → 0.5% deduction of PO value |
| **105.** | Endpoint Agent Performance Impact in DLP |  | DLP agent overhead ≤ 5% CPU & ≤ 10% memory utilization<br>Measurement window -Monthly audit | The Managed Service Provider (MSP) shall be liable to a penalty for SLA breach: 0.05% of PO value. |
| **106.** | Authentication Success & Session Stability in PIM/PAM |  | ≥ 99.9% of legitimate privileged sessions authenticated and stable<br>Measurement window- PAM audit logs | The Managed Service Provider (MSP) shall be liable to a penalty For each 0.1% drop below SLA → 0.02% of PO value. |
| **107.** | Critical Incident Response (e.g., credential leakage, unauthorized privilege escalation) in PIM/PAM |  | Response within 15 minutes<br>Measurement window -SOC/NOC ticketing system | The Managed Service Provider (MSP) shall be liable to a penalty if Delay >15 mins but ≤30 mins → 0.05% PO value per incident >30 mins delay → 0.1% PO value per incident |
| **108.** | Privileged Session Monitoring & Recording in PIM/PAM |  | 100% of privileged sessions must be recorded, stored, and retrievable<br>Measurement window - Audit logs, compliance checks | The Managed Service Provider (MSP) shall be liable to a penalty For each missing session recording → 0.05% of PO value per incident |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| **109.** | Policy Enforcement (e.g., MFA, password rotation, just-in-time access) in PIM/PAM | | ≥ 99.9% enforcement of configured PAM policies<br>Measurement window- Reports & random sampling | The Managed Service Provider (MSP) shall be liable to a penalty For every 0.1% deviation below 99.9%, 0.02% of PO value. |
| **110.** | Change Request Fulfillment (Role/Policy Changes) in PIM/PAM | | Within 8 working hours of approval<br>Measurement window- Change management system | The Managed Service Provider (MSP) shall be liable to a penalty if Delay >8 hrs to ≤24 hrs → 0.05% PO value per request<br>>24 hrs → 0.1% PO value per request |
| **111.** | False Positive / False Lockout Rate in PIM/PAM | | 2% of total privileged accounts per quarter<br>Measurement window -Incident review | The Managed Service Provider (MSP) shall be liable to a penalty If >2% false lockouts, penalty 0.02% of PO value per 0.5% additional deviation |
| **112.** | VA Coverage (Assets/Scope) in Vulnerability Assessment | | 100% of in-scope servers, applications, and network devices must be scanned<br>Measurement window- Scan reports, asset inventory | The Managed Service Provider (MSP) shall be liable to a penalty For each asset missed in the agreed scope → 0.05% of PO value per instance |
| **113.** | Assessment Frequency in Vulnerability | | Quartely VA (or as mandated by NIC/Regulatory body)<br>Measurement window -VA schedules & reports | The Managed Service Provider (MSP) shall be liable to a penalty if Delay ≤7 days → |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | Assessment | | | 0.02% of PO value<br>Delay >7 days → 0.05% of PO value |
| **114.** | Critical Vulnerability Detection in Vulnerability Assessment | | ≥ 99% detection of known CVEs (as per NVD/OEM feeds)<br>Measurement window -OEM scan reports, sample validation | The Managed Service Provider (MSP) shall be liable to a penalty For every 1% drop below SLA → 0.05% of PO value. |
| **115.** | Critical Vulnerability Notification Vulnerability Assessment | | Immediate alerting of critical/high vulnerabilities (within 4 hours of detection)<br>Measurement window -SOC ticketing system | The Managed Service Provider (MSP) shall be liable to a penalty if Delay ≤8 hrs → 0.05% PO value per instance<br>Delay >8 hrs → 0.1% PO value per instance |
| **116.** | False Positive Rate Vulnerability Assessment | | ≤ 5% of total reported vulnerabilities<br>Measurement window -Incident review & validation | The Managed Service Provider (MSP) shall be liable to a penalty If >5% false positives, penalty 0.02% of PO value 1% deviation |
| **117.** | False Negative Rate in Vulnerability Assessment | | ≤ 1% of total validated vulnerabilities per quarter<br>Measurement window -Random sampling & audit | The Managed Service Provider (MSP) shall be liable to a penalty If >1% false negatives, penalty 0.05% of PO value per 0.5% deviation |
| **118.** | Authentication Success Rate<br>In AAA | | ≥ 99.9% of valid users/devices authenticated successfully<br>Measurement window -Audit logs, test cases | The Managed Service Provider (MSP) shall be liable to a penalty For every 0.1% |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | | | | deviation below SLA → 0.02% of PO value |
| **119.** | Authorization Policy Enforcement in AAA | | ≥ 99.9% accuracy in applying configured access policies<br>Measurement window -Policy compliance reports | The Managed Service Provider (MSP) shall be liable to a penalty For each 0.1% deviation below SLA → 0.02% of PO value |
| **120.** | Critical Incident Response (AAA Outage or Authentication Failure Impacting Ops) in AAA | | Response within 15 minutes<br>Measurement window -SOC/NOC ticketing system | The Managed Service Provider (MSP) shall be liable to a penalty if Delay >15 mins ≤30 mins → 0.05% PO value per incident<br>Delay >30 mins → 0.1% PO value per incident |
| **121.** | Accounting / Logging Accuracy in AAA | | 100% of user/admin access and actions logged & retrievable<br>Measurement window -Audit & log review | The Managed Service Provider (MSP) shall be liable to a penalty for Each missing/unavailable log → 0.05% of PO value per instance |
| **122.** | Latency in Authentication/Authorization in AAA | | ≤ 200 ms for 95% of transactions<br>Measurement window -System performance metrics | The Managed Service Provider (MSP) shall be liable to a penalty If >200ms sustained for >5% of transactions → 0.05% of PO value |
| **123.** | Policy/Role Change Impleme | | Within 8 working hours of approval | The Managed Service Provider (MSP) shall be |

| Sr. No | Description/Service | Uptime target | Monthly Target | Monthly Penalty |
|---|---|---|---|---|
| | ntation in AAA | | Measurement -Change management records | liable to a penalty if Delay ≤24 hrs → 0.05% PO value per request<br>Delay >24 hrs → 0.1% PO value per request |

**Note#**

1. Maximum capping of penalty will be 10 % of each above instance and also accumulative penalty will be capped to 10 % of the work order value of hardware and software. Penalty will be deducted from the PBG or any payment due like Next year software renewal payment/AMC payment.
2. The MSP shall be responsible for the availability of monitoring solutions for measuring the uptime of deployed solutions and Service availability as part of its solution without any additional cost to purchaser.
3. In case of TAC support, Incident response and service request, a day shall start from time the incident or service is logged or registered.

### 11.3SLA for manpower and services:

Penalties will be levied on the service provider for the violation of service level agreement of the contract as mentioned below:

| Sr. No | Service level agreement | Penalties for non-compliance |
|---|---|---|
| 1. | Non-deployment of total manpower mentioned in the contract as per the deployment plan | Penalty for each non-deployment resources and day at the rate of daily remuneration of the non-deployed resource (excluding taxes) in addition to treating the non-deployment period as Leave without pay (LWP). |
| 2. | If any manpower allotted to a certain task is temporarily absent or permanently leaves the job. | The bidder will ensure that an interim replacement with expertise in the same area with similar/higher skill level is provided within 48 hours in case of temporary absence and within 2 weeks in case of permanent termination. NIC will also not pay to the bidder the manpower fees for the period of temporarily/permanently absent. During this time, any interruption in services due to absence of such manpower will be the responsibility of the bidder and any penalty arising of the same will be payable by the bidder. In case the Bidder is unable to replace the manpower within the stipulated period of time, it will be liable to pay a penalty equal to the amount of the fee being paid to the bidder for the manpower in addition to deducting the fee for the absent period on a pro-rata basis. |

| Sr. No | Service level agreement | Penalties for non-compliance |
|---|---|---|
| 3. | If any task assigned to a particular resource is pending 24 hours. | After 24 hours there would be a penalty of Rs. 2000 per day till the task is completed. |
| 4. | If the employee is found responsible for any theft, loss of material/ articles and damages | Immediate payment in actuals, equivalent to the value of the article theft/lost/damaged. Replacement within 5 days/cancellation of contract as decided by the buyer depending on the gravity of the act. |
| 5. | If the employee is found responsible for disobedience/ misconduct | Warning/counselling/Immediate replacement of resource within 5 days as decided by the buyer depending on the gravity of the act |
| 6. | If the employee is absent for more than 2 days without informing or getting prior approval. | Equivalent resources should be deployed within 5 days (i.e. substitutes should report to duty on the 6th day or before), failing which, penalty will be charged for each day of absence at the rate of daily remuneration of the absent resource (excluding taxes) in addition to treating the absence as LWP. |
| 7. | If the employee is found responsible for adopting illegal and foul methods or exercising any corrupt practice in collusion with any third party or officials at the workplace | Immediate replacement within 5 days/ cancellation of the contract with cancellation charges @ 10%, as decided by the buyer depending on the gravity of the act. |
| 8. | Delay in deployment of Project manager. | Penalty at the rate of Rs. 15000 per day of absence of Project Manager. |
| 9. | The resources deployed not be used by the buyer for any other project. | If any resource is found to be working on any project/activity, which is not assigned by NIC, then such manpower shall be immediately terminated from the project. A penalty of 1% of quarterly manpower invoice value shall be levied, for each. |
| 10. | Any breach happens due to wrong configuration deployed by resources. | In the instance of any incident 0.1% of quarterly manpower invoice value shall be levied for any such event. |
| 11. | Any outage of any application/ Data Centre due to wrong configuration deployed by resource | 0.1% of quarterly manpower invoice value shall be levied for each |
| 12. | Firewall Port Implementation Security Policy Enforcement | **1.** Policy updates and rule modifications to be implemented within 30 minutes after approval of Firewall request **During business days and business hour**<br>2. Policy updates and rule modifications to be implemented within 4 hours after approval of Firewall request **during Non-Business day and non-business hour**<br>Beyond this penalty will be Rs. 100 per firewall request. |

| Sr. No | Service level agreement | Penalties for non-compliance |
|---|---|---|
| 13. | Vulnerability Scanning and uploading the VA report | Scanning the server/VMs and uploading the VA scan report in Firewall Access Rules Processing System (FARPS) portal within 4 Hours. Beyond this penalty will be Rs. 1000 per VA request. |
| 14. | Impact in servers VMs during the VA scan in VMs /servers/containers | If VA agent is consuming more than 10 % CPU of the VMs/server/container host during the VA scanning.<br>1% PO value of the VA solution for per 5% beyond the 10% CPU utilization. |
| 15. | Impact in servers VMs during the agent installation of the agent of VA in /servers/containers host | Agent should not stop any services of the VMs, Servers/Containers. If any service stopped due to the agent of the VA then 1 % PO value per services of the VM/Server/Container host. |
| 16. | Delay in VA scanning | Each VM/Server/Container host must be scanned within 30 Minutes, beyond this Rs. 50,000 penalty per 10 minutes. |
| 17. | Putting the Website behind the WAF | 6 Hours after receiving the user request. Beyond this, the penalty will be Rs. 1000 per hour. |
| 18. | Agent installation for solutions such as VA, Server Security, DLP etc. | During business days and business hour : Within 30 minutes<br>Non Business day and non-business hour : within 3 hours.<br>Penalty of Rs 100 per occurrence |
| 19. | Agent decommissioning for solutions such as VA, Server Security, DLP etc. | During business days and business hour: Within 30 minutes<br>Non Business day and non-business hour: within 3 hours. Penalty of Rs 100 per occurrence |
| 20. | User Creation and deletion | During business days and business hour: Within 30 minutes<br>Non Business day and non-business hour: within 3 hours.Penalty of Rs 100 per occurrence |

**Note:**

a. Maximum capping of penalty will be 10 % of each above instance and also accumulative penalty will be capped to 10 % of the quarterly manpower cost.

b. If any SLA is breached beyond 3 instances in any billing period with the maximum penalty, then same shall be treated as a breach of contract and buyer will have full rights to terminate the contract after giving a notice of 30 days

## 12. General Terms and Conditions

### 12.1. Overview

12.1.1 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.

12.1.2 Consortium is not allowed.

12.1.3 The bidder or OEM should undertake to provide support for the supplied solution for entire Contract period and any extension thereof.

12.1.4 The warranty of all supplied solutions shall start after the date of Final Acceptance Test (FAT).

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

12.1.6 In case the MSP is found in-breach of any condition(s) of tender or supply order, at any stage during the life cycle of the Contract, the legal action as per rules or laws, shall be initiated against the bidder and bid securing declaration shall be executed or Security Deposits or PBG shall be forfeited.

12.1.7 Any attempt by bidder to bring pressure towards Purchaser's decision-making process shall result in disqualification from further participation in the present tender.

12.1.8 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 or overwriting, if any, in the tender Bids shall be attested properly by the Bidder, failing which, the Bid shall be rejected.

12.1.9 Upon verification, evaluation or assessment, if in case any information furnished by the bidder is found to be false or incorrect, their bid shall be summarily rejected.

12.1.10 In case the manpower is required to travel outside the location of his or her deployment as per approval of the Purchaser, the Purchaser shall bear the expenses like travel or boarding or lodging of the manpower as per entitlement of a central government officer at the Level 13 of 7th CPC. The MSP shall include these expenses in the quarterly invoice along with all relevant documents that include travel tickets, boarding passes, hotel bills in original, etc. However, no expenses are admissible on account of relocation of MSP resources on projects anywhere in India.

12.1.11 Purchaser shall not be responsible for any misinterpretation or wrong assumption by the Bidder, while responding to this tender.

12.1.12 The decision of Purchaser arrived during the various stages of the evaluation of the bids is final and binding on all vendors. Any representation towards these shall not be entertained by Purchaser.

### 12.2. Change Request

12.2.1 Due to the evolving nature of Cyber Security requirements and the complexity of the solutions, the Purchaser recognizes that changes may be required after implementation of the Cyber Security Solutions. 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 Cyber Security Solutions are addressed.

12.2.2 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.

12.2.3 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.

12.2.4 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 Annexure 20: Format for Change Control Note).

### 12.3. Applicable Law

12.3.1The 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 MSP, applicable to the Project.

### 12.4. Labour Laws

12.4.1 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.

12.4.2 Wherever necessary, the MSP shall apply for and obtain license as provided under Contract Labour (Regulation and Abolition) Act, 1970, and must 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 MSP.

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

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

12.4.5 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, if the ESI Act does not apply
(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

12.4.6 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 the Purchaser.

12.4.7 The said manpower is not entitled to any claim, right, preference, etc. over any job or 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.

12.4.8 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).

12.4.9 Medical benefits should be provided by the MSP to all the Resources working on the project.

### 12.5. Liquidated Damages

12.5.1 The delivery dates, timetables, milestones and other requirements mentioned in the RFP and this contract are binding on the MSP and the MSP agrees to accomplish the requirement mentioned under this contract as per the Timelines mentioned in the RFP.

12.5.2 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 penalties given in Sr. No 11 and 12.

12.5.3 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.

12.5.4 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.

12.5.5 Liquidated damages are mentioned as a percentage of certain components of cost. Purchaser can take appropriate action including termination of the Contract if –

- Total applicable penalty exceeds 20% of the monthly payment for two consecutive months.
- Applicable Penalty calculations in any month exceeds 30% of the monthly payment.
- If found that Data Centre is compromised or large data is breached due to misconfiguration of security solution, not applied required rules and policies, not created appropriate signatures and deploy at the security solution, wrong rules implemented etc.
- If found large data is breached found at the Dark web and after confirmation that Data is breached during the contract period.
- If found that Data centre services are not available continuously for 24 hours.

### 12.6. Limitation of Liability

12.6.1Notwithstanding anything contained in this RFP, no party will be liable for any incidental or consequential damages arising out of or in connection with this agreement or any breach hereof (including for loss of data or profits, or cost of cover), whether or not such party has been advised of the possibility of such damages, and whether under a theory of Contract, tort (including negligence) or otherwise; except for liabilities arising out of any violation, misappropriation or infringement of a party's intellectual property rights, or from a breach by either party of its obligation. In no event will either party's aggregate liability arising out of or in connection with this agreement or any breach hereof (whether under a theory of Contract, tort (including negligence), warranty or otherwise) exceed the total value of all Work Orders awarded under the Contract between the Purchaser and the MSP.

### 12.7. Indemnity

12.7.1 The MSP agrees to indemnify and hold harmless Purchaser and its officers, employees, and agents against any and all losses, claims, damages, liabilities, costs (including reasonable legal attorney's fees and disbursements) and expenses (collectively, "Losses") to which the Indemnified Party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from—

a. Any misstatement or any breach of any representation or warranty made by the MSP or

b. The failure by the MSP to fulfil any covenant or condition contained in this RFP, including without limitation the breach of any terms and conditions of this RFP by any employee or agent of the MSP. Against all losses or damages arising from claims by third Parties that any deliverable (or the access, use or other rights thereto), created MSP pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property created by MSP pursuant to this Agreement, or the SLAs,

(i) infringes a copyright, trade mark, trade design enforceable in India,

(ii) infringes a patent issued in India, or

(iii) constitutes misappropriation or unlawful disclosure or use of another Party's trade secretes under the laws of India (collectively, "Infringement Claims"); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by

A. Implementation of Project by itself or through other persons other than MSP or

B. its sub-contractors;

C. Third Parties (i.e., other than MSP or sub-contractors) at the direction of Purchaser; or

c. Any compensation or claim or proceeding by any third party against Purchaser arising out of any act, deed, or omission by the MSP or

d. Claim filed by a workman or employee engaged by the MSP for carrying out work related to this Contract. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts enough to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred. Any payment made under this Contract to an indemnity or claim for breach of any provision of this Contract shall include applicable taxes.

e. The Purchaser stand indemnified from any employment claims that the hired resources or MSP's resources may opt to have towards the discharge of their duties in the fulfilment of the Work Orders.

f. Each party also stands indemnified from any compensation arising out of accidental loss of life or injury sustained by such party's resources while discharging their duty towards fulfilment of the Work Orders caused by the negligence or willful misconduct of the other Party or its agents and representatives.

### 12.8. Intellectual Property Rights

12.8.1 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 the Purchaser.

12.8.2 The Purchaser shall acknowledge that:

i. 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").

ii. 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.

iii. 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 or 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.

iv. 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 or 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.

v. 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 or Purchaser for use as detailed in the Clause (c) above.

vi. Except as specifically and to the extent permitted by the MSP, the organisation or 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.

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

viii. 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).

### 12.9. Integrity Pact

12.9.1 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 the Purchaser.

12.9.2 The pact a Contract between the MSP and the Purchaser, committing the persons or Officials of both sides, not to resort to any corrupt practices in any aspect or stage of the Contract. Only those MSPs, who commit themselves to such a pact with the Purchaser, shall be considered competent to participate in the bidding process.

12.9.3 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 Annexure 12: Format for Integrity Pact.

12.9.4 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 execution of Bid security declaration.

### 12.10. Confidentiality

12.10.1 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.

12.10.2 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.

12.10.3 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 Disclosing Party, its affiliates, their respective clients or suppliers, or other persons or entities with whom they do business, that may be obtained by the Receiving Party from any source or that may be developed for the Disclosing Party as a result of the Contract Agreement.

12.10.4 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 or commissioning of Cyber Security Solution at all 4 NDCs..

12.10.5 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 Receiving Party free of any restriction at the time it is obtained from the Disclosing Party,
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 Receiving Party or any third party.
d) is independently developed by the Receiving Party without reference to or use of any Confidential Information of the Disclosing Party; 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 Receiving Party shall advise the Disclosing Party of such required disclosure promptly upon learning thereof in order to afford the Disclosing Party a reasonable opportunity to contest, limit and/or assist the Receiving Party in crafting such disclosure).

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

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

12.10.8 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.

12.10.9 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 Authorized Person needs the Confidential Information for the performance of obligations under the Contract.
   ii. The Authorized 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

12.10.10 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 Purchaser.

12.10.11 The MSP shall treat all the information provided by Purchaser such as IP schema, Purchaser's 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.

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

12.10.13 The Work Order or Contract with the organization may define more stringent confidentiality obligations depending on the nature of information or data being shared. In such event, the more stringent obligations shall prevail.

### 12.11. Events of Default by MSP

12.11.1 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 or MSP's Team has failed to conform with any of the Service or Facility Specifications or 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.

12.11.2 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 Security Deposit.

12.11.3 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.

### 12.12. Dispute Resolution and Arbitration

12.12.1 Amicable settlements: The Parties shall, in good faith, endeavor to settle amicably all disputes arising out of or in connection with this Agreement or interpretation thereof.

**12.12.2 Dispute resolution**

a) Any dispute, difference or controversy of whatever nature howsoever arising under or out of or in relation to this Agreement (including its interpretation) between the Parties, and so notified in writing by either Party to the other Party (the "Dispute") shall, in the first instance, be attempted to be resolved amicably in accordance with the conciliation procedure set forth in paragraph 13.13.

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, shall be finally decided by reference to arbitration in accordance with paragraph 13.13.4 Arbitration as defined in the RFP.

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.

**12.12.3 Conciliation:**

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

**12.12.4 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 conciliation, then the Parties shall refer such dispute for Arbitration. The Arbitration shall be held in accordance with the provisions of the India International Arbitration Centre Act, 2019 and the rules and regulations made thereunder. The venue of the Arbitration shall be Delhi.

b) The Arbitration award shall be final and binding upon the Parties. Each Party shall bear the cost of preparing and presenting its case, and the cost of Arbitration, including fees and expenses of the Arbitrator, and administrative charges 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.

**12.13. Termination of Contract**

12.13.1 The 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:

**12.13.2 Termination Process:**

Upon occurrence of an event of default as set out in above clauses, the Purchaser will 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.

**12.13.3 Termination for insolvency, dissolution, bribery:**

(a) The Contract may be terminated by the Purchaser and the deposits or guarantees in possession of the Purchaser (Security Deposit and the 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 or 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 and/or the Security Deposit in possession of the Purchaser and the remaining amount may be paid to the liquidator/MSP, as applicable.

**12.13.4 Termination for default or breach:**

The Purchaser may without prejudice to any other remedy for breach of Contract, (including forfeiture of security deposit, 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, the 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:

(i) If the MSP fails to accept the Work Order(s);

(ii) The MSP or MSP's Team has failed to conform with any of the Service or Facility Specifications or 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;

(iii) The MSP goes into liquidation, voluntarily or otherwise;

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

(v) If the MSP fails to deliver services within the time period specified in the Work Orders granted by the Purchaser; and

(vi) If the MSP fails to meet any other terms and conditions under the Contract.

**12.13.5 Termination for convenience:**

The 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, at its convenience. The notice of termination shall specify that the termination is for the 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 shall become effective. The Purchaser reserves the right to cancel the remaining part of the Work Order and/or the Contract, as the case may be, and pay to the MSP an agreed amount for partially completed services.

**12.13.6 Termination for violation of law or 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 or 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 termination shall be made to the MSP in the event of termination.

**12.13.7 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 or breach, and further allow the next successor MSP to take over the obligations of the erstwhile MSP in relation to the execution or continued execution of the scope of the Contract.

(b) Nothing herein shall restrict the right of the Purchaser to invoke the MSP's PBG and/or Security Deposit, enforce the indemnity as defined under Section 13.8, 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.

### 12.14. Exit Management

12.14.1 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.

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

12.14.3 Given the critical nature of the project, it is imperative that a well-defined exit management strategy be made ready which shall enable easy transition of activities when the Contract expires or is truncated.

12.14.4 Accordingly, the MSP shall submit an exit management plan finalized with the Purchaser post signing of the Contract focusing 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.

12.14.5 The MSP shall understand that ensuring a smooth transition at the end of the project period is a key requirement from the 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.

12.14.6 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 transition is made to the other agency as per the agreed exit management plan. In case Purchaser wants to take over the project itself, then MSP has to ensure proper transition to the team designated by Purchaser.

12.14.7 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.

12.14.8 The MSP shall provide all knowledge transfer of the system to the Purchaser as per the agreed exit management plan.

12.14.9 The MSP shall transfer the ownership of all the deployed IT assets to the Purchaser. This includes all hardware, software, licenses, documentation, and any other materials specified in the RFP.

12.14.10 The exit management period starts:

i. In case of expiry of Contract, at least 6 Months prior to the date when the Contract comes to an end, or

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

12.14.11 The exit management period ends on the date agreed upon by the Purchaser or 6 Months after the beginning of the exit management period, whichever is earlier. In case of termination 6 Months exit period applies there also until Purchaser decides otherwise.

### 12.15. Force Majeure

12.15.1 For the purposes of this Agreement, "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.

12.15.2 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 this Agreement and to have avoided or overcome in the carrying out of its obligations hereunder, through exercise of reasonable skill and care.

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

12.15.4 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 given by such Party, seeking concession, to the other, as soon as practicable, but within 21 calendar 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, provided that 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.

### 12.16. Adherence to safety procedures, rules, regulations and restriction

12.16.1 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 or policy.

12.16.2 The MSP 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.

12.16.3 MSP shall also adhere to all security requirement or regulations of the Purchaser during the execution of the Contract.

12.16.4 Access to Purchaser's Data Centre should be strictly restricted in the following manner:

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

ii. No access to any employee of the MSP, except the essential staff who has genuine work-related need, should be given. All such access should be logged in a loss-free manner for permanent record with unique biometric identification of the employee to avoid misrepresentations or mistakes.

### 12.17. Information security

12.17.1 The MSP shall not carry and/or transmit any material, information, layouts, diagrams, storage media or any other goods or material in physical or electronic form, which are proprietary to or owned by the Purchaser, out of data centres and extended location premises without prior written permission from the Purchaser.

12.17.2 MSP acknowledges that Purchaser proprietary information or materials, whether developed by the 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 the Purchaser; and MSP agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized 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 goodwill of the Purchaser depends, among other things, upon MSP keeping such proprietary information confidential and that unauthorized 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.

12.17.3 Any proprietary tools of the MSP, if any used for the project and MSPs Pre-existing IPR will remain with the MSP.

12.17.4 The authorized signatory of the MSP shall sign an NDA with reference to this tender under the provisions of the “The Official Secrets Act, 1923” within 7 days and submit the same along with the acceptance of the Award of the Contract.

12.17.5 All the deployed resources shall sign the NDA with reference to this tender under the provisions of the “The Official Secrets Act, 1923” within 7 days after confirmation of acceptance of the resource by Purchaser.

### 12.18. Publicity

12.18.1 MSP shall not publicize any information pertaining to this assignment or the other party without seeking the prior written consent of the Purchaser.

### 12.19. Conflict of Interest

12.19.1 The MSP shall disclose to the Purchaser in writing, all actual and potential unethical 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.

### 12.20. Severance

12.20.1 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 shall remain in full force and effect.

### 12.21. Continuance of the Contract

12.21.1 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.

### 12.22. Adherence to IT Laws and Government Regulations

12.22.1 The solution 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, NICSI 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.

### 12.23. Sub-contracting

12.23.1 Sub-contracting or outsourcing would be allowed only for works such as :

i. Passive Networking and Civil Work during implementation

ii. Facilities Management System (FMS) staff.

12.23.2 In this regard, MSP shall take prior approval from the Purchaser for sub-contracting any work, as given in paragraph 12.23.

12.23.3 Such sub-contracting shall not relieve the MSP from any liability of the Contract in any manner. The MSP shall be solely responsible for the work activities carried out by subcontracting under the Contract.

### 12.24. Restriction under rule 144 (xi) of the GFR 2017 (Land Border)

12.24.1 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 14.4.1 of the bid. Declaration by the Bidder on their letter head that the Bidder has proposed no such Solution in response to the bid. Please refer to the Govt. notifications provided at https://doe.gov.in/procurement-policy-divisions for details and updates [under Rule 144 (xi) of the General Financial Rules 2017]. The bidder shall submit a certificate in the prescribed format as per Annexure11: Format for Restriction under Rule 144(xi) of the GFR to this effect.

### 12.25. Compliance to Digital Personal Data Protection Act, 2023

12.25.1 MSP shall ensure all the personal data in the MSP supplied components and platforms are 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 tokenized form, or obfuscated or masked; and the access privileges to the back-end data segment are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication.

### 12.26. Official Secrets Act

12.26.1 The MSP 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 MSP 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 MSP 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.

### 12.27. Transfer of Project documentation, data and solutions

12.27.1 Before the expiry of the exit management period, the MSP shall deliver all the relevant and up-to-date records and reports pertaining to the Project and its design, implementation, operation and maintenance, including all operation and maintenance records and manuals pertaining thereto.

12.27.2 The MSP shall provide the Purchaser with complete and up-to-date list of the documents, data and relevant system details to be transferred to the Purchaser's appointed agency, within 30 days of the start of the Exit Management period.

12.27.3 The MSP shall pass on to the Purchaser, subsisting rights in any licensed products on terms not less favorable to the Purchaser than those enjoyed by the MSP.

12.27.4 Even during the Exit Management period, the MSP shall continue to perform all their obligations and responsibilities as stipulated under this Contract, and as may be proper and necessary to execute the scope of work as given in paragraph 5 of the RFP, to execute an effective transition and to maintain business continuity.

12.27.5 At the time expiry of contract or exit from the contract, all solutions provided by the MSP under the scope of the RFP should be interoperable during the transfer or handover at the time of exit or Contract termination. MSP shall handover all cyber security hardware, software, If MSP has developed any portals/ applications/ tools/ solution/ integration/ automation during the contract period to meet the SLA must be transfer to purchaser even if it is not involved in RFP BoQ. No proprietary service is to be used or implemented by the MSP. Any customization, or tools or effort required for smooth transfer of documentation and data necessary for interoperability shall be the responsibility of the MSP. MSP shall also handover exiting manpower to new agency or NIC if required during the Exit the contract

12.27.6 All solutions provided by the MSP under the scope of the RFP should be interoperable during the transfer or handover at the time of exit or Contract termination. No proprietary service is to be used or implemented by the MSP. Any customisation, or tools or effort required for smooth transfer of documentation and data necessary for interoperability shall be the responsibility of the MSP.

12.27.7 All equipment and solutions utilized to deliver the project scope should have valid service Contract and should not be end-of-life or end-of-support during the Contract period.

12.27.8 The MSP shall share the details of all existing service contracts and agreements executed with its current vendors, sub-contractors and service providers to the Purchaser on Yearly basis under an NDA with the Purchaser.

### 12.28. Statutory Requirements

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

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

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

### 12.29. Completion Certificate and Final payment

#### 12.29.1 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 or 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.

#### 12.29.2 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.

#### 12.29.3 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.

#### 12.29.4 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.

#### 12.29.5 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.

**12.29.6 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 or 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 or 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.

**12.29.7 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 or 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.

**12.29.8 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 or member so dying. Nothing in this clause shall be deemed to prejudice or effect the respective rights or obligations of the MSP partners or members and the legal representatives of any deceased MSP partners or members.

**12.29.9 Defects Liability Period**

(a) The MSP warrants that the Services have been delivered as per description, scope or 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 or outcomes attributable to a shortfall in scope or 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 perform the Services or parts thereof, free of cost, at the site.

(d) If the MSP, having been notified, fails to rectify or 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.

## Annexure Documents

## 1. Annexure : Manufacturer's Authorization Format (MAF)

Date: ___________________ RFP No.: _____________________

To,
Tender Division,
National Informatics Centre,
A Block, CGO Complex, Lodhi Road,
New Delhi – 110003

Subject: Manufacturer Authorization for Tender No:

Sir,

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.

We <OEM Name> authorise <Bidder's name> to quote our product for above specified tender as our Authorised Indian Agent.

We confirm that we have understood the installation and configuration 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 7 years from date of completion of installation and commissioning of the equipment/software delivered as per the contract. In case of any difficulties in logging complaint at Bidder end, user shall have option to log complaint at our call support centre.

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. 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.

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.

We understand that any false information/commitment provided here may result in <OEM's Name> getting debarred from doing business with National Informatics Centre .

Thanking You

For <OEM/ Manufacturer name>

<(Authorized Signatory)>

Name of the Authorized Signatory:
Designation:
E-mail ID:
Phone No (Office) :

Signature:
Seal of the Company

Note:
The letter shall be submitted on the letter head of the manufacturer / OEM and shall be signed by the authorised signatory

## 2. Annexure: Bidder’s Blacklisting

Date: ___________________ RFP No.: _____________________

To,
Tender Division,
National Informatics Centre,
A Block, CGO Complex, Lodhi Road,
New Delhi – 110003

Subject: Declaration for bidder’s blacklisting for participation in the RFP titled “ ” and RFP No. .

Sir,

We, <MSP>having our registered office at <MSP address>, are an established authorized partner cum MSP since last <No. of years> and have our registered office at < address of registered office >.

We do here by confirm, that we have read and understood each and every tender terms and conditions of above cited tender and are bidding in complete compliance of all terms and conditions of tender. We understand that it will be our sole responsibility to deliver the product and services as per conditions set out in tender. Any failure at our end will make us liable for penalties as defined in tender and cancelation of empanelment.

We do hereby also confirm that our company has:

i. Not stand declared ineligible/ blacklisted/ banned/ debarred by the Procuring Organisation or its Ministry/ Department from participation in its Tender Processes; and/ or

ii. Not be 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 involving moral turpitude in business dealings under the Prevention of Corruption Act, 1988 or any other law; and/or
- offences under the Indian Penal Code or any other law for causing any loss of life/ limbs/ property or endangering Public Health during the execution of a public procurement contract and/ or
- suspected to be or of doubtful loyalty to the Country or a National Security risk as determined by appropriate agencies of the Government of India.

iii. Not have changed its name or created a new business entity as covered by the definition of “Allied Firm”, consequent to having been declared ineligible/ suspended/ blacklisted/ banned/ debarred as above;

Thanking You
For <MSP>
< (Authorized Signatory)>
Name:
Designation:
Contact Details:
Seal of the Company

## 3. Annexure: Bidder Profile

Date: ____________________ RFP No.: ______________________

| Sl. No. | Area of the details to be provided | | Responding Firm’s/Company Details to be provided |
|---|---|---|---|
| 1 | Name of the Bidder | | |
| 2 | Address of the Bidder | | |
| 3 | Telephone number of the Firm/company | | |
| 4 | Bid number and date | | |
| 5 | Name of the contact person to whom all references shall be made regarding this RFP | | |
| 6 | Designation of the person to whom all references shall be made regarding this tender | | |
| 7 | Address of the person to whom all references shall be made regarding this tender | | |
| 8 | E-mail address of the Firm/company | | |
| 9 | Fax number of the Firm/company | | |
| 10 | Website address of the Firm/company | | |
| 11 | Details of Registration | 1. Registration Number of the Firm/company.<br>2. Name of the place where the firm/company was registered.<br>3. Date when the company was registered.<br>4.Product /Service for which registered<br>5. Validity Period, if applicable. | |
| 12 | Central Service Tax No. | | |
| 13 | VAT/Service Tax No. | | |
| 14 | PAN No. | | |
| 15 | Annual Turnover during last three financial Years last three years.<br>Positive net worth as on 31st March 2022 | | |

| Sl. No. | Area of the details to be provided | Responding Firm's/Company Details to be provided |
|---|---|---|
| 16 | Income Tax Paid during the last three financial Years | |
| 17 | Details of ownership of the firm (Name and Address of the Board of Directors, Partners, etc.) | |
| 18 | Name of the authorized Signatory who is authorized to quote in the tender and enter into the rate Contract (Power of Attorney to be submitted) | |
| 19 | Name of the Bankers along with the branch (as appearing in MICR cheque) and Account # | |
| 20 | Status of Firm/company like Pvt. Ltd. etc. | |

Witness:

Signature -----------------------

Name -----------------------

Address -----------------------

Date ---------------------------

Bidder: -------------------------------

Signature: ----------------------------

Name: --------------------------------

Designation: -------------------------

Company Seal: ---------------------

Date: ----------------------------------

## 4. Annexure: Format for Restriction under Rule 144(xi) of the GFR

Date: ____________________ RFP No.: ______________________

To,
Tender Division,
National Informatics Centre,
A Block, CGO Complex, Lodhi Road,
New Delhi – 110003

Subject: Restriction under Rule 144(xi) of the GFR declaration for participation in the RFP titled " " and RFP No. .

Sir,

I <Authorized Signatory> have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India.

I certify that the bidder <Bidder Name> is not from such a country and does not have any specified transfer of technology (ToT) from such a country or, if from such a country or if having specified ToT from such a country has been registered with the Competent Authority (i.e., Registration Committee constituted by Department for Promotion of Industry and Internal Trade (DPIIT)).

I hereby certify that this bidder fulfils all the requirements in this regard and is eligible to be considered for the participation in this RFP. [where applicable, evidence of valid registration by the Competent Authority shall be attached along with this Annexure]

Thanking you,

For <Bidder Name>
< (Authorized Signatory)>
Name:
Designation:
Contact Details:

Seal of the Company

## 5. Annexure: Site Not Ready Declaration

Date: ____________________ RFP No.: ______________________

| Site Not Ready Certificate | | |
|---|---|---|
| 1 | MSP Name | |
| 2 | Purchase order No. and date | |
| 3 | Location Name | |
| 4 | Equipment Name | |
| 5 | Date of delivery | |
| 6 | Date of 1st Visit for installation | |
| 7 | Site not ready reason | |
| 8 | Tentative date of site being ready for installation | |

Name of NIC Site in charge: ……………………………………………….

Designation: ……………………………………………………………………

Signature (with official seal): ……………………………………………………………

## 6. Annexure: A Hardware Unpriced BOQ

| Sr. No | Item Description | Unit of Measurement | Initial Procurement Qty | Maximum qty to be ordered |
|---|---|---|---|---|
| 1. | Type 1 POD Firewall | Per Firewall appliance | 28 | 36 |
| 2. | Type 2 POD Firewall | Per Firewall appliance | 12 | 16 |
| 3. | Type 3 Perimeter Firewall | Per Firewall appliance | 10 | 14 |
| 4. | DDoS | Per DDoS appliance | 8 | 10 |
| 5. | WAF | Per WAF appliance | 34 | 44 |
| 6. | NDR | Per NDR | 25 | 25 |
| 7. | Type-1 IPS | Per IPS appliance | 4 | 6 |
| 8. | Type-2 IPS | Per IPS appliance | 8 | 10 |
| 9. | Type-3 IPS | Per IPS appliance | 10 | 14 |
| 10. | Anti APT | Per APT appliance | 16 | 22 |
| 11. | Type 1 SSL Off loader | Per SSL Offloaded appliance | 2 | 4 |
| 12. | Type 2 SSL Off loader | Per SSL off loader appliance | 12 | 16 |
|  | Grand Total |  | 169 | 217 |

Next procurement will be initiated only when:

- All the items/solution ordered in initial procurement has been successfully delivered, installed and operationalized.
- Satisfactory services provided by the MSP

Note:

- The delivery location of the Cyber Security Solution infrastructure shall be provided in the Work order.
- The purchaser will order in phase wise as quantity specified in the table above in one or multiple work orders

## 7. Annexure: B Software Unpriced BOQ

| Sr. No | Item Description | Unit of Measure | Initial Procurement (Quantity) | Maximum (Quantity) to be ordered |
|---|---|---|---|---|
| 1. | Privileged Identity and Access Management (PIM/PAM) | User | 2500 | 5000 |
| 2. | Server Security | Per IP/VM/Server | 30000 | 45,000 |
| 3. | Patch Management | Virtual Machines/ Physical Server/ Appliance | 30000 | 45,000 |
| 4. | Host based Data Leak Prevention System | Asset | 100 | 100 |
| 5. | Web Application Firewall (2 Gbps) | Instance | 50 | 150 |
| 6. | Database Activity Monitoring | per DB instances | 100 | 100 |
| 7. | AAA | Virtual Appliances | 2 | 4 |
| 8. | Vulnerability Assessment (VA) | Per IP | 30000 | 45000 |

**Note :**

1. The purchaser may procure the license **(Quantity)** of the cyber security solutions as specified in the table above in one or multiple work orders under the contract.
2. MSP has to provide underlying hardware to run these software along with these software

## 8. Annexure: C Manpower Requirement

| Sr. No | Designation / Role | Quantity | Experience (in years) |
|---|---|---|---|
| 1 | Lead Security Administrator | 3 | 8 |
| 2 | Senior Security Administrator | 6 | 5 |
| 3 | Security Administrator | 23 | 3 |
| 4 | Security Operator | 25 | 1 |
| 5 | Project Manager | 1 | 10 |
| **Grand Total** | | **58** | |

## 9. Annexure: Format for Gross Total Value

Prices should be quoted in Indian Rupees and indicated both in figures and words. Price in words will prevail, in the event of any mismatch.

| | |
|---|---|
| **Grand Total Value (GTV) (i.e., Total Charge)** | **Rs.** |
| **(Rupees________________________________________________________) in words** | |

**Note:** Please ensure that the Grand Total Value (GTV) must match the Total (Table C1+ Table C2 +Table C3) of detailed financial bid value given in **Annexure: Detailed Financial Bid.**

Signature ……………………………………

Name of the Authorized Signatory

…………………………………….............

Seal of Company ………………………….

Dated………………………………………….

# 10. Annexure : Detailed Financial Bid

## 10.1. Financial Bid GTV

| Sr No. | Component | Amount (including Tax/ GST) |
|---|---|---|
| 1. | Table 1: Cost Cyber Security Hardware | Total Cost C1 as per Table 1 |
| 2. | Table 2: Cost of Manpower | Total Cost C2 as per Table 2 |
| 3. | Table 3 Cost of Cyber Security Software Solutions (subscription and support cost) | Total Cost C3 as per Table 3 |
| | **Grand Total Value** | |

**Grand Total Value (GTV) = Total Cost C1 + Total Cost C2 + Total Cost C3**

**Grand Total Value (GTV) (in words) = ______________________________________________** (All values are inclusive of taxes/GST)

## 10.2. Table 1: Cost Cyber Security Hardware

| Sr. No | Item Description | OEM | Make/Model No. with details of sub assembly /components | Unit of Measure | Qty | Unit cost with 1 year warranty (incl. of GST) | Unit AMC cost for 2nd Year (incl. GST) | Unit AMC cost for 3rd year (incl. GST) | Per unit cost with 3-year support / warranty | Total Cost | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | A | B | C | D | E=(B+C+D) | F=A*E | |
| 1. | Type 1 POD Firewall (30 Gbps) | | | Per Firewall appliance | 36 | | | | | | |
| 2. | Type 2  POD Firewall (100 –Gbps) | | | Per Firewall appliance | 16 | | | | | | |
| 3. | Type 3 Perimeter Firewall (150–Gbps | | | Per Firewall appliance | 14 | | | | | | |
| 4. | DDOS (150Gbps) clean traffic | | | Per DDoS appliance | 10 | | | | | | |
| 5. | WAF (90 Gbps) | | | Per WAF appliance | 44 | | | | | | |
| 6. | NDR(30 Gbps) | | | Per NDR appliance | 25 | | | | | | |
| 7. | IPS Type-1 (20 Gbps) | | | Per IPS appliance | 6 | | | | | | |
| 8. | IPS Type-2 (40 Gbps) | | | Per IPS appliance | 10 | | | | | | |
| 9. | IPS Type-3 (100 Gbps) | | | Per IPS appliance | 14 | | | | | | |

| Sr. No | Item Description | OEM | Make/Model No. with details of sub assembly /components | Unit of Measure | Qty | Unit cost with 1 year warranty (incl. of GST) | Unit AMC cost for 2nd Year (incl. GST) | Unit AMC cost for 3rd year (incl. GST) | Per unit cost with 3-year support / warranty | Total Cost | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | A | B | C | D | E=(B+C+D) | F=A*E | |
| 10. | Anti-APT (20 Gbps) | | | Per APT appliance | 22 | | | | | | |
| 11. | Type 1 SSL off loader (40 Gbps) | | | Per SSL off loader appliance | 4 | | | | | | |
| 12. | Type 2 SSL off loader (90 Gbps) | | | Per SSL off loader appliance | 16 | | | | | | |
| **Grand Total (C1)** | | | | | | | | | | | |

**Note:**

1. The Total Cost arrived column F is inclusive of Installation, Configuration, testing, commissioning and operationalized of cyber security solution and. In case any additional order is placed on the MSP, the MSP shall Installation, Configuration, testing, commissioning and operationalized the additional procured solution within the existing rates.
2. The Unit cost at column B above shall be the unit price with one-year warranty, exclusive of GST, price of packaging, forwarding, freight, insurance charges, Installation, Configuration, testing, commissioning and operationalized or any other logistic cost till Project Start.
3. **The AMC cost quoted for 2nd year and 3rd year should not be less than 12 % of the unit cost at column (B)** .
4. In case of the contract is extended beyond three years then AMC rate will be 3rd year AMC cost quoted by Bidder.
5. The warranty will be start from the date of Final acceptance date.
6. The 2nd year AMC shall commence from the expiry of warranty.

7. The Purchaser reserves the right to order any of the items in the Table 1 for installing at NDC Delhi, Pune, Hyderabad, Bhubaneshwar and Guwahati.
8. If AMC period is less than 1year then AMC amount will be paid on the basis of pro rata basis.

### 10.3. Table 2: Cost of Manpower

| Sr. No | Item Description | QTY(Minimum)* | Ist Year man month Rate (excl. GST | 2nd Year man month Rate Cost (excl. GST) | 3rd Year man month Rate (excl. GST) | Total manpower Cost for 3 years (excl. GST) | GST (in %) | Total Cost (incl. GST) |
|---|---|---|---|---|---|---|---|---|
| | | **(Q)** | **(A)** | **(B)** | **( C)** | **D=Q*(A+B+C)*12** | **(G)** | **E=D*(1+G%)** |
| 1. | Lead Security Administrator | 3 | | | | | | |
| 2. | Senior Security Administrator | 6 | | | | | | |
| 3. | Security Administrator | 23 | | | | | | |
| 4. | Security Operator | 25 | | | | | | |
| 5. | Project Manager | 1 | | | | | | |
| **Total** | | **58** | | | | | | |
| **Grand Total (C2)** | | | | | | | | |

** These are the minimum resources envisaged by purchaser. However, bidder can quote more resources to meet SLA requirements

## 10.4. Table 3 : Cost of Cyber Security Software Solutions (subscription and support cost)

| Sr. No | Item Description | Unit of Measure | Qty | Make. Name of Solution with details of sub assembly /components | 1st Year unit cost (excl. of GST) | 2nd Year unit cost (excl. of GST) | 3rd Year unit cost (excl. of GST) | Total unit Cost (excl. of GST) | Total Cost (exc. of GST) | GST (in %) | Total cost |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | A | B | C | D=A=B+C | E=D*Qty | F | G=E(1+F%) |
| 1. | Privileged Identity and Access Management /Per user PIM/PAM | User | 5000 | | | | | | | | |
| 2. | Server Security | Per IP | 45000 | | | | | | | | |
| 3. | Patch Management | Virtual Machines/Physical Server/Appliance | 45000 | | | | | | | | |
| 4. | Host based Data Leak Prevention System | Asset | 100 | | | | | | | | |
| 5. | Virtual Web Application Firewall (2 Gbps) | Instance | 150 | | | | | | | | |
| 6. | Database Activity Monitoring | per DB instances | 100 | | | | | | | | |
| 7. | AAA | Virtual Appliances | 4 | | | | | | | | |
| 8. | Vulnerability Assessment | Per IP | 45000 | | | | | | | | |
| | **Grand Total (C3)** | | | | | | | | | | |

## 11. Annexure : Manpower/resource categories, skillset, qualifications and requirements

**Manpower deployment details:**

The bidder shall propose the year wise manpower deployment in the format provided below:

| Sr. No | Designation | Total resources | Location | | | |
|---|---|---|---|---|---|---|
| | | | Delhi | Hyderabad | Pune | BBSR |
| 1. | Lead Security Administrator | 3 | 3 | - | - | - |
| 2. | Senior Security Administrator | 6 | 6 | - | - | - |
| 3. | Security Administrator | 23 | 20 | 1 | 1 | 1 |
| 4. | Security Operator | 25 | 10 | 5 | 5 | 5 |
| 5. | Project Manager | 1 | 1 | - | - | - |
| **Total** | | **58** | **40** | **6** | **6** | **6** |

**Note:**

1. The number of resources proposed by the MSP for each designation shall not be reduced during the entire Contract Period.
2. When subsequent orders for additional hardware are placed by the Purchaser during the Contract Period, the MSP shall deploy the additional manpower required for ensuring uninterrupted 24×7 operations of the overall project. Such additional manpower shall be provided by the MSP within the quoted cost.
3. If, at any stage during the Contract Period, the Purchaser observes that the number of onsite resources is inadequate and is adversely affecting the operation and maintenance of the project, the Purchaser may direct the MSP to deploy additional resources. The MSP shall comply with such directions without claiming any additional payment.
4. For the position of Project Manager, the MSP shall provide the name and details of the proposed resource in the prescribed format. The proposed Project Manager shall remain assigned to the project until the commissioning and acceptance of the complete solution. Any change in this position prior to that stage shall require prior written approval from the Purchaser.

## 12. Annexure: Technical Specifications of Hardware

### 12.1. Type 1 Firewall (30 Gbps)

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **General Requirements:** | | |
| 2. | Make:<br>Model No: | | |
| 3. | **Licensing** | | |
| 4. | The proposed solution should be per device license for unlimited users for Firewall and other features. The Licences should include<br>1. NGFW (Application Visibility & Control)<br>2. Next Generation Threat Prevention (Application Visibility & Control, IPS, Encrypted traffic inspection Anti-Virus/Anti-Malware, Anti-Bot, Basic File Blocking, URL filtering, web security & Threat Intelligence)<br>All the licences must be provided from day-1. | | |
| 5. | **Central Management** | | |
| 6. | 1. The proposed solution should be provided with a separate / dedicated appliance in HA for Firewall Management and Log Analysis with all the required licenses for managing the all firewall physical as well as Virtual, monitoring, reporting etc.<br>2. The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3. The proposed management solution must have the capability to manage minimum 100 physical firewall and 200 virtual system firewalls and adequate licenses for managing these Firewalls must be supplied from Day 1.<br>4. The solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>5. The proposed solution should have access through GUI and user management must be based on RBAC.<br>6. The proposed solution must have integrated security architecture with multi-tenancy, analytics, Logging and must have API access for enhanced automation capabilities. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 7. The proposed solution must provide firewall administration control by segmenting management into multiple virtual domains if required.<br>8. The proposed solution must allow single policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, and scheduling at single place and single locations<br>9. The proposed solution should have separate real time logging base for all traffic that includes Threats, User IDs, URL filtering, Data filtering, content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities.<br>10. The proposed solution should have Inter-cluster communication between firewalls configured in high availability and communication with central management should be secure and encrypted.<br>11. Proposed solution must to allow export and forwarding of logs in well-known SIEM formats including Syslog<br>12. The proposed solution should support API for automation. | | |
| 7. | **Performance Parameter:-** | | |
| 8. | 1. The proposed solution should provide minimum 30 Gbps NGFW real world throughput (Application Visibility & Control, with Logging enabled)<br>2. The proposed solution should provide minimum 20 Gbps NGTP real world throughput (Application Visibility & Control, IPS, Anti-Virus/Anti-Malware, Anti-Bot, Basic File Blocking, , web security & Threat Intelligence with Logging enabled)<br>3. Proposed solution must support URL filtering.<br>4. The proposed solution should provide minimum 500K new connections/sec on Layer-4 or 250K new session or connection/sec on Layer-7.<br>5. The proposed solution should provide minimum 15M concurrent connections on Layer-4 or<br>2M concurrent connection on Layer-7.<br>1. Interface Requirement<br>The proposed solution should have:<br>i. Minimum 1x1G management port | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | ii. Minimum 8x10G SFP+ Port and 4X25G/40G/100G SFP28 Ports<br>.<br>MSP has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| 9. | The proposed solution  should support IEEE 802.1q VLAN Tagging with minimum of 1024 VLANs supported (in NAT/Route mode) | | |
| 10. | The proposed solution should support virtualization (i.e. Virtual Systems / Virtual Domains/Virtual Instances) with minimum 10 instances per device provisioned from day 1. The virtual system should have all the features as of physical device. | | |
| 11. | The proposed solution should have dual and  hot swappable power supply modules along with redundant fan tray modules | | |
| 12. | **Network/Routing Requirements ( For both IPv4 and IPv6)** | | |
| 13. | The proposed solution must support static routing | | |
| 14. | The proposed solution must support policy based routing | | |
| 15. | The proposed solution must support dynamic routing (RIP, OSPF,BGP) | | |
| 16. | The proposed solution must support multicast routing. | | |
| 17. | The proposed solution must support dual stack IPv4 and IPv6. | | |
| 18. | The proposed solution must support DNS64 & DHCPv6 from day-1 | | |
| 19. | **Firewall Features Requirement:** | | |
| 20. | The proposed solution should be ICSA Labs certified or EAL 4 or higher certified. | | |
| 21. | The Proposed solution must support below deployment modes<br>1. Bridge<br>2. Transparent<br>3. NAT | | |
| 22. | The proposed solution must support creating access rule with IPv4 and IPv6 objects simultaneously. | | |
| 23. | The proposed solution should support in-built multiple security groups/profile and the same security groups/Profile can be used globally for all virtual domains/instances/contexts. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 24. | The proposed solution must be capable of sending logs in syslog format and its raw log format should be supported by all leading SIEM solutions. | | |
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface. | | |
| 26. | The proposed solution should have management plane separated from the data plane, with capability to allocate each plane having dedicated resources like CPUs cores, interface and RAM modules to handle the processing functions. Support for segmentation via virtual firewalls/contexts/tenants, with per-tenant policy and logs | | |
| **27.** | **NAT Requirements** | | |
| 28. | The proposed solution must provide NAT functionality, including PAT. | | |
| 29. | The Proposed solution must support NAT 44, NAT 64, and NAT 66, NAT46 from Day 1 and must support at least 5,000 NAT from Day 1. | | |
| 30. | The proposed solution should also support IPv4 to IPv6,IPv6 to IPv4,IPv6 to IPv6,IPv4 to IPv4 communication | | |
| 31. | The proposed solution should support “Policy-based NAT”. | | |
| 32. | The proposed solution should provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP. | | |
| 33. | The proposed solution must have capability to log traffic bidirectional with bytes in/out information. | | |
| 34. | The proposed solution should support NAT within IPSec/SSL VPN tunnels | | |
| 35. | **Authentication Requirements:** | | |
| 36. | The proposed solution must support for authentication for users and Firewall Administrators LDAP/ RADIUS/ TACACS*/ AAA/ AD for authentication and management of the device. | | |
| 37. | The proposed solution must support for multi factor authentication. | | |
| 38. | The proposed solution should support PKI / Digital Certificate based two-factor authentication for both Users and Firewall Administrators. | | |
| 39. | The solution should identify the device address/host name. | | |
| 40. | **High Availability Requirements:** | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 41. | The proposed solution must support Active-Active as well as Active-Passive redundancy in IPv4 and IPv6. | | |
| 42. | The proposed solution must support State full failover for both Firewall and VPN sessions. | | |
| 43. | The proposed solution must support :<br>If any appliance in the cluster malfunctions, hangs, or loses network connectivity due to hardware or software issues, the appliance cluster (either active-active or active-passive) must be able to automatically switch-over to the healthy appliance without any manual intervention. | | |
| 44. | The Proposed solution should support VRRP or equivalent and Link Failure Control. | | |
| 45. | **Encryption / VPN Requirements** | | |
| 46. | The VPN functionalities should be integrated within firewall for both IPsec and SSL-TLS in IPv4 and IPv6 ie in dual stack. It should support the following protocols but not limited to DES and 3DES, MD5, SHA-1 and the more secure SHA-256 authentication, Diffie-Hellman Group 1, Group 2, Group 5 and the more secure Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm. The new encryption standard AES 128, and 256 (Advanced Encryption Standard), IPSec VPN should support multi factor authentication. | | |
| 47. | The proposed solution must be able to create IPSec tunnelling and Site to Site VPN tunnelling. | | |
| 48. | The proposed solution must support Deep SSL Inspection on latest SSL protocols versions including TLS1.3. It shall support the deep packet inspection of different SSL / TLS based Web /any other applications simultaneously. | | |
| 49. | The proposed solution should support packet capture/sniffer to examine the contents of individual data packets that traverse through the firewall appliance for troubleshooting, diagnostics and general network activity. | | |
| 50. | The proposed solution should have integrated traffic shaping / QoS functionality. | | |
| 51. | The proposed solution should be able to support blacklist and whitelist based on Geo-IP including selection based on country name. | | |
| 52. | The proposed solution shall have capability to analyse and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP etc. | | |
| 53. | The proposed solution should maintain the audit trail for the management activities of individual users and administrators accessing and using the deployed solution. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 54. | The proposed solution should provide capability to understand unused security capabilities and turn them on with best practices, to understand gaps in configuration best practices, recommendations to close security gaps, detect hardware and software system issues. | | |
| 55. | The proposed solution should provide for Role-Based Access Control (RBAC) and provide access based on the least privilege criteria on the NGFW devices. | | |
| 56. | The proposed solution should comply with FIPS-140-2 standard for cryptographic modules as well as USGv6/IPv6. | | |
| 57. | The proposed solution should have protection for at least 15000, IPS signatures. | | |
| 58. | The proposed solution should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use. | | |
| 59. | **DNS Security** | | |
| 60. | The proposed solution should be enabled with the enterprise protection DNS Security capabilities within the same appliances from day 1 along with OEM threat intelligence feed. | | |
| 61. | The proposed solution should support DNS security in line mode or proxy mode | | |
| 62. | Proposed solution DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence. | | |
| 63. | The proposed solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection. | | |
| 64. | The proposed solution should support capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers. | | |

### 12.2. Type 2 Firewall (100 Gbps)

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **General Requirements:** | | |
| 2. | Make:<br>Model No: | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 3. | **Licensing** | | |
| 4. | The proposed solution should be per device license for unlimited users for Firewall and other features. The Licences should include<br>1. NGFW (Application Visibility & Control)<br>2. Next Generation Threat Prevention (Application Visibility & Control, IPS, Encrypted traffic inspection Anti-Virus/Anti-Malware, Anti-Bot, Basic File Blocking, URL filtering, web security & Threat Intelligence)<br>All the licences must be provided from day-1. | | |
| 5. | **Central Management** | | |
| 6. | 1. The proposed solution should be provided with a separate / dedicated appliance in HA for Firewall Management and Log Analysis with all the required licenses for managing the all firewall physical as well as Virtual, monitoring, reporting etc.<br>2. The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3. The proposed management solution must have the capability to manage minimum 100 physical firewall and 200 virtual system firewalls and adequate licenses for managing these Firewalls must be supplied from Day 1.<br>4. The solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>5. The proposed solution should have access through GUI and user management must be based on RBAC.<br>6. The proposed solution must have integrated security architecture with multi-tenancy, analytics, Logging and must have API access for enhanced automation capabilities.<br>7. The proposed solution must provide firewall administration control by segmenting management into multiple virtual domains if required.<br>8. The proposed solution must allow single policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, and scheduling at single place and single locations | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 9. The proposed solution should have separate real time logging base for all traffic that includes Threats, User IDs, URL filtering, Data filtering, content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities.<br>10. The proposed solution should have Inter-cluster communication between firewalls configured in high availability and communication with central management should be secure and encrypted.<br>11. Proposed solution must allow export and forwarding of logs in well-known SIEM formats including Syslog<br>12. The proposed solution should support API for automation. | | |
| 7. | **Performance Parameter:-** | | |
| 8. | 1. The proposed solution should provide minimum 100 Gbps NGFW real world throughput (Application Visibility & Control, with Logging enabled)<br>2. The proposed solution should provide minimum 80 Gbps NGTP real world throughput (Application Visibility & Control, IPS, Anti-Virus/Anti-Malware, Anti-Bot, Basic File Blocking, , web security & Threat Intelligence with Logging enabled)<br>3. Proposed solution must support URL filtering.<br>4. The proposed solution should provide minimum 2M new connections/sec on Layer-4 or 700K new session or connection/sec on Layer-7.<br>5. The proposed solution should provide minimum 40M concurrent connections on Layer-4 or<br>20M concurrent connection on Layer-7.<br>6. Interface Requirement<br>The proposed solution should have:<br>iii. Minimum 1x1G management port<br>iv. Minimum 16x10G SFP+ Port and 4X25G/100G SFP Port<br>.<br>MSP has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 9. | The proposed solution should support IEEE 802.1q VLAN Tagging with minimum of 1024VLANs supported (in NAT/Route mode) | | |
| 10. | The proposed solution should support virtualization (i.e. Virtual Systems / Virtual Domains/Virtual Instances) with minimum 30 instances per device provisioned from day 1. The virtual system should have all the features as of physical device. | | |
| 11. | The proposed solution should have dual and hot swappable power supply modules along with redundant fan tray modules | | |
| 12. | **Network/Routing Requirements (For both IPv4 and IPv6)** | | |
| 13. | The proposed solution must support static routing | | |
| 14. | The proposed solution should also support IPv4 to IPv6, IPv6 to IPv4, IPv6 to IPv6, IPv4 to IPv4 communication | | |
| 15. | The proposed solution must support policy-based routing | | |
| 16. | The proposed solution must support dynamic routing (RIP, OSPF,BGP) | | |
| 17. | The proposed solution must support multicast routing. | | |
| 18. | The proposed solution must support dual stack IPv4 and IPv6. | | |
| 19. | The proposed solution must support DNS64 & DHCPv6 from day-1 | | |
| 20. | **Firewall Features Requirement:** | | |
| 21. | The proposed solution should be ICSA Labs certified or EAL 4 or higher certified. | | |
| 22. | The Proposed solution must support below deployment modes<br>1. Bridge<br>2. Transparent<br>3. NAT | | |
| 23. | The proposed solution must support creating access rule with IPv4 and IPv6 objects simultaneously. | | |
| 24. | The proposed solution should support in-built multiple security groups/ profile and the same security groups/Profile can be used globally for all virtual domains/instances/contexts. | | |
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 26. | The proposed solution must be capable of sending logs in syslog format and its raw log format should be supported by all leading SIEM solutions. | | |
| 27. | The proposed solution should have management plane separated from the data plane, with capability to allocate each plane having dedicated resources like CPUs cores, interface and RAM modules to handle the processing functions. Support for segmentation via virtual firewalls/contexts/tenants, with per-tenant policy and logs | | |
| **28.** | **NAT Requirements** | | |
| 29. | The proposed solution must provide NAT functionality, including PAT. | | |
| 30. | The Proposed solution must support NAT 44, NAT 64, and NAT 66, NAT 46 from Day 1 and must support at least 5,000 NAT from Day 1. | | |
| 31. | The proposed solution should support “Policy-based NAT”. | | |
| 32. | The proposed solution should provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP. | | |
| 33. | The proposed solution must have capability to log traffic bidirectional with bytes in/out information. | | |
| 34. | The proposed solution should support NAT within IPSec/SSL VPN tunnels | | |
| 35. | **Authentication Requirements:** | | |
| 36. | The proposed solution must support for authentication for users and Firewall Administrators LDAP/ RADIUS/ TACACS*/ AAA/ AD for authentication and management of the device. | | |
| 37. | The proposed solution must support for multi factor authentication. | | |
| 38. | The proposed solution should support PKI / Digital Certificate based two-factor authentication for both Users and Firewall Administrators. | | |
| 39. | The solution should identify the device address/host name . | | |
| 40. | **High Availability Requirements:** | | |
| 41. | The proposed solution must support Active-Active as well as Active-Passive redundancy in IPv4 and IPv6. | | |
| 42. | The proposed solution must support Statefull failover for both Firewall and VPN sessions. | | |
| 43. | The proposed solution must support : | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
|  | If any appliance in the cluster malfunctions, hangs, or loses network connectivity due to hardware or software issues, the appliance cluster (either active-active or active-passive) must be able to automatically switch-over to the healthy appliance without any manual intervention. |  |  |
| 44. | The Proposed solution should support VRRP or equivalent and Link Failure Control. |  |  |
| 45. | **Encryption / VPN Requirements** |  |  |
| 46. | The VPN functionalities should be integrated within firewall for both IPsec and SSL-TLS in IPv4 and IPv6 i.e. in dual stack. It should support the following protocols but not limited to DES and 3DES , MD5, SHA-1 and the more secure SHA-256 authentication, Diffie-Hellman Group 1, Group 2, Group 5 and the more secure Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm. The new encryption standard AES 128, and 256 (Advanced Encryption Standard), IPSec VPN should support multi factor authentication. |  |  |
| 47. | The proposed solution must be able to create IPSec tunnelling and Site to Site VPN tunnelling. |  |  |
| 48. | The proposed solution must support Deep SSL Inspection on latest SSL protocols versions including TLS1.3. It shall support the deep packet inspection of different SSL / TLS based Web /any other applications simultaneously. |  |  |
| 49. | The proposed solution should support packet capture/sniffer to examine the contents of individual data packets that traverse through the firewall appliance for troubleshooting, diagnostics and general network activity. |  |  |
| 50. | The proposed solution should have integrated traffic shaping / QoS functionality. |  |  |
| 51. | The proposed solution should be able to support blacklist and whitelist based on Geo-IP including selection based on country name. |  |  |
| 52. | The proposed solution shall have capability to analyse and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP etc. |  |  |
| 53. | The proposed solution should maintain the audit trail for the management activities of individual users and administrators accessing and using the deployed solution. |  |  |
| 54. | The proposed solution should provide capability to understand unused security capabilities and turn them on with best practices, to understand gaps in configuration best practices, recommendations to close security gaps, detect hardware and software system issues. |  |  |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 55. | The proposed solution should provide for Role-Based Access Control (RBAC) and provide access based on the least privilege criteria on the NGFW devices. | | |
| 56. | The proposed solution should comply with FIPS-140-2 standard for cryptographic modules as well as USGv6/IPv6. | | |
| 57. | The proposed solution should have protection for at least 15000, IPS signatures. | | |
| 58. | The proposed solution should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use. | | |
| 59. | **DNS Security** | | |
| 60. | The proposed solution should be enabled with the enterprise protection DNS Security capabilities within the same appliances from day 1 along with OEM threat intelligence feed. | | |
| 61. | The proposed solution should support DNS security in line mode or proxy mode | | |
| 62. | Proposed solution DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence. | | |
| 63. | The proposed solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection. | | |
| 64. | The proposed solution should support capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers. | | |

### 12.3. Type 3 Firewall (150 Gbps)

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| **1.** | **General Requirements:** | | |
| **2.** | Make:<br>Model No: | | |
| **3.** | **Licensing** | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| **4.** | The proposed solution should be per device license for unlimited users for Firewall and other features. The Licences should include<br>1. NGFW(Application Visibility & Control)<br>2. Next Generation Threat Prevention( Application Visibility & Control, IPS, Encrypted traffic inspection Anti-Virus/Anti-Malware, Anti-Bot, Basic File Blocking, URL filtering, web security & Threat Intelligence)<br>All the licences must be provided from day-1. | | |
| **5.** | **Central Management** | | |
| **6.** | 1. The proposed solution should be provided with a separate / dedicated ppliance in HA for Firewall Management and Log Analysis with all the required licenses for managing the all firewall physical as well as Virtual, monitoring, reporting etc.<br>2. The proposed management solution should be either in Physical or Virtual Form Factor . In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3. The proposed management solution must have the capability to manage minimum 100 physical firewall and 200 virtual system firewalls and adequate licenses for managing these Firewalls must be supplied from Day 1.<br>4. The solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>5. The proposed solution should have access through GUI and user management must be based on RBAC.<br>6. The proposed solution must have integrated security architecture with multi-tenancy, analytics, Logging and must have API access for enhanced automation capabilities.<br>7. The proposed solution must provide firewall administration control by segmenting management into multiple virtual domains if required.<br>8. The proposed solution must allow single policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, and scheduling at single place and single locations<br>9. The proposed solution should have separate real time logging base for all traffic that includes Threats, User IDs, URL filtering, Data filtering, content filtering, unknown | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities.<br>10. The proposed solution should have Inter-cluster communication between firewalls configured in high availability and communication with central management should be secure and encrypted.<br>11. Proposed solution must to allow export and forwarding of logs in well-known SIEM formats including Syslog<br>12. The proposed solution should support API for automation. | | |
| 1. | **Performance Parameter:-** | | |
| 2. | 1. The proposed solution should provide minimum 150 Gbps NGFW  real world throughput (Application Visibility & Control, with Logging enabled)<br>2. The proposed solution should provide minimum 120 Gbps NGTP real world throughput (Application Visibility & Control, IPS,  Anti-Virus/Anti-Malware,Anti-Bot, Basic File Blocking, , web security & Threat Intelligence with Logging enabled)<br>3. Proposed solution must support URL filtering.<br>4. The proposed solution should provide  minimum 3M new connections/sec on Layer-4 or 1M new session or connection/sec on Layer-7.<br>5. The proposed solution should provide   minimum 60M concurrent connections on Layer-4 or<br>40M concurrent connection on Layer-7.<br>6. Interface Requirement<br>The proposed solution should have:<br>v. Minimum 1x1G management port<br>vi. Minimum 16x10G SFP+ Port and 4X25G/100G  SFP Port<br>.<br>MSP has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| 3. | The proposed solution  should support IEEE 802.1q VLAN Tagging with minimum of 4094 VLANs supported (in NAT/Route mode) | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 4. | The proposed solution should support virtualization (i.e. Virtual Systems / Virtual Domains/Virtual Instances) with minimum 50 instances per device provisioned from day 1. The virtual system should have all the features as of physical device. | | |
| 5. | The proposed solution should have dual and hot swappable power supply modules along with redundant fan tray modules | | |
| 6. | **Network/Routing Requirements ( For both IPv4 and IPv6)** | | |
| 7. | The proposed solution should also support IPv4 to IPv6,IPv6 to IPv4,IPv6 to IPv6,IPv4 to IPv4 communication | | |
| 8. | The proposed solution must support static routing | | |
| 9. | The proposed solution must support policy based routing | | |
| 10. | The proposed solution must support dynamic routing (RIP, OSPF,BGP) | | |
| 11. | The proposed solution must support multicast routing. | | |
| 12. | The proposed solution must support dual stack IPv4 and IPv6. | | |
| 13. | The proposed solution must support DNS64 & DHCPv6 from day-1 | | |
| 14. | **Firewall Features Requirement:** | | |
| 15. | The proposed solution should be ICSA Labs certified or EAL 4 or higher certified. | | |
| 16. | The Proposed solution must support below deployment modes<br>1. Bridge<br>2. Transparent<br>3. NAT | | |
| 17. | The proposed solution must support creating access rule with IPv4 and IPv6 objects simultaneously. | | |
| 18. | The proposed solution should support in-built multiple security groups/profile and the same security groups/Profile can be used globally for all virtual domains/instances/contexts. | | |
| 19. | The proposed solution must support communication over the IPv6 protocol on the management interface. | | |
| 20. | The proposed solution must be capable of sending logs in syslog format and its raw log format should be supported by all leading SIEM solutions. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 21. | The proposed solution should have management plane separated from the data plane, with capability to allocate each plane having dedicated resources like CPUs cores, interface and RAM modules to handle the processing functions.Support for segmentation via virtual firewalls/contexts/tenants, with per-tenant policy and logs | | |
| **22.** | **NAT Requirements** | | |
| 23. | The proposed solution must provide NAT functionality, including PAT. | | |
| 24. | The Proposed solution must support NAT 44, NAT 64, and NAT 66, NAT46 from Day 1 and must support at least 5,000 NAT from Day 1. | | |
| 25. | The proposed solution should support “Policy-based NAT”. | | |
| 26. | The proposed solution should provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP. | | |
| 27. | The proposed solution must have capability to log traffic bidirectional with bytes in/out information. | | |
| 28. | The proposed solution should support NAT within IPSec/SSL VPN tunnels | | |
| 29. | **Authentication Requirements:** | | |
| 30. | The proposed solution must support for authentication for users and Firewall Administrators LDAP/ RADIUS/ TACACS*/ AAA/ AD for authentication and management of the device. | | |
| 31. | The proposed solution must support for multi factor authentication. | | |
| 32. | The proposed solution should support PKI / Digital Certificate based two-factor authentication for both Users and Firewall Administrators. | | |
| 33. | The solution should identify the device address/host name . | | |
| 34. | **High Availability Requirements:** | | |
| 35. | The proposed solution must support Active-Active as well as Active-Passive redundancy in IPv4 and IPv6. | | |
| 36. | The proposed solution must support Statefull failover for both Firewall and VPN sessions. | | |
| 37. | The proposed solution must support :<br>If any appliance in the cluster malfunctions, hangs, or loses network connectivity due to hardware or software issues, the appliance cluster (either active-active or active-passive) must be able to automatically switch-over to the healthy appliance without any manual intervention. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 38. | The Proposed solution should support VRRP or equivalent and Link Failure Control. | | |
| 39. | **Encryption / VPN Requirements** | | |
| 40. | The VPN functionalities should be integrated within firewall for both IPsec and SSL-TLS in IPv4 and IPv6 ie in dual stack. It should support the following protocols but not limited to DES and 3DES ,MD5, SHA-1 and the more secure SHA-256 authentication, Diffie-Hellman Group 1, Group 2, Group 5 and the more secure Group 14,Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm. The new encryption standard AES 128, and 256 (Advanced Encryption Standard),IPSec VPN should support multi factor authentication. | | |
| 41. | The proposed solution must be able to create IPSec tunnelling and Site to Site VPN tunnelling. | | |
| 42. | The proposed solution must support Deep SSL Inspection on latest SSL protocols versions including TLS1.3. It shall support the deep packet inspection of different SSL / TLS based Web /any other applications simultaneously. | | |
| 43. | The proposed solution should support packet capture/sniffer to examine the contents of individual data packets that traverse through the firewall appliance for troubleshooting, diagnostics and general network activity. | | |
| 44. | The proposed solution should have integrated traffic shaping / QoS functionality. | | |
| 45. | The proposed solution should be able to support blacklist and whitelist based on Geo-IP including selection based on country name. | | |
| 46. | The proposed solution shall have capability to analyse and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP etc. | | |
| 47. | The proposed solution should maintain the audit trail for the management activities of individual users and administrators accessing and using the deployed solution. | | |
| 48. | The proposed solution should provide capability to understand unused security capabilities and turn them on with best practices, to understand gaps in configuration best practices, recommendations to close security gaps, detect hardware and software system issues. | | |
| 49. | The proposed solution should provide for Role-Based Access Control (RBAC) and provide access based on the least privilege criteria on the NGFW devices. | | |
| 50. | The proposed solution should comply with FIPS-140-2 standard for cryptographic modules as well as USGv6/IPv6. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 51. | The proposed solution should have protection for at least 15000, IPS signatures. | | |
| 52. | The proposed solution should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use. | | |
| 53. | **DNS Security** | | |
| 54. | The proposed solution should be enabled with the enterprise protection DNS Security capabilities with in the same appliances from day 1 along with OEM threat intelligence feed. | | |
| 55. | The proposed solution  should support DNS security in line mode or proxy mode | | |
| 56. | Proposed solution DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence. | | |
| 57. | The proposed solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection. | | |
| 58. | The proposed solution should support capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers. | | |

Note#

Type-1 and Type-2 Firewall will be deployed in POD and Type-3 Firewall will be deployed at Perimeter Layer

### 12.4. Anti- Distributed Denial of Services (DDoS) (150 Gbps)

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | Make:<br>Model No: | | |
| 2. | The Proposed solution should be a dedicated appliance (Not a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any State Full Appliance). | | |
| 3. | The Proposed solution must have below performance parameters: | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 1. The proposed solution should have clean real-world throughput: Minimum 150 Gbps<br>2. The proposed solution should have attack mitigation throughput: Minimum 150 Gbps<br>3. The proposed solution must have new connections per second over SSL on 2K key: Minimum 100K with TLS1.3 Hardware acceleration support<br>4. The proposed solution must have minimum 20x10G Ports<br>5. The proposed solution must have minimum 4x40G/100G ports<br>6. The proposed solution must have attack concurrent sessions: Unlimited<br>7. The proposed solution must have attack Mitigation Capacity: Minimum 250 MPPS<br>8. The proposed solution must have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port<br>9. The proposed solution must have Redundant Power Supply.<br>MSP must provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| 4. | The Proposed solution should support horizontal and vertical port scanning behavioural protection. | | |
| 5. | The proposed solution should support behavioural analysis using behavioural algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. | | |
| 6. | The proposed solution should have capability to utilize behavioural algorithms and stateless solution to detect and defend against threats at L3- L7. | | |
| 7. | The Proposed solution must have Behavioural DoS (Behavioural Denial of Service) protection which should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.<br>Network-flood protection should include:<br>i. UDP flood<br>ii. ICMP flood | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | iii. IGMP flood<br>iv. TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood<br><br>Solution should be capable to mitigate layer-7 unknown/Random/Dynamic URI based DoS/DDoS flood attacks. | | |
| 8. | The Proposed solution should have DNS Flood protection for each type of query including, A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV etc. | | |
| 9. | The Proposed solution should have Positive Security Model advanced behaviour-analysis technologies to separate malicious threats from legitimate traffic. | | |
| 10. | The proposed solution should provide advanced real-time detection and mitigation of both known and zero-day DNS DDoS attacks. | | |
| 11. | The proposed solution should handles DNS DDoS attacks with its adaptive technology which comprises of at least following main components:<br>a. Behavioural detection automatically learns normal DNS traffic patterns during peacetime<br>b. Attack characterization automatically identifies the DNS domains or FQDNs<br>c. Accurate mitigation involves adaptive responses tailored to the specific DNS DDoS vectors and attack patterns. | | |
| 12. | The Proposed solution must have inbuilt or out of box SSL decryption features to mitigate Layer-7 DDoS attacks. | | |
| 13. | The Proposed solution must detect, characterize, and mitigate SSL attacks | | |
| 14. | The Proposed Solution should support DNS Challenge and DNS Rate Limit. | | |
| 15. | 1. The Proposed solution should have functionality of TLS Fingerprint to block SSL attacks and should also have mechanism to defend against Web DDoS attacks<br>2. The proposed solution must capable to inspect Layer-7 attack like https DDoS attacks etc. and also mitigate attacks. | | |
| 16. | The Proposed solution should support HTTP Challenge Response authentication. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 17. | The Proposed solution should have following protections but not limited to SIP Flood Protection, UDP and UDP Fragmented Flood. | | |
| 18. | The Proposed solution should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1 | | |
| 19. | 1. The Proposed solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment<br>2. The proposed solution should also be transparent to tunnelling protocols such as L2TP, GRE, and IP-in-IP traffic. | | |
| 20. | 1. The Proposed solution should protect against Zero Day DDoS Attacks. Zero day attack protection should be provided using behaviour-based technology.<br>2. The proposed solution should generate automatic real time signature/ challenge response mechanism, without any manual intervention for protection against Zero Day DDoS Attacks. | | |
| 21. | | | |
| 22. | The proposed solution should have below security protection profiles:<br>a. DNS Protections<br>b. SYN-Flood Protection.<br>c. HTTPS Flood protections<br>d. Anti-Scanning Profile. | | |
| 23. | The Proposed solution should protect from DDoS attacks behind a CDN Network. | | |
| 24. | The Proposed solution should able to protect from the below vulnerabilities/threats<br>i. Server-based vulnerabilities:<br>ii. Web server vulnerabilities<br>iii. Mail server vulnerabilities<br>iv. FTP server vulnerabilities<br>v. SQL server vulnerabilities<br>vi. DNS server vulnerabilities<br>vii. SIP server vulnerabilities<br>viii. Trojans and backdoors | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | ix. IRC bots<br>x. Phishing | | |
| 25. | **The proposed solution should use the following Block Actions:**<br>i. Drop packet,<br>ii. Reset (source, destination, both),<br>iii. Suspend (source IP address, source port, destination IP address, destination port or any combination),<br>iv. Challenge-Response for TCP, HTTP and DNS suspicious traffic | | |
| 26. | The proposed solution should have at least below tracked mechanism to count and act upon:<br>1. Per Source<br>2. Per Destination<br>3. Per Source and Destination Pair<br>4. Track returning traffic from destination and suspend corresponding sources | | |
| 27. | The proposed solution should provide Geo-Location blocking, all known active attacks and signature update along with under attack service from day-1 | | |
| 28. | **Central Management Solution** | | |
| 29. | 1) The Management solution should be provided and deployed in HA mode and must have the capability to store and analyse logs for a minimum period of 90 Days.<br>2) The management solution should have the capability to manage minimum 20 pairs of DDoS devices and adequate licenses for managing these DDoS must be supplied from Day 1.<br>3) The proposed solution should be provided for Management and Log Analysis with all the required licenses for managing, monitoring, reporting etc.<br>4) The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>5) The proposed solution should have access through GUI and user management must be based on RBAC.<br>6) The proposed solution should have separate real time logging base for storing log of all Traffic that includes Threats, User IDs, and correlated log view base on other logging activities. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 7) The proposed solution should support API for automation. | | |
| 30. | The proposed solution should be able to define an attack threshold based on the average incoming traffic flow, thereby dropping the excess traffic which exceeds defined threshold. | | |
| 31. | The proposed solution should have the capability to create more than or equal to 200 network protection policy. | | |
| 32. | The proposed solution must have redundant power supply. | | |
| 33. | The proposed solution must support IPV6 Stack, IPV4 Stack and DUAL Stack. The proposed solution should also support IPv4 to IPv6, IPv6 to IPv4, IPv6 to IPv6, IPv4 to IPv4 communication | | |
| 34. | The proposed solution must support communication over the IPv6 protocol on the management interface | | |
| 35. | The proposed solution must support whitelist based on IP and Subnet. | | |
| 36. | The proposed solution must support blacklist based on IP and Subnet. | | |
| 37. | The proposed solution must be able to protect against DDOs in both inbound and outbound direction. | | |
| 38. | The proposed solution must support to be deployable in layer 2 transparent mode. | | |
| 39. | The proposed solution should be capable to mitigate low and slow attacks. | | |
| 40. | The proposed solution must support reporting through email. | | |
| 41. | The proposed solution must support syslog and SNMPV3. | | |
| 42. | The proposed solution must provide<br>i. Historical Incident tracking<br>ii. Daily activity reporting<br>iii. Produce reporting summaries<br>iv. The solution should have capability to create graphical report of incoming and outgoing traffic in Mbps/Kbps/Gbps and connection per second and concurrent sessions.<br>v. The solution should have the capability to show the traffic, connection per second for a particular application/Server/Website<br>vi. The proposed solution should have the provision to create report based on source, destination IPs, and source and destination ports with specific values. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 43. | The Proposed solution must have security reports and must have selectable output formats including HTML and PDF. | | |
| 44. | The proposed solution should support the common Event Format (CEF). | | |
| 45. | The Proposed solution must support authentication mechanisms including Radius, Local Password and TACACS+. | | |
| 46. | The Proposed solution must support remote administration using SSH and HTTPS. | | |

## 12.5. Network Detection and Response (NDR) Specifications

| Network Detection and Response (NDR) Specifications | | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| Sr. No. | Requirement Specification | | |
| 1 | The proposed Sensor/Probe must be capable of providing flow records according to IETF RFC7011 IPFIX formats. | | |
| | The proposed Sensor/Probe must be capable of monitoring Layer 7 information including SSL, DNS, HTTP, SIP, Samba/CIFS, DHCP/DHCPv6, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, QUIC, DNS over HTTPS or DNS over QUIC and, TCP session timing information. | | |
| 2 | The proposed solution should be able to join multiple unidirectional flow records coming from different sources like routers, switches, firewall that are associated with a single session and represent them as a single bidirectional flow record. | | |
| 3 | The proposed probe should make use of deep packet inspection technology to extract protocol and application level details from raw packets and create detailed flow record for each session. | | |
| 4 | The proposed solution should support 25 Gbps throughput. | | |
| | The proposed probe appliance should be able to process traffic at the rate of 1-million packet per second. | | |
| 5 | The proposed solutions should be capable of analysing encrypted communication without the need for any decryption technology being put in place. The Sensor/Probe Probe must also utilize encrypted flow fingerprinting methodologies to identify potentially malicious flows in addition to using anomaly detection. | | |
| 6 | The proposed solution should analyse flow records and include information about entity including geolocation, service provider, age, nature/intent of communication such as download, upload, push, request/response, etc. | | |
| 7 | The proposed solution should be capable of building and continuously updating its model of network behavior. | | |
| | The solution should be capable of analysing recent traffic against historical traffic using different types of network/host/application behavior models. | | |

| | | | |
|---|---|---|---|
| 8 | The proposed solution should atleast follow one standard framework MITRE/NIST/CSF etc. for anomalies detection | | |
| 9 | The proposed solution should able to detect security incidents, operational issues and network anomalies. | | |
| 10 | The proposed solution should utilize/ ingest threat intelligence feeds from third parties, using industry standards for threat information sharing | | |
| 11 | The proposed solution should be capable of segregating & accurately labeling traffic originated by humans and automatic machine origin traffic for better applicability in a heterogeneous environment that has traffic from smart-devices, IoT and, traditional north-south & east-west data-centre environment. | | |
| 12 | The proposed solution should provide API to allow to implement response actions. | | |
| 13 | The proposed solution should be capable of closing an offending connection without the need for any integration should such a need arise. | | |
| 14 | The proposed solution should support web-browser based end-user interface for configuration, monitoring, management and analysis and must include a dashboard along with the capability of making custom dashboards | | |
| | **Central Management** | | |
| | 1. A separate Centralized Management / Reporting solution must be provided and deployed in HA mode.<br>2. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>3. The proposed solution must have the capability to manage minimum 50 NDR solution and adequate licenses for managing these NDR must be supplied from Day 1.<br>4. The proposed management solution should be either in Physical or Virtual Form Factor . In case of virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>5. The proposed solution Should have access through GUI and user management must be based on RBAC.<br>6. The proposed solution should support API for automation. | | |
| 15 | The proposed solution should employ signature matching, pattern matching, threshold matching, behavior correlation, statistical rules and, predictive techniques to detect threats, anomalies and, risks in the network. | | |

| | | | |
|---|---|---|---|
| 16 | The proposed solution should be capable of mapping risks to a well-known/understood security framework such as the Kill-Chain or MITRE ATT&CK framework. | | |
| 17 | The proposed solution should be capable of detecting threats including behavior anomalies in real time without delays. | | |
| 18 | The proposed solution should be capable of detecting threats based on IP, Domain and, URL reputation. | | |
| 19 | The proposed solution should be capable of integrating Vulnerability Management tools to highlight suspicious traffic targeting vulnerable applications and services. | | |
| 20 | The proposed solution should be capable of directly responding to threats in locally connected LAN segments by preventing network connection of an infected host. | | |
| 21 | The proposed solution should automatically discover domains active in the network and qualify the risk they pose. | | |
| 22 | The proposed solution should discover and classify device and set up device groups for easy association with alerts/risks and rules. | | |
| 23 | The proposed solution should automatically discover types of Bot (User-Agent) active in the networks | | |
| 24 | The proposed solution should optionally be capable of capturing and retaining raw packet captures if needed for forensics. | | |
| 25 | The solution should be capable of building a timeline of attack by leveraging historical data visualization capabilities. | | |
| 26 | The solution should identify normal network traffic and highlight suspicious traffic that falls outside the normal range | | |
| 27 | The solution should offer behavioral techniques (non-signature-based detection), such as machine learning or advanced analytics in addition to signature based techniques. | | |
| 28 | The solution should provide automatic or manual response capabilities to react to the detection of suspicious network traffic | | |
| 29 | The solution should be capable of detecting threats/risks in remote network segments without the need for forwarding full packet capture data over wide area networks. | | |
| 30 | The solution must automatically identify and classify threats, including attack phase and risk, without requiring any intervention. | | |
| 31 | The solution must be able to differentiate key assets declared from other hosts for risk prioritization. | | |
| 32 | The solution should automatically score and prioritize each individual attacker behavior detected. | | |

| | | | |
|---|---|---|---|
| 33 | The solution should automatically score and prioritize each host based on its behaviors over time. | | |
| 34 | The solution must have the notification capabilities for the detections. | | |
| 35 | The solution must provide packet captures of identified attacker behaviors for analysis. | | |
| 36 | The solution must have the ability to analyze and correlate network traffic: North, South, East, West traffic | | |
| 37 | The solution should be capable of identifying Virtual Machines deployed in the network. | | |
| 38 | The solution should have the ability to perform matching on IOCs | | |
| 39 | The Solution must have the capabilities to be integrated with some leading SIEM solution like (McaFee, Qradar, ArcSight..etc) | | |
| 40 | The solution must natively integrate with some EDR Vendors, also have an API capable of integrating with others when needed. | | |
| 41 | The solution should detect the following type of threats (including but not limited to): | | |
| 42 | Remote access tunnels used by Attackers to control compromised systems | | |
| 43 | Hidden tunnels over http, https, or DNS to communicate with C&C or to exflitrate data | | |
| 44 | Web based command and control (independed of IP reputaiton and treat lists) | | |
| 45 | Malware using a fake browser | | |
| 46 | Relay hosts | | |
| 47 | Malware replicating a payload to /exploiting vulnerabilities against other hosts | | |
| 48 | TOR Anonymization | | |
| 49 | Peer-to-peer traffic | | |
| 50 | Botnet monetization behaviours: Click Fraud, Bitcoin Mining, outbound DoS, outbound SPAM | | |
| 51 | Ransomware activity: encrypting file shares | | |
| 52 | Network reconnaissance scans: port scans, port sweeps, scanning unused IPs. | | |
| 53 | Privilege anomaly: to find use cases realter Privilege escalation, accounts take over, credentials theft and misuse - Use of a stolen credential from a host it has not previously been used on | | |
| 54 | Use of a stolen credential from its normal system, but asking for unusual services or in excessive volume | | |
| 55 | A host trying many credentials to attempt to gain access to a server | | |
| 56 | Kerberos service scans, Fake Kerberos servers | | |
| 57 | Brute force attacks | | |

| | | | |
|---|---|---|---|
| 58 | Use of administrative protocols, including RDP, SSH, IDRAC, and IPMI, where the target host is not typically administered by the source host on that protocol | | |
| 59 | A host exfiltrating data to an unusual destination | | |
| 60 | A host gathering unusual volumes of data and then sending exfiltrating to an external IP | | |
| 61 | A host being used as a relay to exfiltration data to an external system" | | |
| 62 | The solution should have the ability to detect enumeration of file shares | | |
| 63 | The solution should have the ability to detect AD/LDAP reconnaissance using techniques similar to Bloodhound | | |
| 64 | The solution should have the ability to detect use of PowerShell/WMI and RPC to move laterally via remote code execution | | |
| 65 | The solution should have the ability to detect reconnaissance of RDP servers. | | |
| 66 | The solution should have the ability to detect the use of PSexec and other remote administration tools to move laterally via SMB. | | |
| 67 | The solution should have the ability to detect anomalies for protocols | | |
| 68 | Even if the license exceeded, the NDR platform must work normally from technical perspective | | |
| 69 | The solution must be able to forward the network security metadata to an existing Data Lake or SIEM. Or can use a dedicated hardware for on-prem storage. | | |
| 70 | The solution should support detection of application over Encrypted Traffic | | |
| 71 | The solution should support detection of cyber-attacks on SSH without decrypting network traffic | | |
| 72 | The solution should support detection of deviation in network traffic based on Protocol/Domain/IP | | |
| 73 | The solution should have visual connectivity for user activity based on criticality | | |
| 74 | The solution should have network traffic enrichment & threat hunting support. | | |
| 75 | The solution should enable Detection of Command and Control and, abnormal behaviour. | | |
| 76 | The solution should highlight immediately any domain which needs immediate attention | | |
| 77 | The solution should provide a list of User-Agent Active in the network (Example: Bitsadmin etc.) | | |
| 78 | The solution should provide a list of public IP with no dns communication | | |
| 79 | The solution should have an API available for Integration with SIEM/SOAR | | |
| 80 | The solution should have on-demand automated Custom Signature creation | | |
| 81 | The solution should be able to deploy response to Firewall (NGFW/IPS etc) | | |

| | | | |
|---|---|---|---|
| 82 | The solution should optionally provide log signalling ( Detect and Automation logging from Network Devices) | | |
| 83 | The solution should support automated investigation at Endpoint against malicious/suspicious traffic | | |
| 84 | The solution should provide a Case and Change management as an integral part of the tool | | |
| 85 | The solution should provide support for API based Integration with Third Party Case/Change Management | | |
| 86 | The solution should support agent based and agentless collection of flow data and, detection of malicious activity | | |
| 87 | The solution should provide a queriable and referencible serverless data-store without using any database server | | |
| 88 | The solution should support generating a device with application inventory list and be able to prevent access to devices that do not match whitelisted client access profile. | | |
| 89 | The solution should provide direct integration with Active-Directory Servers, Switches and Routers to identify clients, device types, platforms, host names, signed in users, access privilege for better assessment of security risks. | | |
| 90 | The solution should provide a remote shell capability to manage and query the database using standard SQL for administrative reporting and exploration. | | |
| 91 | The solution should provide contextual details around alerts in the UI and should provide suggested response/remedial action. | | |
| 92 | The solution must support centralized connectivity and management of multiple distributed NDR sensors, including configuration, health monitoring, and policy synchronization from a single console. | | |
| 93 | The solution must provide flow aggregation and de-duplication capabilities, ensuring that redundant events from multiple sensors are intelligently correlated and stored only once. | | |
| 94 | The Solution must serve as a unified monitoring and analytics platform, offering real-time dashboards, historical reporting, and enterprise-wide alert management. | | |

### 12.6. Web Application Firewall (WAF) 90 Gbps)

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| **1.** | **General Requirements:** | | |
| **2.** | Make:<br>Model No: | | |
| 3. | The Proposed solution should be a dedicated hardware Solution with hardened OS and deployable in standard data center racks. | | |
| 4. | i. The proposed solution must use it's own Hypervisor which should be a specialized purpose build hypervisor and NOT a commercially available hypervisor like XEN, KVM etc.<br>ii. The proposed solution must have a virtualized hypervisor that only support OEM's own OS, and third-party OS (open source, Linux, different OEM solution) should not be allowed to be installed on hardware. | | |
| 5. | The Proposed web application firewall solution should provide specialized application threat protection. | | |
| 6. | The Proposed solution should protect against application layer attacks targeted at web applications. | | |
| 7. | The Proposed solution should provide bi-directional protection against sophisticated threats like SQL injection, cross-site scripting and support OWASP application security methodology. | | |
| 8. | The Proposed solution should provide controls to prevent identity theft. | | |
| **9.** | **Performance requirements** | | |
| 10. | The Proposed solution should be able to provide a WAF of SSL throughput minimum 90 Gbps along with below hardware requirement.<br>1. Appliance must provide minimum SSL TPS of 150 with RSA 2K keys and 100K TPS with ECC ECDSA P-256<br>2. Minimum: 4x40G and 4x10G ports from day 1<br>3. Dual Power Supply<br>4. The solution must support at least 16 virtual instances from day 1. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| | MSP has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| **11.** | **Feature specifications.** | | |
| 12. | The Proposed solution should be able to perform in multiple modes such as active/passive mode, transparent mode and proxy mode. | | |
| 13. | The Proposed solution should continuously track the availability of the servers being protected. | | |
| 14. | The Proposed solution should have Data Leak Prevention functionality to analyse all outbound traffic alerting/blocking any credit card/Aadhaar No leakage and information disclosure. | | |
| 15. | The Proposed solution should provide controls to meet PCI DSS compliance requirements for web application servers. | | |
| 16. | The Proposed solution should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks. | | |
| 17. | The Proposed solution should support automatic signature updates to protect against known and potential application security threats. | | |
| 18. | The Proposed solution should have the ability to define different WAF policies with different settings like parameter length, URL prefix, meta characters, allowed and disallowed URL, parameter types etc. for different applications instead of one single policy or a global setting. | | |
| 19. | The Proposed solution should have the ability to create custom attack signatures or events. | | |
| 20. | The proposed solution should have the capability to protect certain hidden form fields. | | |
| 21. | The Proposed solution must provide ability to allow or deny a specific URL access/IP(s). | | |
| 22. | The Proposed solution should support normalization methods such as URL decoding, Null Byte string, termination, converting back slash to forward slash character etc. | | |
| 23. | The Proposed solution should support IP reputation service and able to provide up to date information about threatening sources. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 24. | The Proposed solution must support IPv6 for reverse proxy deployments and it should also support IPv4 to IPv6 and IPv6 to IPv4 communication. | | |
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface | | |
| 26. | The Proposed solution should have BOT mitigation functionality (including CAPTCHA or equivalent):<br>(a) Without having to go on internet for some cloud-based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc<br>or<br>(b) Equivalent technology for bot mitigation. | | |
| 27. | The Proposed solution should have file upload violation capabilities and should provide support for scanning of malicious content. | | |
| 28. | The proposed solution should detect and mitigate HTTP Parameter Pollution (HPP) attacks, preventing malicious manipulation of query parameters and preserving the intended behaviour of web applications | | |
| 29. | The Proposed solution should be able to employ connection pooling technology to optimize backend network operations and server resources. | | |
| 30. | The Proposed solution should have features to hide errors from server and redirect to customized page. | | |
| 31. | The Proposed solution should allow IP addresses or IP address range for bypassing applied security policy for one particular hosted application but should not bypass others. | | |
| 32. | The Proposed solution should facilitate in hiding/masking specific sensitive parameters pertaining to specific applications. | | |
| 33. | The Proposed solution should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address permanently or for a time period. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 34. | The Proposed solution should inspect Simple Object Access Protocol (SOAP) and extensible Mark-up Language (XML), in addition to HTTP (HTTP headers, form fields, and the HTTP body). | | |
| 35. | The Proposed solution should have the negative security model it should detect and protect attack based on Signature (Regular expression) and complex logic (logical AND, Logical OR) against incoming URL request and the same may be extended for all parts (i.e., URI, parameters, headers, cookies.) | | |
| 36. | The Proposed solution should have the positive security model and it should validate URLs, directories, cookies, headers, form/query parameters, HTTP methods, File upload Extensions, allowed meta characters etc. | | |
| 37. | The Proposed solution should support profiling to configure fine grained controls for each deployed web application. | | |
| 38. | The Proposed solution should support all operating systems/development frameworks and their versions including but not limited to Windows, AIX, Unix, Linux, Solaris, HP Unix. | | |
| 39. | The Proposed solution should provide HTML rewriting functionality (e.g., edit, add, delete request and response header, rewrite and redirect the URL in the request, rewrite response body etc.). | | |
| 40. | The Proposed solution should have the ability to generate and issue CAPTCHA or equivalent queries to challenge suspicious clients. | | |
| 41. | The Proposed solution should have the capability to auto-learn security profiles required to protect the Infrastructure. | | |
| 42. | The Proposed solution should provide a statistical view on collected application traffic. | | |
| 43. | The Proposed solution should detect and prevent brute force attack (repeated requests for the same resource) against any part of the applications. | | |
| 44. | The Proposed solution should provide protection from application layer DDOS attacks. | | |
| 45. | The Proposed solution must protect against SYN-flood type of attacks. | | |
| 46. | The Proposed solution should be able to protect cookie poisoning and cookie tampering. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 47. | The Proposed solution must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2.0 and HTTP/3.0 | | |
| 48. | The Proposed solution should support restricting/controlling the methods used. | | |
| 49. | The Proposed solution should validate header length, content length, Body length, Parameter length, body line length etc. | | |
| 50. | The Proposed solution should support hosting/terminating of SSL web applications and should allow to upload the certificates and private/public key pairs for the web servers. | | |
| 51. | The Proposed solution should work In termination mode, the backend traffic (i.e., the traffic from the WAF to the web server) can be encrypted via SSL. | | |
| 52. | The Proposed solution must support all major cipher suites. | | |
| 53. | The Proposed solution should provide protection against SSL based attacks. | | |
| 54. | The Proposed solution should support for SSL offloading. | | |
| 55. | The Proposed solution should support high availability in active/passive and active/active mode. | | |
| 56. | The Proposed solution should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers. | | |
| 57. | The Proposed solution must be integrated with third party vulnerability scanning tools to provide virtual patching with required understanding of WAF policy. | | |
| 58. | The Proposed solution should support secure administrative access using HTTPS and SSH. | | |
| 59. | The Proposed solution should support role-based access control for Management. | | |
| 60. | The Proposed solution should have ability to remotely manage appliances. | | |
| 61. | The Proposed solution should have management user interface support for both GUI and CLI access. | | |
| 62. | The Proposed solution should have separate network interface for SSH/HTTPS access. | | |
| 63. | The Proposed solution must support for trusted hosts. | | |
| 64. | The Proposed solution must have Role-based management with user authentication. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| **65.** | **Central Management Solution** | | |
| 66. | 7. Centralized Management / Reporting solution must be provided a separate Centralized Management and Reporting solution and deployed in HA mode<br>8. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>9. The proposed solution must have the capability to manage minimum 50 WAF solution and adequate licenses for managing these WAF must be supplied from Day 1.<br>10. The proposed management solution should be either in Physical or Virtual Form Factor . In case of virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>11. The proposed solution Should have access through GUI and user management must be based on RBAC.<br>12. The proposed solution should support API for automation. | | |
| 67. | The Proposed solution should support two factor authentication for login into the management Web GUI. | | |
| **68.** | **Logging, Reporting and Troubleshooting** | | |
| 69. | The Proposed solution should have ability to identify and notify system faults and loss of performance. | | |
| 70. | The Proposed solution should support log aggregation. | | |
| 71. | The Proposed solution should support multiple log formats such as CSV, Syslog, TXT, etc. | | |
| 72. | The Proposed solution should support reporting and sending the report via E-Mail. | | |
| 73. | Proposed solution should support report formats in PDF, HTML/WORD/RTF, etc. | | |
| 74. | The proposed solution must have facility to send all logs to separate log server/SIEM solutions as per standard norms. | | |
| 75. | The Proposed solution must have mechanism to raise alert to SOC team through Email, Syslog, SNMP Trap, Notification etc. for blocking the traced malicious IP source causing specific attack. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 76. | The Proposed solution should support to generate reports like pie-chart, bar-chart based on user defined security compliance baseline. | | |
| 77. | The Proposed solution should allow commands from WAF for troubleshooting network related issues like Ping and traceroute. | | |
| 78. | The Proposed solution should support to generate vulnerability reports based on standard vulnerability database like CVE, NVD etc. | | |
| 79. | The Proposed solution should support to take full secure configuration backup on a physical disk or SAN/NAS storage. | | |
| **80.** | **Service Support** | | |
| 81. | OEM should be able to deploy the Web application firewall appliance and remove it from the network with minimal impact on the existing web applications or the network architecture. | | |
| 82. | Appliance should support integration with orchestration systems and APIs if required. | | |

## 12.7. Type-1 Intrusion Prevention System (IPS) (20 Gbps)

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **Platform Requirement** | | |
| 2. | Make:<br>Model No: | | |
| 3. | The IPS solution must be a purpose-built dedicated appliance (not a subset of firewall or UTM appliance and its firmware should be dedicated firmware and should not be same or shared with any other blades i:e: Firewall, DDoS, UTM Etc. The solution should not use the same firmware/underlying OS for Next Generation Firewall AND/OR IPS offering. | | |
| 4. | The proposed solution must have separate dedicated interface for management | | |
| 5. | The proposed solution must have inbuilt internal Redundant Power Supply (RPS). | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 6. | The proposed solution should be able to support the inbound and outbound TLS/SSL decryption for traffic inspection and attack identification | | |
| 7. | **Performance requirement** | | |
| 8. | 1. The Proposed solution must have below hardware requirements<br>2. The proposed solution must have minimum inspected throughput of 20 Gbps for all kinds of real-world traffic.<br>3. The proposed solution must be support minimum SSL throughput-10 Gbps.<br>4. The proposed solution should have SSL connection per second: Minimum 10K<br>5. The proposed solution must have New Connections Per Second: Minimum 500K<br>6. The proposed solution must have Concurrent Connection: Minimum 15M<br>7. The proposed solution must be supported minimum ACL-1800.<br>8. The proposed solution must have minimum 16x10G SFP Ports<br>9. All ports should be bypass mode. Bypass mode port should not be included in these ports. These ports will be used for traffic only.<br>10. The proposed solution, which acts as transparent device to the network have a fail open feature in all port.<br>11. When IPS transparent device goes down, traffic does not stop.<br>12. If the device does not have fail open feature in built, then they facilitate bypass/fail open kit to achieve the functionality.<br>13. The proposed solution should offer traffic bypassing capability on the provided inbuilt interfaces i.e. in case of power and/or HW failure the traffic should be able to flow without interruption from the respective interfaces<br>14. The proposed solution must have 1GxManagement Interface & RJ-45 Serial Console Port<br>15. The proposed solution must have Redundant Power Supply<br>16. The proposed solution Latency must be < 60 microseconds<br>17. The proposed solution must be Rack mountable<br>18. The proposed solution must have 20,000 IPS signatures.<br>19. Bidder has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| 9. | **Features** | | |
| 10. | The proposed solution must accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, crypto-mining brute force, L3 to L7 attacks and zero-day attacks . | | |
| 11. | The proposed solution must use prevention techniques and provide zero-day protection against Worms, Trojans, Spyware, Key Loggers, and other malware from penetrating the network. | | |
| 12. | 1. The proposed solution must perform traffic inspection based on Signatures, Protocol anomaly, Behaviour anomaly, Reputation (IP and URL).<br>2. The Proposed solution must support following deployment Modes.<br>a) IDS<br>b) SPAN<br>c) Inline<br>d) L2<br>e) Bridge | | |
| 13. | The proposed solution must accurately detect the following attack categories: - Malformed traffic, Invalid Headers, DoS, Vulnerability exploitation, Zero-day and unknown attacks | | |
| 14. | The proposed solution must support IP (IPv4 and IPv6), URLs, Hashes and file reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist | | |
| 15. | The offered IPS solution should be able to integrate with the on-premises zero-day (sandboxing) solution of the same OEM | | |
| 16. | 1. The proposed solution must support vulnerability based and exploit based signatures.<br>2. It must detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability) | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 17. | The device must handle following traffic inspection and support: IPv6, IPv4, MPLS, Tunnelled, the proposed solution should also support IPv4 to IPv6 and IPv6 to IPv4, IPv6 to IPv6, IPv4 to IPv4 communication, | | |
| 18. | The proposed solution must support Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection | | |
| 19. | a) The proposed solution must be capable to support protection against Client-side attacks,<br>b) The proposed solution must be capable to support protection for both IPv4 & IPv6 simultaneously. Dual-stack or native dual-stack IP implementations provide complete IPv4 and IPv6 protocol stacks in the same network node and native communications can be done between nodes using either protocol,<br>c) The proposed solution must be capable to support zero-day botnet protection.<br>d) The proposed solution must be capable to protect against DoS/DDoS attacks,<br>e) The proposed solution must be capable to inspect DNS response packets for blacklisted domains, Malware scan on HTTP, FTP and SMTP protocols.<br>The proposed solution OEM must have its own threat intelligence analysis centre and shall share threat intelligence with NIC regularly. | | |
| 20. | The proposed solution must capable to protect application anomalies, P2P attacks, TCP segmentation and IP fragmentation. | | |
| 21. | 1. The proposed solution must be capable to perform entire packet capture of the traffic for analysis. (e.g. for capturing the traffic between two IP address for a specific period),<br>2. The proposed solution must be  capable to support NTP ( Network Time Protocol),<br>3. The solution must have Capability to restrict access of URL/IP based on Geo-location (County), | | |
| 22. | The proposed  solution should provide protection with security engines like anomaly detection /behavioural based, anti-scan and should have rate based, pattern based, vulnerability based, exploit based prevention capabilities and support for custom defined signatures | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 23. | The proposed solution should also ensure defense against all types of encrypted attacks, exploits and vulnerabilities. | | |
| 24. | The proposed solution should have capability to protect based on Rate-based threats, Statistical anomalies | | |
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface | | |
| 26. | The Proposed solution must prevent SSL protocol-based attacks | | |
| 27. | The proposed solution must Protect against IPv6 based attacks | | |
| 28. | The proposed solution must support block attacks based on IP reputation, DNS Inspection, Geo-location, URL Inspection. | | |
| 29. | The proposed solution should support file reputation/type on the basis of application protocol including http, https, FTP, SMB (no file must be sent to Cloud) | | |
| 30. | The proposed solution should be intuitive and provide most of the features through the GUI only including enabling the XFF to identify the true-client IP | | |
| 31. | a) The proposed solution must be capable of signature-less intrusion detection technology allowing the IPS to identify network traffic and stops zero-day attacks for which no signatures exist.<br>b) The proposed solution should have the capability to enable/disable each individual signature for specific source and destination. | | |
| 32. | The proposed solution must have the ability to block connection to or from outside network based on the reputation of the IP address that is trying to communicate with the network | | |
| 33. | a) The proposed solution must protect against vulnerability in Web applications, Databases.<br>b) The Proposed solution must have features for time-based security policies like Geo-location, white list and blacklist.<br>c) The proposed solution should also have source IP quarantine feature. | | |
| 34. | The proposed solution must protect against DOS attacks based on: | | |
| 35. | Heuristic-based detection | | |
| 36. | Must have the feature for creating user-defined signature. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 37. | Must have the feature for importing SNORT signatures. | | |
| 38. | a) The proposed solution OEM must have its own threat intelligence analysis center.<br>b) The proposed solution must have features to search signature-based CVE IDs. | | |
| 39. | Prevention and Response | | |
| 40. | The proposed solution must support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done and its logging. | | |
| 41. | The proposed solution must support a wide range of response actions such<br>a) Drop<br>b) Block<br>c) Allow<br>d) Reject<br>e) Quarantine<br>f) Trace/Packet Capture<br>g) Rate limit<br>h) Log traffic/monitor traffic | | |
| 42. | 1. The proposed solution shall provide source reputation-based analysis.<br>2. The proposed solution must support source lookup for IP and domain reputation. | | |
| 43. | The proposed solution must support following capabilities of packet capture, from particular source, destination and protocol through GUI. Email alert, SNMP alert, Syslog alert | | |
| 44. | The proposed solution should ensure defence against all types of encrypted attacks by inspecting and blocking malicious SSL traffic from day-one. | | |
| 45. | The offered product capable to protect- Web applications, Web 2.0, Databases, Network and Security Devices. | | |
| 46. | Policy Configuration | | |
| 47. | The proposed solution should have facility to exempt IPS inspection for a particular signature based on- Source or Destination IP/Subnet, Between two IP/subnet | | |
| 48. | 1. The proposed solution should have facility to enable/disable each individual signature. Each signature to allow granular tuning, | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 2. The proposed  solution should  be capable to support granular management and allow policy to be assigned per device, port, VLAN tag, IP address/range,<br>3. The proposed  solution should   have facility to exempt a particular IP/Subnet from IPS inspection and generate logs for this particular activity | | |
| 49. | The solution must be capable of mapping IP addresses to username, and making this information available for event management purposes. | | |
| 50. | The proposed solution must support authenticated NTP synchronization. | | |
| 51. | **Central Management** | | |
| 52. | 1) The proposed solution should be provided and deployed with a separate / dedicated Appliance in HA for IPS Management and Log Analysis with all the required licenses for monitoring, reporting etc.<br>2) The proposed management solution should be either in Physical or Virtual Form Factor . In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3) The proposed Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>4) The proposed solution must have the capability to manage minimum 50 pairs of IPS devices and adequate licenses for managing these IPS must be supplied from Day 1.<br>5) The proposed solution should have access through GUI and user management must be based on RBAC.<br>6) The proposed solution must have integrated security architecture with multi-tenancy, analytics, Logging and must have API access for enhanced automation capabilities.<br>7) The proposed solution should support API for automation. | | |
| 53. | The proposed solution must be accessible over secure channel. | | |
| 54. | **Role based administration:-** | | |
| 55. | The proposed solution must facilitate administrator to manage multiple IPS devices over network. | | |
| 56. | The proposed solution must support multiple roles like administrator, operator etc. | | |
| 57. | The proposed solution must support to remote administration of individual IPS devices from specific IP addresses / subnets / user id's only. | | |
| 58. | The proposed solution must support audit log facility. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 59. | The proposed solution must support export / import of configuration files for each IPS device. | | |
| 60. | The proposed solution must support updation of IPS signatures on the IPS devices from the centralized management solution. | | |
| 61. | The proposed solution must update its attack signature database regularly on management solution and it must be configurable to update the signatures automatically without manual intervention. | | |
| 62. | The proposed solution must notify automatically through e-mail/displayed in manager window about the availability of new signatures and new product releases. | | |
| 63. | The proposed solution must make new attack signatures and new major software releases available for download from its Web site. | | |
| 64. | The proposed solution must support centralized performance/Health monitoring of IPS devices. | | |
| 65. | The proposed solution must have the facility to display: - Real-time Log and Historical log for a given period | | |
| 66. | The proposed solution must support a wide variety of pre-built as well as custom reports. | | |
| 67. | The proposed solution must be able to output report data into a variety of different file formats like HTML, PDF etc. | | |
| 68. | 1. The proposed solution must support auto-email of pre-defined and customized reports at a scheduled time.<br>2. The proposed solution should be able to send the notifications to management console, remote syslog and email once the signature is triggered | | |
| 69. | The proposed solution must support the archiving and backup of events. | | |
| 70. | The proposed solution must support policy configuration and event management functions for the IPS appliances. | | |
| 71. | The proposed solution should have real-time Dashboard and should have the following parameters:<br>1. Top attacks<br>2. Top Source/Destination IPs.<br>3. Top Targets<br>4. Device Health | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 6. CPU Utilization<br>7. Throughput Utilization<br>8. Top Attack Category/ Subcategory<br>9. Top Application | | |
| 72. | The proposed solution must support integration with all leading SIEM solution. | | |
| 73. | i. Proposed solution should capability to integrate with leading Identity access management tools<br>ii. The proposed solution should support TACACS+ and radius natively for authentication, authorization and accounting. | | |

## 12.8. Type-2 Intrusion Prevention System (IPS) (40 Gbps)

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **Platform Requirement** | | |
| 2. | Make:<br>Model No: | | |
| 3. | The IPS solution must be a purpose-built dedicated appliance (not a subset of firewall or UTM appliance and its firmware should be dedicated firmware and should not be same or shared with any other blades i:e: Firewall, DDoS, UTM Etc. The solution should not use the same firmware/underlying OS for Next Generation Firewall AND/OR IPS offering. | | |
| 4. | The proposed solution must have separate dedicated interface for management | | |
| 5. | The proposed solution must have inbuilt internal Redundant Power Supply (RPS). | | |
| 6. | The proposed solution should be able to support the inbound and outbound TLS/SSL decryption for traffic inspection and attack identification | | |
| 7. | **Performance requirement** | | |
| 8. | 1. The Proposed solution must have below hardware requirements | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
|  | 2. The proposed solution must have minimum inspected throughput of 40 Gbps for all kinds of real-world traffic.<br>3. The proposed solution must be support minimum SSL throughput-20 Gbps.<br>4. The proposed solution should have SSL connection per second: Minimum 10K<br>5. The proposed solution must have New Connections Per Second: Minimum 1M<br>6. The proposed solution must have Concurrent Connection: Minimum 30M<br>7. The proposed solution must be supported minimum ACL-1800.<br>8. The proposed solution must have minimum 8x10G SFP Ports+ 4X40G/100G ports.<br>9. All ports should be bypass mode. Bypass mode port should not be included in these ports. These ports will be used for traffic only.<br>10. The proposed solution, which acts as transparent device to the network have a fail open feature in all port.<br>11. When IPS transparent device goes down, traffic does not stop.<br>12. If the device does not have fail open feature in built, then they facilitate bypass/fail open kit to achieve the functionality.<br>13. The proposed solution should offer traffic bypassing capability on the provided inbuilt interfaces i.e. in case of power and/or HW failure the traffic should be able to flow without interruption from the respective interfaces<br>14. The proposed solution must have 1GxManagement Interface & RJ-45 Serial Console Port<br>15. The proposed solution must have Redundant Power Supply<br>16. The proposed solution Latency must be < 60 microseconds<br>17. The proposed solution must be Rack mountable<br>18. The proposed solution must have 20,000 IPS signatures.<br>19. Bidder has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. |  |  |
| 9. | **Features** |  |  |
| 10. | The proposed solution must accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, |  |  |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | suspicious activity, DoS, DDoS, vulnerability exploitation, , crypto-mining brute force, L3 to L7 attacks and zero-day attacks . | | |
| 11. | The proposed solution must use prevention techniques and provide zero-day protection against Worms, Trojans, Spyware, Key Loggers, and other malware from penetrating the network. | | |
| 12. | 1. The proposed solution must perform traffic inspection based on Signatures, Protocol anomaly, Behaviour anomaly, Reputation (IP and URL).<br>2. The Proposed solution must support following deployment Modes.<br>f) IDS<br>g) SPAN<br>h) Inline<br>i) L2<br>j) Bridge | | |
| 13. | The proposed solution must accurately detect the following attack categories:- Malformed traffic, Invalid Headers, DoS, Vulnerability exploitation, Zero-day and unknown attacks – | | |
| 14. | The proposed solution must support IP(IPv4 and IPv6), URLs, Hashes and file reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist | | |
| 15. | The offered IPS solution should be able to integrate with the on-premise zero day(sandboxing) solution of the same OEM | | |
| 16. | 1. The proposed solution must support vulnerability based and exploit based signatures.<br>2. It must detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability) | | |
| 17. | The device must handle following traffic inspection and support: IPv6, IPv4, MPLS, Tunnelled, The proposed solution should also support IPv4 to IPv6 and IPv6 to IPv4, IPv6 to IPv6,IPv4 to IPv4 communication, | | |
| 18. | The proposed solution must support Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 19. | a) The proposed solution must be capable to support protection against Client side attacks,<br>b) The proposed solution must be capable to support protection for both IPv4 & IPv6 simultaneously. Dual-stack or native dual-stack IP implementations provide complete IPv4 and IPv6 protocol stacks in the same network node and native communications can be done between nodes using either protocol,<br>c) The proposed solution must be capable to support zero day botnet protection.<br>d) The proposed solution must be capable to protect against DoS/DDoS attacks,<br>e) The proposed solution must be capable to inspect DNS response packets for blacklisted domains, Malware scan on HTTP, FTP and SMTP protocols.<br>f) The proposed solution OEM must have its own threat intelligence analysis centre, and shall share threat intelligence with NIC regularly. | | |
| 20. | The proposed solution must capable to protect application anomalies, P2P attacks, TCP segmentation and IP fragmentation. | | |
| 21. | 1. The proposed solution must be capable to perform entire packet capture of the traffic for analysis. (e.g. for capturing the traffic between two IP address for a specific period),<br>2. The proposed solution must be capable to support NTP ( Network Time Protocol),<br>3. The solution must have Capability to restrict access of URL/IP based on Geo-location (County), | | |
| 22. | The proposed solution should provide protection with security engines like anomaly detection /behavioural based, anti-scan and should have rate based, pattern based, vulnerability based, exploit based prevention capabilities and support for custom defined signatures | | |
| 23. | The proposed solution should also ensure defense against all types of encrypted attacks, exploits and vulnerabilities. | | |
| 24. | The proposed solution should have capability to protect based on Rate-based threats, Statistical anomalies | | |
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 26. | The Proposed solution must prevent SSL protocol-based attacks | | |
| 27. | The proposed solution must Protect against IPv6 based attacks | | |
| 28. | The proposed solution must support block attacks based on IP reputation, DNS Inspection, Geo-location, URL Inspection. | | |
| 29. | The proposed solution should support file reputation/type on the basis of application protocol including http, https, FTP, SMB (no file must be sent to Cloud) | | |
| 30. | The proposed solution should be intuitive and provide most of the features through the GUI only including enabling the XFF to identify the true-client IP | | |
| 31. | a) The proposed solution must be capable of signature-less intrusion detection technology allowing the IPS to identify network traffic and stops zero-day attacks for which no signatures exist.<br>b) The proposed solution should have the capability to enable/disable each individual signature for specific source and destination. | | |
| 32. | The proposed solution must have the ability to block connection to or from outside network based on the reputation of the IP address that is trying to communicate with the network | | |
| 33. | a) The proposed solution must protect against vulnerability in Web applications, Databases.<br>b) The Proposed solution must have features for time-based security policies like Geo-location, white list and blacklist.<br>c) The proposed solution should also have source IP quarantine feature. | | |
| 34. | The proposed solution must protect against DOS attacks based on: | | |
| 35. | Heuristic-based detection | | |
| 36. | Must have the feature for creating user-defined signature. | | |
| 37. | Must have the feature for importing SNORT signatures. | | |
| 38. | a) The proposed solution OEM must have its own threat intelligence analysis center.<br>b) The proposed solution must have features to search signature-based CVE IDs. | | |
| 39. | Prevention and Response | | |
| 40. | The proposed solution must support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done and its logging. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 41. | The proposed  solution must support a wide range of response actions such<br>i) Drop<br>j) Block<br>k) Allow<br>l) Reject<br>m) Quarantine<br>n) Trace/Packet Capture<br>o) Rate limit<br>p) Log traffic/monitor traffic | | |
| 42. | 1. The proposed solution shall provide source reputation-based analysis.<br>2. The proposed solution must support source lookup for IP and domain reputation. | | |
| 43. | The proposed solution must support following capabilities of packet capture, from particular source, destination and protocol through GUI. Email alert, SNMP alert, Syslog alert | | |
| 44. | The proposed solution should ensure defence against all types of encrypted attacks by inspecting and blocking malicious SSL traffic from day-one. | | |
| 45. | The offered product capable to protect- Web applications, Web 2.0, Databases, Network and Security Devices. | | |
| 46. | Policy Configuration | | |
| 47. | The proposed  solution should  have facility to exempt IPS inspection for a particular signature based on- Source or Destination IP/Subnet, Between two IP/subnet | | |
| 48. | 1. The proposed solution should have facility to enable/disable each individual signature. Each signature to allow granular tuning,<br>2. The proposed  solution should  be capable to support granular management and allow policy to be assigned per device, port, VLAN tag, IP address/range,<br>3. The proposed  solution should   have facility to exempt a particular IP/Subnet from IPS inspection and generate logs for this particular activity | | |
| 49. | The solution must be capable of mapping IP addresses to username, and making this information available for event management purposes. | | |
| 50. | The proposed solution must support authenticated NTP synchronization. | | |
| 51. | **Central Management** | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 52. | 1) The proposed solution should be provided and deployed with a separate / dedicated Appliance in HA for IPS Management and Log Analysis with all the required licenses for monitoring, reporting etc.<br>2) The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3) The proposed Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>4) The proposed solution must have the capability to manage minimum 50 pairs of IPS devices and adequate licenses for managing these IPS must be supplied from Day 1.<br>5) The proposed solution should have access through GUI and user management must be based on RBAC.<br>6) The proposed solution must have integrated security architecture with multi-tenancy, analytics, Logging and must have API access for enhanced automation capabilities.<br>7) The proposed solution should support API for automation. | | |
| 53. | The proposed solution must be accessible over secure channel. | | |
| 54. | **Role based administration :-** | | |
| 55. | The proposed solution must facilitate administrator to manage multiple IPS devices over network. | | |
| 56. | The proposed solution must support multiple roles like administrator, operator etc. | | |
| 57. | The proposed solution must support to remote administration of individual IPS devices from specific IP addresses / subnets / user id's only. | | |
| 58. | The proposed solution must support audit log facility. | | |
| 59. | The proposed solution must support export / import of configuration files for each IPS device. | | |
| 60. | The proposed solution must support updation of IPS signatures on the IPS devices from the centralized management solution. | | |
| 61. | The proposed solution must update its attack signature database regularly on management solution and it must be configurable to update the signatures automatically without manual intervention. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 62. | The proposed solution must notify automatically through e-mail/displayed in manager window about the availability of new signatures and new product releases. | | |
| 63. | The proposed solution must make new attack signatures and new major software releases available for download from its Web site. | | |
| 64. | The proposed solution must support centralized performance/Health monitoring of IPS devices. | | |
| 65. | The proposed solution must have the facility to display:- Real-time Log and Historical log for a given period | | |
| 66. | The proposed solution must support a wide variety of pre-built as well as custom reports. | | |
| 67. | The proposed solution must be able to output report data into a variety of different file formats like HTML, PDF etc. | | |
| 68. | 1. The proposed solution must support auto-email of pre-defined and customized reports at a scheduled time.<br>2. The proposed solution should be able to send the notifications to management console, remote syslog and email once the signature is triggered | | |
| 69. | The proposed solution must support the archiving and backup of events. | | |
| 70. | The proposed solution must support policy configuration and event management functions for the IPS appliances. | | |
| 71. | The proposed solution should have real-time Dashboard and should have the following parameters:<br>1. Top attacks<br>2. Top Source/Destination IPs.<br>3. Top Targets<br>4. Device Health<br>6. CPU Utilization<br>7. Throughput Utilization<br>8. Top Attack Category/ Subcategory<br>9. Top Application | | |
| 72. | The proposed solution must support integration with all leading SIEM solution. | | |
| 73. | i. Proposed solution should capability to integrate with leading Identity access management tools | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | ii. The proposed solution should support TACACS+ and radius natively for authentication, authorization and accounting. | | |

### 12.9. Type-3 Intrusion Prevention System (IPS) (100 Gbps)

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **Platform Requirement** | | |
| 2. | Make:<br>Model No: | | |
| 3. | The IPS solution must be a purpose-built dedicated appliance (not a subset of firewall or UTM appliance and its firmware should be dedicated firmware and should not be same or shared with any other blades i.e.: Firewall, DDoS, UTM Etc. The solution should not use the same firmware/underlying OS for Next Generation Firewall AND/OR IPS offering. | | |
| 4. | The proposed solution must have separate dedicated interface for management | | |
| 5. | The proposed solution must have inbuilt internal Redundant Power Supply (RPS). | | |
| 6. | The proposed solution should be able to support the inbound and outbound TLS/SSL decryption for traffic inspection and attack identification | | |
| 7. | **Performance requirement** | | |
| 8. | 1. The Proposed solution must have below hardware requirements<br>2. The proposed solution must have minimum inspected throughput of 100 Gbps for all kinds of real-world traffic.<br>3. The proposed solution must be support minimum SSL throughput-40 Gbps. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 4. The proposed solution should have SSL connection per second: Minimum 10K<br>5. The proposed solution must have New Connections Per Second: Minimum 1M<br>6. The proposed solution must have Concurrent Connection: Minimum 50M<br>7. The proposed solution must be supported minimum ACL-1800.<br>8. The proposed solution must have minimum 8x10G SFP Ports+ 4X40G/100G ports.<br>9. All ports should be bypass mode. Bypass mode port should not be included in these ports. These ports will be used for traffic only.<br>10. The proposed solution, which acts as transparent device to the network have a fail open feature in all port.<br>11. When IPS transparent device goes down, traffic does not stop.<br>12. If the device does not have fail open feature in built, then they facilitate bypass/fail open kit to achieve the functionality.<br>13. The proposed solution should offer traffic bypassing capability on the provided inbuilt interfaces i.e. in case of power and/or HW failure the traffic should be able to flow without interruption from the respective interfaces<br>14. The proposed solution must have 1GxManagement Interface & RJ-45 Serial Console Port<br>15. The proposed solution must have Redundant Power Supply<br>16. The proposed solution Latency must be < 60 microseconds<br>17. The proposed solution must be Rack mountable<br>18. The proposed solution must have 20,000 IPS signatures.<br>19. Bidder has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| 9. | **Features** | | |
| 10. | The proposed solution must accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, , crypto-mining brute force, L3 to L7 attacks and zero-day attacks . | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 11. | The proposed solution must use prevention techniques and provide zero-day protection against Worms, Trojans, Spyware, Key Loggers, and other malware from penetrating the network. | | |
| 12. | 1. The proposed solution must perform traffic inspection based on Signatures, Protocol anomaly, Behaviour anomaly, Reputation (IP and URL).<br>2. The Proposed solution must support following deployment Modes.<br>k) IDS<br>l) SPAN<br>m) Inline<br>n) L2<br>o) Bridge | | |
| 13. | The proposed solution must accurately detect the following attack categories:- Malformed traffic, Invalid Headers, DoS, Vulnerability exploitation, Zero-day and unknown attacks – | | |
| 14. | The proposed solution must support IP(IPv4 and IPv6), URLs ,Hashes and file reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist | | |
| 15. | The offered IPS solution should be able to integrate with the on-premise zero day(sandboxing) solution of the same OEM | | |
| 16. | 1. The proposed solution must support vulnerability based and exploit based signatures.<br>2. It must detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability) | | |
| 17. | The device must handle following traffic inspection and support: IPv6, IPv4, MPLS, Tunnelled, The proposed solution should also support IPv4 to IPv6 and IPv6 to IPv4, IPv6 to IPv6,IPv4 to IPv4 communication, | | |
| 18. | The proposed solution must support Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection | | |
| 19. | a) The proposed solution must be capable to support protection against Client side attacks, | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | b) The proposed solution must be capable to support protection for both IPv4 & IPv6 simultaneously. Dual-stack or native dual-stack IP implementations provide complete IPv4 and IPv6 protocol stacks in the same network node and native communications can be done between nodes using either protocol,<br>c) The proposed solution must be capable to support zero day botnet protection.<br>d) The proposed solution must be  capable to protect against DoS/DDoS attacks,<br>e) The proposed solution must be capable to inspect DNS response packets for blacklisted domains, Malware scan on HTTP, FTP and SMTP protocols.<br>f) The proposed solution OEM must have its own threat intelligence analysis centre, and shall share threat intelligence with NIC regularly. | | |
| 20. | The proposed solution must capable to protect application anomalies, P2P attacks, TCP segmentation and IP fragmentation. | | |
| 21. | 1. The proposed solution must be capable to perform entire packet capture of the traffic for analysis. (e.g. for capturing the traffic between two IP address for a specific period),<br>2. The proposed solution must be  capable to support NTP ( Network Time Protocol),<br>3. The solution must have Capability to restrict access of URL/IP based on Geo-location (County), | | |
| 22. | The proposed  solution should provide protection with security engines like anomaly detection /behavioural based, anti-scan and should have rate based, pattern based, vulnerability based, exploit based prevention capabilities and support for custom defined signatures | | |
| 23. | The proposed solution should also ensure defense against all types of encrypted attacks, exploits and vulnerabilities. | | |
| 24. | The proposed  solution should  have capability to protect based on Rate-based threats, Statistical anomalies | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface. | | |
| 26. | The Proposed solution must prevent SSL protocol-based attacks | | |
| 27. | The proposed solution must Protect against IPv6 based attacks | | |
| 28. | The proposed solution must support block attacks based on IP reputation, DNS Inspection, Geo-location, URL Inspection. | | |
| 29. | The proposed solution should support file reputation/type on the basis of application protocol including http, https, FTP, SMB (no file must be sent to Cloud) | | |
| 30. | The proposed solution should be intuitive and provide most of the features through the GUI only including enabling the XFF to identify the true-client IP | | |
| 31. | a) The proposed solution must be capable of signature-less intrusion detection technology allowing the IPS to identify network traffic and stops zero-day attacks for which no signatures exist.<br>b) The proposed solution should have the capability to enable/disable each individual signature for specific source and destination. | | |
| 32. | The proposed solution must have the ability to block connection to or from outside network based on the reputation of the IP address that is trying to communicate with the network | | |
| 33. | a) The proposed solution must protect against vulnerability in Web applications, Databases.<br>b) The Proposed solution must have features for time-based security policies like Geo-location, white list and blacklist.<br>c) The proposed solution should also have source IP quarantine feature. | | |
| 34. | The proposed solution must protect against DOS attacks based on: | | |
| 35. | Heuristic-based detection | | |
| 36. | Must have the feature for creating user-defined signature. | | |
| 37. | Must have the feature for importing SNORT signatures. | | |
| 38. | a) The proposed solution OEM must have its own threat intelligence analysis center.<br>b) The proposed solution must have features to search signature-based CVE IDs. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 39. | Prevention and Response | | |
| 40. | The proposed solution must support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done and its logging. | | |
| 41. | The proposed solution must support a wide range of response actions such<br>a) Drop<br>b) Block<br>c) Allow<br>d) Reject<br>e) Quarantine<br>f) Trace/Packet Capture<br>g) Rate limit<br>h) Log traffic/monitor traffic | | |
| 42. | 1. The proposed solution shall provide source reputation-based analysis.<br>2. The proposed solution must support source lookup for IP and domain reputation. | | |
| 43. | The proposed solution must support following capabilities of packet capture, from particular source, destination and protocol through GUI. Email alert, SNMP alert, Syslog alert | | |
| 44. | The proposed solution should ensure defence against all types of encrypted attacks by inspecting and blocking malicious SSL traffic from day-one. | | |
| 45. | The offered product capable to protect- Web applications, Web 2.0, Databases, Network and Security Devices. | | |
| 46. | Policy Configuration | | |
| 47. | The proposed solution should have facility to exempt IPS inspection for a particular signature based on- Source or Destination IP/Subnet, Between two IP/subnet | | |
| 48. | 1. The proposed solution should have facility to enable/disable each individual signature. Each signature to allow granular tuning,<br>2. The proposed solution should be capable to support granular management and allow policy to be assigned per device, port, VLAN tag, IP address/range, | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
|  | 3. The proposed  solution should   have facility to exempt a particular IP/Subnet from IPS inspection and generate logs for this particular activity |  |  |
| 49. | The solution must be capable of mapping IP addresses to username, and making this information available for event management purposes. |  |  |
| 50. | The proposed solution must support authenticated NTP synchronization. |  |  |
| 51. | **Central Management** |  |  |
| 52. | 1) The proposed solution should be provided and deployed with a separate / dedicated Appliance in HA for IPS Management and Log Analysis with all the required licenses for monitoring, reporting etc.<br>2) The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3) The proposed Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>4) The proposed solution must have the capability to manage minimum 50 pairs of IPS devices and adequate licenses for managing these IPS must be supplied from Day 1.<br>5) The proposed solution should have access through GUI and user management must be based on RBAC.<br>6) The proposed solution must have integrated security architecture with multi-tenancy, analytics, Logging and must have API access for enhanced automation capabilities.<br>7) The proposed solution should support API for automation. |  |  |
| 53. | The proposed solution must be accessible over secure channel. |  |  |
| 54. | **Role based administration :-** |  |  |
| 55. | The proposed solution must facilitate administrator to manage multiple IPS devices over network. |  |  |
| 56. | The proposed solution must support multiple roles like administrator, operator etc. |  |  |
| 57. | The proposed solution must support to remote administration of individual IPS devices from specific IP addresses / subnets / user id's only. |  |  |
| 58. | The proposed solution must support audit log facility. |  |  |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 59. | The proposed solution must support export / import of configuration files for each IPS device. | | |
| 60. | The proposed solution must support updation of IPS signatures on the IPS devices from the centralized management solution. | | |
| 61. | The proposed solution must update its attack signature database regularly on management solution and it must be configurable to update the signatures automatically without manual intervention. | | |
| 62. | The proposed solution must notify automatically through e-mail/displayed in manager window about the availability of new signatures and new product releases. | | |
| 63. | The proposed solution must make new attack signatures and new major software releases available for download from its Web site. | | |
| 64. | The proposed solution must support centralized performance/Health monitoring of IPS devices. | | |
| 65. | The proposed solution must have the facility to display:- Real-time Log and Historical log for a given period | | |
| 66. | The proposed solution must support a wide variety of pre-built as well as custom reports. | | |
| 67. | The proposed solution must be able to output report data into a variety of different file formats like HTML, PDF etc. | | |
| 68. | 1. The proposed solution must support auto-email of pre-defined and customized reports at a scheduled time.<br>2. The proposed solution should be able to send the notifications to management console, remote syslog and email once the signature is triggered | | |
| 69. | The proposed solution must support the archiving and backup of events. | | |
| 70. | The proposed solution must support policy configuration and event management functions for the IPS appliances. | | |
| 71. | The proposed solution should have real-time Dashboard and should have the following parameters :<br>1. Top attacks<br>2. Top Source/Destination IPs.<br>3. Top Targets | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
|  | 4. Device Health<br>6. CPU Utilization<br>7. Throughput Utilization<br>8. Top Attack Category/ Sub Category<br>9. Top Application |  |  |
| 72. | The proposed solution must support integration with all leading SIEM solution. |  |  |
| 73. | i. Proposed solution should capability to integrate with leading Identity access management tools<br>ii. The proposed solution should support TACACS+ and radius natively for authentication, authorization and accounting. |  |  |

## 12.10. Anti-APT Solution

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| **1.** | Make:<br>Model No: |  |  |
| **2.** | The proposed Anti-Advanced Persistent Threat Solution should be a dedicated purpose built platform deployed independently without any functional reliance on existing layers of security like NGFW, NGIPS, UTM ,Proxy etc adhering to defense in depth architecture, where, If any of the layers of core underlying security get replaced or non-functional, the proposed solution must be capable to function on its own. |  |  |
| **3.** | a) The proposed solution should be able to inspect multi-protocol sessions to detect and flag suspicious activity including file downloads through the web, mail attachments and internal infections.<br>b) It should not have any port-based restrictions and should support all ports. |  |  |
| **4.** | The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files, Flash files, RTF files and/or other objects without relying upon any other 3rd party solutions |  |  |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| **5.** | The proposed solution should have event detection capabilities that should include malware type/ severity, source and destination of attack and the history of the movement of the malware in the network. | | |
| **6.** | Performance Parameters:<br>a) Proposed solution should have real world Network Throughput: Minimum 20 Gbps<br>b) Proposed solution should have minimum 4X10G Interface ports.<br>c) Proposed solution should have minimum 2x40G/100G Interface ports<br>d) Proposed solution should have capability Minimum File size to process: 100MB<br>e) Proposed solution should have capability Files Per Hour Processing : Minimum 2000<br>f) Proposed solution should have parallel running of sandbox guest operating system VMs : Minimum 50<br>g) Proposed solution must support analysis of minimum 100+ different file types, including portable executable (PEs), active web content, archives, images, Java, Microsoft and Adobe applications and multimedia etc. with a proven capability to analyse network session flows and Server O.S file types. At the minimum file types like 3gp, 7zip, a3x, ace, acrobat security settings, ahk, alz, apk, app, applet, arj, asf, au3,avi, bat, bz2, cab, cdf, chm, cmd, com, com1, csv, dll, dmg, doc, docm, docx, dual(multiple extensions), dylib, eeml, eg, ehdr, elf, eml, empty, exe, fdf, flv, gen, gif, gz,hlp, hml, hta, htm, hwp, hwt, ico, jar, jpeg, jpg, js, jsp, jtd, lnk, lzh, mach-o, mht, mhtml, midi, mov, mp3, mp4, mpg, mpkg, msg, msi, mso, one, pdf, php, pkg, pl, png, pps, ppsx, ppt, pptx, ps1, pub, py, qt, rar, rb, rm, rmi, rtf, scf, sct, sh, swf, tiff, tnef, unk, url, url-applet, uue, vbs, vcf, vcs, wav, war, wma, wsf, xdp, xls, xlsx, xml, xor, xps, xsl, zip, RunELF, PHP Webshell, JSP Webshell, WAR Webshell, RunScript, : LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg/.iso, .dll, .sys/.wsf, .com and .hwp Python 2.7 , elf and shell scripts (.sh/py/pl at a minimum) etc with capabilities like code analysis, that includes function, entropy and similarity analysis of Files, URL's, Objects, network flows, scripts. must be supported. | | |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | h) The proposed solution/ models should include any additional ports and subcomponents necessary to support the specified throughput requirements of the Purchaser | | |
| **7.** | 1. The proposed solution must detect zero-day, multi-stage, fileless and other evasive advanced attacks using dynamic, signature-less analysis in a safe, anti-evasive execution environment.<br>2. The Proposed solution should be sized appropriately by the bidder including all other costs required for performance, scalability and efficiency. | | |
| **8.** | a) The Proposed solution should detect suspicious files uploaded to web servers through HTTP- POST and FTP protocols and provide mapping of methodology & alert techniques to MITRE ATT&CK framework.<br>b) The proposed solution should also detect attempted data exfiltration, beaconing including other advanced techniques. | | |
| **9.** | The proposed solution should be deployed on premise along with on premise sandbox capability. | | |
| **10.** | **Central Management Solution** | | |
| **11.** | 1. The proposed solution should be provided with a separate / dedicated Appliance in HA for Anti-APT Management and Log Analysis with all the required licenses for monitoring, reporting etc.<br>2. The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>4. The proposed solution must have the capability to manage minimum 50 Anti APT solution and adequate licenses for managing these APTs must be supplied from Day 1.<br>5. The proposed solution should have access through GUI and user management must be based on RBAC.<br>6. The proposed solution should API for automation. | | |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| **12.** | Bidders are required to provide integrated security threat intel content as part of the solution, without requirement to send any analysis or data to cloud for analysis or decisions. Threat intel must be proposed in non-sharing mode. | | |
| **13.** | The Proposed appliance must support SSL inspection on-board. If Solution does not have SSL decryption feature, they may propose an enterprise grade SSL decryption tool along with their offering. | | |
| **14.** | The proposed solution must have analysis engine must support micro tasking within Dynamic Analysis Operating System VM's (Windows & Linux environments), such as analysis using different versions and service packs of operating systems and different versions of applications (Adobe PDF, MS Word and etc) by performing the analysis in parallel (i.e. To use multiple virtual machines in parallel) with all licenses and dependencies included in the platform. | | |
| **15.** | The proposed solution must have capability to identify malicious exploits, malware, phishing attacks and command and control (CnC) call back while extracting and submitting suspicious network traffic to the dynamic analysis engine for a definitive verdict analysis. | | |
| **16.** | The proposed solution must support server side detections, lateral movement detection and detection on post-exploitation traffic | | |
| **17.** | The proposed solution must be capable of protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, cryptominers etc | | |
| **18.** | The proposed solution should have the capability to store the complete file (if the file is identified as malware or its current state cannot be determined) and its associated artefacts. | | |
| **19.** | The proposed solution should be able to store packet captures (PCAP) that are associated with specified detections such as Malicious communications/ ransomware. | | |
| **20.** | The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP address of a host in a proxy environment. | | |
| **21.** | The proposed solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack. | | |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| **22.** | The proposed solution should be able to support up to 3 network segments for in and out traffic on a single appliance | | |
| **23.** | The proposed solution should be able to detect and block communications to known command and control servers and detect reputation of URL being accessed. | | |
| **24.** | The proposed solution should be able to identify and understand the severity and stage of each attack. | | |
| **25.** | The proposed solution must support communication over the IPv6 protocol on the management interface. | | |
| **26.** | The proposed solution should have built in capabilities to add exceptions for detections and have capabilities to configure files/ IP, URLs and domains to blacklist or whitelist. | | |
| **27.** | The proposed solution must provide a web service interface/API for end users to customize integration. | | |
| **28.** | The proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, filenames, process names, windows registry entries, file hashes, malware detections and malware families through a portal. | | |
| **29.** | The proposed solution should support SIEM integration using varied methods like open standards/API/Syslog/CEF/LEEF etc. | | |
| **30.** | The proposed solution should have capability of horizontal scalability. | | |
| **31.** | The proposed solution should support HTTP, HTTPS, SMTP, SMTP CIFS, FTP and other protocols | | |
| **32.** | The proposed solution should support all major protocols on Single Sandbox appliance. | | |
| **33.** | The proposed solution should have an option to deploy in ‘fail open’ mode in any case of any device failure | | |
| **34.** | The proposed solution should have a combination of static and dynamic analysis techniques to unmask cleverly disguised malware. | | |
| **35.** | The proposed solution should have the ability to block all outbound call-back communication initiated by the internal clients (infected) or also within Sandbox environment. | | |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 36. | The proposed solution should be able to give user notification over Email, Web and support customization of user notification. | | |
| 37. | a) The proposed solution should be able to provide a customized or a purpose-built sandbox environment for execution analysis of files, objects, flows, attachments, URLs etc.<br>b) The Sandbox must support multiple operating systems for both 32-bits and 64-bits OS and should support multiple version of OS to have the ability to simulate the entire threat behaviour | | |
| 38. | The proposed solution should have provision to identify entry point of malware. | | |
| 39. | The proposed solution should have grayware detection capabilities and should detect network attacks and exploits. | | |
| 40. | The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation. | | |
| 41. | The proposed solution has the capability to perform tracking and analysis of virus downloads and suspicious files. | | |
| 42. | The proposed solution should have capabilities to scan inside archives. | | |
| 43. | The proposed solution should have capabilities to detect malwares and spywares on windows and non-windows platforms and have capabilities to detect and mitigate Linux malwares. | | |
| 44. | The proposed solution should be able to detect known malwares/threats and known bad URLs based on various engines before sending suspicious files to Sandbox for analysis. | | |
| 45. | The proposed solution must be able to quarantine/clean infected files once it is determined to be malicious. | | |
| 46. | The proposed solution should have an automated incident analysis function that provides a comprehensive view of attack flow, root cause, business impact, and entry point to enable accelerated remediation | | |
| 47. | The proposed solution should support forensics analysis of malicious files. | | |
| 48. | The proposed solution should not require users to specify the operating system and application used during the analysis. The solution proposed should offer the | | |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
|  | necessary intelligence to provide the right environment to draw out the malware behaviour based on the file telemetry information. |  |  |
| 49. | The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like Sandbox detection, Blacklist and license events etc. |  |  |
| 50. | The proposed solution should also support IPv4 to IPv6,IPv6 to IPv4,IPv6 to IPv6,IPv4 to IPv4 communication |  |  |
| 51. | The proposed Anti-APT solution should be deployable in inline mode. |  |  |
| 52. | The proposed solution should detect and analyse the URL which is pointed from a file or any other source. |  |  |
| 53. | The Proposed solution should be able to Identify suspicious embedded object in document file like OLE, Macro extraction, Shell code and exploit matching. |  |  |
| 54. | The proposed solution should be able to detect if file has suspicious attributes like True-file type and Naming trick. |  |  |
| 55. | The proposed solution should block and hold/quarantine file from spreading across all endpoints i.e., prevent lateral movement natively or by using endpoint security solution |  |  |
| 56. | The proposed solution should utilize multiple machine learning, AI and correlation engines represent a collection of contextual, dynamic rules engines that detects and blocks malicious activity in real-time / retroactively, based on the latest machine-, attacker- and victim- intelligence. |  |  |
| 57. | a) The proposed solution should support CLI and must be administered through a web-based console using SSH/HTTPS.<br>b) The proposed solution should support AAA for role-based administration |  |  |
| 58. | The proposed solution should have feasibility to receive Threat feeds/Updates from OEM cloud. |  |  |
| 59. | The proposed solution should have an intuitive Dashboard that offers real time threat visibility and attack characteristics. |  |  |
| 60. | The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats. |  |  |

| Sr.no | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 61. | The proposed solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time). | | |
| 62. | The proposed solution should support logging of important parameters like source IP, destination IP, ports, protocol, domain, time stamp etc. of the attacks sessions. | | |
| 63. | The proposed solution should have the flexibility to provide customizable dashboard. | | |
| 64. | The proposed solution should have the option to provide an investigative dashboard that is capable of displaying graphical data that is based on link-graph, geo-map, chart, tree-map / pivot table. | | |
| 65. | The proposed solution should be able to provide in-depth reporting including the level of risk, sandbox assessment, and network activity analysis. | | |
| 66. | The proposed solution must be able to provide intelligence via a portal for malware information, threat profile, source, destination, and user where applicable. | | |
| 67. | The proposed solution should be able to generate out of box reports to highlight infections, C&C behaviour and lateral Movement. | | |
| 68. | The proposed solution shall support local password and Radius/ Active Directory (AD)/ TACACS+ for authentication schemes | | |
| 69. | The OEM should have a local TAC Centre in India for support for faster replacements. | | |
| 70. | The proposed solution should address known/unknown malwares using multi layered security methodology and should not be only dependent on Sandboxing. | | |
| 71. | The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing. | | |
| 72. | The proposed solution should be able to provide details of files with very low prevalence, Footprint (Identification of system, IP’s and user machines) of a given file and provide detailed file execution report for all sandbox detections. | | |

### 12.11. Type 1 SSL Off loader (40 Gbps)

| Sr No | Minimum Specification | Compliance (Yes/No) | Reference Document/Page no |
|---|---|---|---|
| 1. | Make:<br>Model No: | | |
| 2. | The Proposed solution must be deployed in Inline, Inbound layer 3 Reverse Proxy, Forward proxy, Transparent mode or L2 Mode, High availability with TCP session resiliency with latest cipher TLS 1.3 support with full key length. | | |
| 3. | The proposed solution must support robust cipher and protocol i.e. TLS1.1,1.2,1.3, RSA, DHE, ECDHE with forward secrecy SHA, SHA2, AES, AES-GCM and proxy level control over ciphers and protocols. | | |
| 4. | The proposed solution must have capability to intercept SSL traffic for inbound and outbound layer 3 explicit proxy, outbound layer 3 transparent proxy. | | |
| 5. | The Proposed solution must support VLAN. | | |
| 6. | The Proposed solution must support SSL/TLS decryption independent of standard TCP port. | | |
| 7. | The Proposed solution should provide a one-box solution for high-performance visibility into SSL/TLS traffic and must be able to feed multiple devices with a single decryption stream in sequence as a service chain. | | |
| 8. | **Performance Parameter** | | |
| 9. | 1. The Proposed solution must support minimum 80,000 Connections/Transactions Per Second on RSA - 2048 Bit Key size<br>2. The Proposed solution must support minimum 50,000 Connections/Transactions per second on ECC/TLS1.3<br>3. The Proposed solution must have minimum 40 Gbps of SSL throughput.<br>4. The Proposed solution must have minimum 8x10G ports and 2x40/100G" ports from Day 1.<br>5. The Proposed solution must be fully populated in all respects like memory, ports, storage etc. | | |

| Sr No | Minimum Specification | Compliance (Yes/No) | Reference Document/Page no |
|---|---|---|---|
|  | MSP has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. |  |  |
| 10. | The Proposed solution must support virtualization on same hardware. |  |  |
| 11. | The proposed solution should have minimum latency. |  |  |
| 12. | 1. The Proposed solution must transparently intercepts and decrypts SSL/TLS traffic and must have ability to service chain dynamically.<br>2. The proposed solution should decrypt in the SSL traffic and send specific decrypted traffic to selective security solutions as defined.<br>3. The proposed solutions should have the ability to insert or delete security solutions in the service chain. |  |  |
| 13. | The Proposed SSL Visibility solution should monitor the availability (for those security solution that have a service health monitor) and should automatically remove the unavailable security solution from the service chain. |  |  |
| 14. | The Proposed solution should be capable to load balance traffic between security devices and Selective bypass of security device in case of failure. |  |  |
| 15. | The Proposed solution must support policy-based steering of decrypted traffic, decoupled from physical interface, port or VLANs, service resiliency, service monitoring. |  |  |
| 16. | The Proposed solution must support High Availability in Active-Active/Active-Passive mode |  |  |
| 17. | The Proposed solution should be able to terminate SSL. |  |  |
| 18. | The Proposed solution must securely manage SSL certificate and keys. |  |  |
| 19. | The Proposed solution should support manually defined URL bypass list |  |  |
| 20. | The Proposed solution must support dual stack (IPv4 and IPv6). The proposed solution should also support IPv4 to IPv6, IPv6 to IPv4, IPv6 to IPv6, IPv4 to IPv4 communication |  |  |
| 21. | The Proposed solution should integrate with variety of security solutions from the leading vendors. |  |  |
| 22. | The Proposed solution should be able to control traffic based on customer defined policies. |  |  |
| 23. | **Central Management Solution** |  |  |

| Sr No | Minimum Specification | Compliance (Yes/No) | Reference Document/Page no |
|---|---|---|---|
| 24. | 1) The proposed solution should be provided with a separate / dedicated Appliance in HA for SSL offloader Management and Log Analysis with all the required licenses for monitoring, reporting etc.<br>2) The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3) The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>4) The proposed solution must have the capability to manage minimum 50 SSL Offloader and adequate licenses for managing these SSL Offloader must be supplied from Day 1.<br>5) The proposed solution should have access through GUI and user management must be based on RBAC.<br>6) The proposed solution should support API/ REST APIs/ Netconf/OpenConfig for automation. | | |
| 25. | The proposed solution must support communication over the IPv6 protocol on the management interface | | |
| 26. | The Proposed solution should support a CLI interface to carry out configuration and to focus on security parameters. | | |
| 27. | The Proposed solution should support SNMP Version 3 | | |
| 28. | The Proposed solution should support appropriate backup types. | | |
| 29. | The Proposed solution should support integration with existing infrastructure i.e. SIEM solution, Syslog etc. | | |
| 30. | The Proposed solution should support a GUI to carry out configuration and to focus on security parameters. | | |
| 31. | The Proposed solution must have out-of-band Management Port- RJ45. | | |
| 32. | The Proposed solution must support LDAP/RADIUS/TACACS for authentication and management of the device | | |
| 33. | The Proposed solution must support DUAL power supply. | | |

## 12.12. Type 2 SSL Off loader (90 Gbps)

| Sr No | Minimum Specification | Compliance (Yes/No) | Reference Document/Page no |
|---|---|---|---|
| 1. | Make:<br>Model No: | | |
| 2. | The Proposed solution must be deployed in Inline, Inbound layer 3 Reverse Proxy, Forward proxy, Transparent mode or L2 Mode, High availability with TCP session resiliency with latest cipher TLS 1.3 support with full key length. | | |
| 3. | The proposed solution must support robust cipher and protocol i.e. TLS1.1, 1.2, 1.3, RSA, DHE, ECDHE with forward secrecy SHA, SHA2, AES, AES-GCM and proxy level control over ciphers and protocols. | | |
| 4. | The proposed solution must have capability to intercept SSL traffic for inbound and outbound layer 3 explicit proxy, outbound layer 3 transparent proxy. | | |
| 5. | The Proposed solution must support VLAN. | | |
| 6. | The Proposed solution must support SSL/TLS decryption independent of standard TCP port. | | |
| 7. | The Proposed solution should provide a one-box solution for high-performance visibility into SSL/TLS traffic and must be able to feed multiple devices with a single decryption stream in sequence as a service chain. | | |
| 8. | **Performance Parameter** | | |
| 9. | 1. The Proposed solution must support minimum180K Connections/Transactions Per Second on RSA - 2048 Bit Key size<br>2. The Proposed solution must support minimum 120K Connections/Transactions per second on ECC/TLS1.3<br>3. The Proposed solution must have minimum 90 Gbps of SSL throughput.<br>4. The Proposed solution must have minimum 4x10G/25G ports and 4x40/100G" ports from Day 1.<br>5. The Proposed solution must be fully populated in all respects like memory, ports,storage etc. | | |

| Sr No | Minimum Specification | Compliance (Yes/No) | Reference Document/Page no |
|---|---|---|---|
| | MSP has to provide all transceivers SFPs, network cards, network slots as per above requirement from day-1 along with all the passive components like optical fibre cables, console cables, Cat 6 cables, Power cables as per NIC existing rack power units. | | |
| 10. | The Proposed solution must support virtualization on same hardware. | | |
| 11. | The proposed solution should have minimum latency. | | |
| 12. | 1. The Proposed solution must transparently intercepts and decrypts SSL/TLS traffic and must have ability to service chain dynamically.<br>2. The proposed solution should decrypt in the SSL traffic and send specific decrypted traffic to selective security solutions as defined.<br>3. The proposed solutions should have the ability to insert or delete security solutions in the service chain. | | |
| 13. | The Proposed SSL Visibility solution should monitor the availability (for those security solution that have a service health monitor) and should automatically remove the unavailable security solution from the service chain. | | |
| 14. | The Proposed solution should be capable to load balance traffic between security devices and Selective bypass of security device in case of failure. | | |
| 15. | The Proposed solution must support policy based steering of decrypted traffic, decoupled from physical interface, port or VLANs, service resiliency, service monitoring. | | |
| 16. | The Proposed solution must support High Availability in Active-Active/Active-Passive mode | | |
| 17. | The Proposed solution should be able to terminate SSL. | | |
| 18. | The Proposed solution must securely manage SSL certificate and keys. | | |
| 19. | The Proposed solution should  support manually defined URL bypass list | | |
| 20. | The Proposed solution must support dual stack (IPv4 and IPv6). The proposed solution should also support IPv4 to IPv6,IPv6 to IPv4,IPv6 to IPv6,IPv4 to IPv4 communication | | |
| 21. | The Proposed solution should integrate with variety of security solutions from the leading vendors. | | |
| 22. | The Proposed solution should be able to control traffic based on customer defined policies. | | |
| 23. | **Central Management Solution** | | |

| Sr No | Minimum Specification | Compliance (Yes/No) | Reference Document/Page no |
|---|---|---|---|
| 24. | 1) The proposed solution should be provided with a separate / dedicated Appliance in HA for SSL offloader Management and Log Analysis with all the required licenses for monitoring, reporting etc.<br>2) The proposed management solution should be either in Physical or Virtual Form Factor. In case of Virtual appliance then underlying infrastructure for deployment of virtual appliances must be provided.<br>3) The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>4) The proposed solution must have the capability to manage minimum 50 SSL Offloader and adequate licenses for managing these SSL Offloader must be supplied from Day 1.<br>5) The proposed solution should have access through GUI and user management must be based on RBAC.<br>6) The proposed solution should support API/ REST APIs/ Netconf/OpenConfig for automation. | | |
| 25. | The Proposed solution should support a CLI interface to carry out configuration and to focus on security parameters. | | |
| 26. | The Proposed solution should support SNMP Version 3 | | |
| 27. | The proposed solution must support communication over the IPv6 protocol on the management interface. | | |
| 28. | The Proposed solution should support appropriate backup types. | | |
| 29. | The Proposed solution should support integration with existing infrastructure i.e. SIEM solution, Syslog etc. | | |
| 30. | The Proposed solution should support a GUI to carry out configuration and to focus on security parameters. | | |
| 31. | The Proposed solution must have out-of-band Management Port- RJ45. | | |
| 32. | The Proposed solution must support LDAP/RADIUS/TACACS for authentication and management of the device | | |
| 33. | The Proposed solution must support DUAL power supply. | | |

## 13. Annexure: Technical Specifications of Software

### 13.1. Privileged Access Management

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | The proposed solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices. | | |
| 2. | The proposed solution should have a generic target system connector to enable one to use this connector for non-standard devices etc. | | |
| 3. | The proposed solution should be agent less, So no agent will be deploy on target devices. | | |
| 4. | The proposed solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism | | |
| 5. | The proposed solution should also provide local authentication and all the security features as per best standards. | | |
| 6. | The proposed solution should support an application integration framework for web based as well as .exe-based applications. There should be strong out of the box support including ease of integration with any third-party connectors. | | |
| 7. | The proposed solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business. | | |
| 8. | The proposed solution should provide multi-domain feature whereby the entire operations can operate in a distributed environment. | | |
| 9. | The proposed solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacentres may have multiple secondary installations, but the primary installation will also simultaneously work for all users and all locations. | | |
| 10. | The proposed solution should have the capability to set passwords options at customizable regular intervals of days, months, years and compliance via the use of policy. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 11. | The proposed solution should have ability to create exception policies for selected systems, applications and devices. | | |
| 12. | The proposed solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system. | | |
| 13. | The proposed solution should have flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period. | | |
| 14. | All locally stored target-account passwords should be encrypted using AES or similar encryption with at least 256-bit keys. | | |
| 15. | The proposed solution should have the ability to reconcile passwords manually upon demand. | | |
| 16. | The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests. | | |
| 17. | The proposed solution should have the capability to seamlessly change the passwords for the large number of servers/appliances and desktops. | | |
| 18. | The proposed solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user. | | |
| 19. | The proposed solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd / telnet access, application access, tab restrictions) from session initiated with PAM. | | |
| 20. | The proposed solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user. | | |
| 21. | The proposed solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+ (client/) and other database systems front-end database utilities on any combination of target account, group or target system and end-user. | | |
| 22. | The proposed solution should provide for inbuilt database management utility to enable granular control on database access for SQL, MYSQL, DB2, Oracle etc. | | |
| 23. | The proposed solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc.) and should be able to request for approval on the fly for those commands which are critical. | | |
| 24. | The proposed solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 25. | The proposed solution should be able to define critical commands for alerting and monitoring purpose. With automatic suspension of the session basis critical commands, it should prevent a user from interacting with an active session until a security manager resumes it. The solution should allow security teams to review the potentially risky session's audit trail to determine whether to allow the privileged user to continue their work. The solution should allow to resume the suspended active session and allow the privileged user to continue working post the security team confirmation | | |
| 26. | The proposed solution should be able to support a session recording on any session initiated via PAM solution including servers, network devices, databases and virtualized environments. | | |
| 27. | The proposed solution should be able to log commands for all commands fired over SSH Session and for database access through SSH, SQL+ and others. | | |
| 28. | The proposed solution should be able to log / search text commands for all sessions of database even through the third-party utilities. | | |
| 29. | The proposed solution should be able to log / search text commands for all sessions on RDP. | | |
| 30. | All logs created by the solution should be tamper proof and should have legal hold. | | |
| 31. | The proposed solution should log all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The solution can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group. | | |
| 32. | The proposed solution should have capability to restrict access to different reports by administrator, group or role. | | |
| 33. | The proposed solution should generate reports in at least the following formats: HTML, CSV and PDF | | |
| 34. | The proposed solution should be able to define critical commands for alerting and monitoring purpose through SMS or Email alerts. | | |
| 35. | The proposed solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video-based formats. | | |
| 36. | The session recording should be SMART to help jump to the right session through the text logs. | | |
| 37. | Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 38. | The proposed solution should be TLS 1.2, SHA-2 or higher compliant for PCI-DSS compliance. | | |
| 39. | All communication between system components, including components residing on the same server should be encrypted. | | |
| 40. | All communication between the client PC and the target server should be completely encrypted using secured gateway. | | |
| 41. | The administrator user cannot see the data (passwords) that are controlled by the solution. | | |
| **42.** | **Central Management** | | |
| 43. | 1. Must provide a dedicated central management system software for management of PIM/PAM solution<br>2. The Proposed PIM /PAM solution management should have management console in HA for each Data Centre i.e., NDCSP Delhi, NDC Pune, NDC Hyderabad and NDC Bhubaneswar for all functionalities including anti-malware, HIPS, File Integrity Monitoring, Application control etc<br>3. Underlying ICT Infrastructure (Hardware and software) to run the PIM/PAM software must be supplied by MSP along with PIM/PAM solution.<br>4. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>5. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>6. The proposed solution must have the capability to manage minimum 5000 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>7. The proposed solution should have access through GUI and user management must be based on RBAC.<br>8. The proposed solution should support API for automation<br>9. The solution must support a web-based GUI centralised management for primary and secondary instances.<br>10. The centralised management must support management of software upgrades on both primary and secondary instances. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 11. | The proposed solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container. | | |
| 12. | The proposed solution should have central administration web based console for unified administration. | | |
| 13. | The tool uses Active Directory/LDAP as an identity store for administrators and end users. | | |
| 14. | Administrative configurations (e.g. configuration of user matrix) should be accessible via a separate client where client access is controlled by IP address. | | |
| 15. | Important configuration changes in the solutions (example changes to masters) should be based on multiple level workflow approval process and logged accordingly. | | |
| 16. | Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.). | | |
| 17. | The proposed solution should provide for self-service portal for users and devices for ease of on boarding both users and devices. | | |
| 18. | The proposed solution architecture should be highly scalable both vertically as well as horizontally. | | |
| 19. | The proposed solution should provide multi-tier architecture where the database and application level is separated. | | |
| 20. | The proposed solution should have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data center locations. | | |
| 21. | The proposed solution should have built-in options for backup or integration with existing backup solutions | | |
| 22. | The proposed solution should handle loss of connectivity to the centralized password management solution automatically. | | |
| 23. | The proposed solution s should l not require any network topology changes in order to ensure all privileged sessions are controlled by the solution. | | |
| 24. | The proposed solution should support distributed network architecture where different segments need to be supported from a central location. | | |
| 25. | The proposed solution should support both client based and browser based administration. | | |
| 26. | The proposed solution should be 100% agentless that includes password storage, password management and session recording features. | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 27. | The proposed solution must support parallel execution of password resets for multiple concurrent requests. | | |
| 28. | The solution if required should be available to install on a virtual sever | | |
| 29. | The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. | | |
| 30. | The proposed solution should have an ability to have direct connection to target device as well as using secured gateway channel. | | |
| 31. | The proposed solution should have an ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism. | | |
| 32. | The proposed solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc. | | |
| 33. | The proposed solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods | | |
| 34. | Application Servers Support - The solution should support removing static hard coded passwords from data sources in application servers. | | |
| 35. | The proposed solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation. | | |
| 36. | The proposed solution should have an ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts) | | |
| 37. | The  proposed solution should have an ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key | | |
| 38. | The proposed  solution should have capability to provide alerts and notification for critical PAM events over SMS / Email | | |
| 39. | The proposed solution should have capability to provide alerts and notification for all administration/ configuration activities over SMS / Email | | |
| 40. | Customizable notification for command executed on SSH and Telnet based devices | | |
| 41. | Customizable notification for command/Process executed on Windows | | |

| S.No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 42. | The proposed solution should have inbuilt workflow to manage - | | |
| | 1. Digital Approval based Password Retrieval | | |
| | 2. The solution should support Onetime access / Time Based / Permanent Access | | |
| | 3. Multiple level approval workflow with E-mail and SMS notification with delegation rules | | |
| | 4. Ability to provide for delegation at all levels in the workflow | | |
| 43. | Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phone | | |
| 44. | Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model . | | |
| 45. | Supports a workflow approval process that requires approvers to be in sequence before final approval is granted. | | |
| 46. | Ability to log workflow processes and/or have the ability to be reported or audited. | | |
| 47. | Dashboard Capabilities should include real-time view of activities performed by the administrators | | |
| 48. | The solution should have ability to report on all system administrative changes performed by PAM Administrators with relevant auditable records | | |
| 49. | System should support for implemented in high availability mode. The solution is to be configured as Active-Passive / Active-Active mode in HA between DC to DR with Synchronization and Auto failover. | | |
| 50. | The proposed solution should have the capability to discover and manage permissions and entitlements in the private Cloud. | | |
| 51. | The proposed solution should provide centralized visibility and controls of permissions and entitlements across organizations private Cloud. | | |
| 52. | The proposed solution should have the capability to monitor and identify any changes in the entitlement or permissions in real-time and report/notify of any inappropriate changes | | |
| 53. | The proposed solution should have the capability to provide remediation to excessive privileges based on policies defined | | |

### 13.2. Server Security

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| | **Server Security** | | |
| 1. | The proposed solution should be on-Prem and all threat intel must be provided on Prem via downloading from the cloud or real time through a dedicated url. | | |
| 2. | The solution should have state full Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Web Reputation Device control in single module or an in single agent. | | |
| 3. | The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites. | | |
| 4. | The Solution should have featured a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations. | | |
| 5. | The Solution should be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities. | | |
| 6. | The Solution should provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred. | | |
| 7. | The Solution should have out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services etc. | | |
| 8. | The Solution should include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits | | |
| 9. | The Solution should shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot. | | |
| 10. | The solution must protect against all kinds of viruses, Trojans and worms including but not limited to: boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits | | |
| 11. | The solution should provide real time integrity monitoring of critical operating system and application elements such as directories, files, registry keys and values to detect and report suspicious activity such as modifications | | |

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| 12. | On detection of a malware infection, the solution should allow removal of traces of malware from the system by cleaning up the following automatically or via remote remediation from a centralized management console: a) Detected malicious file, b) Affected registry entries, c) Any new files dropped by malware, d) Windows services created by malware, e) Any other system settings affected by malware. | | |
| 13. | The Solution should cover of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.) with fine-grained filtering (IP and MAC addresses, ports) and basic prevention of denial of service (DoS) attack | | |
| 14. | The Solution should able to detect and protect from reconnaissance scans and solution. | | |
| 15. | The Solution should be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes. | | |
| 16. | The proposed Solution must have certificate based allow/block feature in endpoint Application Control | | |
| 17. | The Solution should provide virtual protection which shields vulnerable systems that are awaiting a security patch. Shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes. | | |
| 18. | The solution should support Application control, behaviour monitoring, Ransomware protection and Zero day threat protection along with simulation engine. | | |
| 19. | The proposed solution should provide vulnerability protection & CVE number visibility against vulnerability. | | |
| 20. | The solution be on premises with Zero day attack prevention along with customize simulation engine as per infrastructure. | | |
| 21. | The Solution must have the capability to classify applications which are attempting network access and block unauthorized connections and data transfers by malicious programs | | |
| 22. | It should support Signature as well as behavioral based detection along with the automatic rollback features when the system is compromised with ransomware attack. | | |
| 23. | Solution must have the capability to accept new software added automatically through verification by authorized processes. | | |
| 24. | The solution should not be dependent on any external software for verification of allowed/banned application. Verification of added software should be verified by itself server security solution | | |

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| 25. | The proposed Solution must provide Web Reputation with an option to add custom url/domain | | |
| 26. | Identify and block botnet and targeted attack C&C Communication. | | |
| 27. | Shields vulnerabilities before they are patched officially, reducing the window of exposure, especially beneficial for legacy systems or mission-critical workloads where patching is delayed. | | |
| 28. | Protect critical servers and applications using a unified agent that delivers advanced security controls, including Intrusion Prevention System (IPS), integrity monitoring, machine learning-based threat detection, application control, host-based firewall, | | |
| 29. | The application control solution should allow the execution of files with a malicious reputation for analysis purposes. All related observations and behaviors must be reported to a centralized console, which will support the fine-tuning of rules and policies based on real-world insights | | |
| 30. | The Proposed solution should Offers host-based firewall capabilities for network filtering. | | |
| 31. | The solution should support real-time change tracking with audit logs. The audit logs must include details such as the file name, user, program name, and the contents that have changed. Additionally, the solution must provide change prevention capabilities as part of its core functionality | | |
| 32. | The proposed solution must have capability to control the external devices like USB,LPT ports , Wireless devices ,external storage devices etc. | | |
| | It should have to control full access/read only/block mode. | | |
| **33.** | **Host Intrusion Prevention System (HIPS) Features** | | |
| 34. | Threat Detection and Prevention: The proposed solution should have the following given features. | | |
| 35. | The proposed solution should Enables threat detection, identification, prevention. | | |
| 36. | Analyses all server-bound packets for intrusions. | | |
| 37. | Supports adaptive mode or integrated blocking for traffic. | | |
| 38. | Uses vulnerability-based signatures for intrusion prevention. | | |
| 39. | **Server Protection: The proposed solution should have the following given features** | | |

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| 40. | Provides protection for web and database servers. | | |
| 41. | Guards against SQL injection attacks. | | |
| 42. | Shields against cross-site scripting (XSS). | | |
| 43. | **Security Features: The proposed solution should have the following given features** | | |
| 44. | Supports system lock-down with application white-listing. | | |
| 45. | Offers built-in alerting, blocking, and logging. | | |
| 46. | Allows response adjustment per signature/policy. | | |
| 47. | Offers timed block or targeted prevention policies. | | |
| 48. | **Centralized Management and Reporting:** | | |
| 49. | 1. Must provide a dedicated central management system software for management of agents.<br>2. The Proposed server security solution should have management console in HA for each Data Centre i.e., NDCSP Delhi, and NDC Bhubaneswar for all functionalities including anti-malware, HIPS, File Integrity Monitoring, Application control etc<br>3. Underlying ICT Infrastructure (Hardware and software) to run the Server Security software must be supplied by MSP along with Server security solution.<br>4. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>5. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>6. The proposed solution must have the capability to manage minimum 50000 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>7. The proposed solution should have access through GUI and user management must be based on RBAC.<br>8. The proposed solution should support API for automation<br>9. The solution must support a web-based GUI centralised management for primary and secondary instances.<br>10. The centralised management must support management of software upgrades on both primary and secondary instances. | | |

| S. No. | Minimum Requirements | Complianc e (Yes/No) | References(Document/P age No) |
|---|---|---|---|
| 50. | The Solution must have the capability to generate infected systems report with their source and destination IP address. | | |
| 51. | Agents managed by central administration system. | | |
| 52. | Supports various reports in HTML, PDF formats. | | |
| 53. | **Endpoint Based Intrusion Prevention System** | | |
| 54. | Solution must provide endpoint-based Intrusion Prevention System to proactively block and safely eliminate malwares and potentially unwanted program from endpoints. | | |
| **55.** | **Anti Malware features** | | |
| 56. | Solution must scan, detect, clean, delete and quarantine the infected files. | | |
| 57. | Solution must clean/ delete/ block malicious codes/software in real time, including viruses, worms, Trojan horses, bot, spyware, adware, mass mailing worms and Rootkit for Windows based Operating systems /Root kit along with web shell(s) for UNIX/Linux based operating systems | | |
| 58. | Solution must have capability to scan, detect and clean the boot sector and Master boot record | | |
| 59. | Solution must have embedded behavioural analysis and protection technology apart from signature based clean/delete/quarantine for unknown threats. | | |
| 60. | Solution must scan, detect and clean or delete malicious code for protocols like POP3 /IMAP/FTP etc., | | |
| 61. | Solution must provide to install antivirus agent through various techniques like web based, MSI package or other methods in workgroup and Active Directory/LDAP environment. | | |
| 62. | Solution must provide to scan single file/directory/entire system and detect, clean, delete or quarantine the infected file. | | |
| 63. | Solution must provide file reputation and web reputation and blocking of intrusion using browsers like Opera, Safari, Chrome , IE etc | | |
| 64. | Solution must provide scheduled scan configuration for full-disks scan at designated time from central manager for clean, delete or quarantine infected file. | | |
| 65. | Solution must provide to prevent endpoint users from uninstalling or disabling the managed antivirus services. | | |
| 66. | Solution must provide to exclude the specified files/directories from real time and manual scan. | | |
| 67. | Solution must provide a utility program for clean uninstallation process of the corrupted antivirus. | | |
| 68. | Solution must be fully IPv4 and IPv6 compliant | | |
| 69. | Solution must provide virtualized environment | | |

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| 70. | Solution must submit the suspected files for which signature has been developed to NIC. | | |
| 71. | Solution must allow for creating whitelisting of application programs, DLLs and executable files and block all remaining programs, DLLs. executable files for execution. | | |
| 72. | Solution must provide self-learning whitelisting, and block applications attempting to execute on any endpoint, unless explicitly allowed by administrator. | | |
| 73. | Solution must provide prevention of tampering and hijacking of applications | | |
| 74. | Solution must have the capability to classify applications which are attempting network access and block unauthorized connections and data transfers by malicious programs. | | |
| 75. | Solution must provide to protect against zero-day attacks | | |
| 76. | The solution should provide an on-premises sandboxing system along with server security to enable zero-day threat detection and prevention. The sandboxing solution must support Windows and Linux operating systems. | | |
| 77. | Solution must have the capability to accept new software added automatically through authorized processes. | | |
| 78. | Solution must provide all the supported versions/latest versions of Microsoft Windows Operating Systems. | | |
| 79. | Solution must have the capability to generate infected systems report with their source and destination IP address. | | |
| 80. | Solution must provide to generate malware, name-wise reports based on source and destination IP address. | | |
| 81. | Solution must provide to generate user defined reports from database. In case reports are provided in raw logs, vendor must be able to generate meaningful reports by exporting into a database. | | |
| 82. | Solution must provide to generate following reports: | | |
| 83. | Current Virus Definition. | | |
| 84. | Virus Definition updates. | | |
| 85. | Report generated must be exported to other applications like HTML, Microsoft Excel, CSV or PDF. | | |
| 86. | Graphical Charts for malwares, infected endpoints etc. for managed clients. | | |
| 87. | Solution must provide to send endpoint logs based on IP and MAC address automatically up to the central manager. | | |
| 88. | Solution must provide that the managed endpoints must send Antivirus event logs. | | |

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| 89. | Solution must provide to send logs of device control and application control to the central manager | | |
| 90. | Solution must provide that the managed endpoints must send Antivirus firewall logs i.e. compliance violations and access log. | | |
| 91. | Solution must provide that the managed endpoints must send Endpoint Based Intrusion Prevention System compliance violations and access log. | | |
| 92. | Solution must provide to integrate with 3rd Party Log Analyser Application Software like Arc-Sight. | | |
| 93. | Solution must provide a Utility program for all supported Windows operating systems for collecting logs of infected endpoints for analysing and developing signatures. | | |
| 94. | Vendor must provide log analysis of infected systems and submit required suspected files to OEM lab for new signature | | |
| 95. | **Sand Boxing** | | |
| 96. | The proposed server security solution should be capable to do On-Prem sandbox which should be able to support at least 3 unique OS images on single appliance and should run at least 60 parallel sandboxes for analysis and support 35,000 samples/day | | |
| 97. | The Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviours for advanced threat detection. | | |
| 98. | The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing, and solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms. | | |

### 13.3. Patch Management

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **Functional Requirements on Central Management Console** | | |
| 2. | The proposed solution must provide management/monitoring of following functions through central console: | | |
| 3. | **Patch Deployment** | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 4. | The solution must be able to manually group endpoints together based on asset and software information for deployment of patches | | |
| 5. | Proposed solution must be Ensured to support for zero-day patch handling (rapid deployment). | | |
| 6. | The proposed solution must be able to integrate with SIEM/SOC tools for real-time monitoring and alerting. | | |
| 7. | The proposed solution must be Ensured to handle third-party applications (Adobe, Java, browsers, etc.), not only OS patches. | | |
| 8. | The proposed solution must have pre-deployment testing in a staging environment before production rollout. | | |
| 9. | The proposed solution must support for rollback with snapshot/restore points in case patch causes issues. | | |
| 10. | The proposed solution must classify the patches based on the severity levels of the missing patches and provide description of severity level | | |
| 11. | The proposed solution must provide to download the available patches from the OEM to keep in repository for distribution. The storage capacity for the repository is to be factored by the MSP/OEM. | | |
| 12. | The proposed solution must allow administrator to define different patch deployment policies | | |
| 13. | The proposed solution must provide real-time patch deployment status | | |
| 14. | The proposed solution must have provision to schedule the deployment of the patches depending on the criticality of the patches over a predefined period of time (which may be immediate or scheduled by the administrator) . Customized alert messages should be sent to the endpoints through pop up messages/ mail/SMS | | |
| 15. | The proposed solution must allow to restart/shutdown the selected endpoints from central console | | |
| 16. | The proposed solution must allow to create custom scripts to deploy third party/user created patches on the endpoints | | |
| 17. | The proposed solution must be able to install all previously installed patches automatically to endpoints that are subsequently added to network | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 18. | The solution must have the feature to customize the messages displayed in a pop-up message box on the endpoints to include the time warning to restart the systems for deployment of the patches | | |
| 19. | The proposed solution must provide deployment of new patches on the computer systems running over different supported OS flavours from central console without intervention from the users of the endpoints | | |
| 20. | The proposed solution must be able to push the missing patches on computer systems running over different supported OS flavours from central console and should path the discovered vulnerabilities in the same os version without upgrading the OS version | | |
| 21. | The proposed solution must provide to roll-back, uninstall and remove deployed patches for OS, any in-house developed application software and any other third-party application software from central console. | | |
| 22. | The proposed solution must provide to deploy patches on the endpoints from central console on Subnet, IP Range, User Group or OS platform basis | | |
| 23. | The Proposed solution must be fully IPv4 and IPv6 compliant (dual-stackable) | | |
| 24. | **ASSET DISCOVERY** | | |
| 25. | The proposed solution must discover and group assets/devices connected in the network such as Servers, Switches, and Routers etc. on the Subnet, IP Range, User Group or OS platform basis. | | |
| 26. | The proposed solution must be able to discover managed (client systems with patch agent installed) and unmanaged assets (client systems with patch agent not installed) on the network. | | |
| 27. | The proposed solution must have cloud/hybrid asset discovery (VMs, containers, SaaS endpoints) | | |
| 28. | The proposed solution must Identify end-of-life (EOL) OS, Servers, appliances and application software to ensure unsupported systems are reported. | | |
| 29. | **ASSET INVENTORY(HARDWARE/SOFTWARE)** | | |
| 30. | The proposed solution must detect hardware configuration of systems like RAM, CPU, Hard Disk and free space on hard disk. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 31. | The proposed solution must detect running OS, any other software applications and their installed patches. | | |
| 32. | **SOFTWARE DISTRIBUTION** | | |
| 33. | The proposed solution must be able to deploy third party application software (including newer versions) and any other in-house developed application on client systems running over different supported OS flavours. | | |
| 34. | The proposed solution must provide to download any third-party application software in the same patch management repository for distribution) | | |
| 35. | The proposed solution must provide to schedule the deployment of other software across NICNET on Segment, IP range, OS and User Group basis | | |
| 36. | The proposed solution must provide to deploy any Patch Management Solution on the systems across NICNET from central console. | | |
| **37.** | **Central Management** | | |
| 38. | 1. Must provide a dedicated central management system software for management of Patch Management agents.<br>2. The Proposed Patch Management solution should have management console in HA for each Data Centre i.e., NDCSP Delhi, NDC Pune, NDC Hyderabad and NDC Bhubaneswar for all functionalities.<br>3. Underlying ICT Infrastructure (Hardware and software) to run the Patch Management must be supplied by MSP along with Patch Management solution.<br>4. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>5. The proposed solution must have the capability to manage minimum 50000 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>6. The proposed solution should have access through GUI and user management must be based on RBAC.<br>7. The proposed solution should support API for automation<br>8. The solution must support a web-based GUI centralised management for primary and secondary instances. | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 9. The centralised management must support management of software upgrades on both primary and secondary instances. | | |
| 10. | **REPORT GENERATION** | | |
| 11. | The proposed solution must provide to generate reports of installed patches, missing patches, failed patches, application software, antivirus solution and their signature version on daily, weekly and monthly basis. | | |
| 12. | The proposed solution must provide to generate reports of compliant and non-compliant systems in graphical formats like pie-chart, bar-chart based on user defined security compliance baseline. | | |
| 13. | The proposed solution must provide to design and generate various user defined (customized) reports from database and raw log files. | | |
| 14. | The proposed solution must report existing vulnerabilities/severities in the systems based on the missing patches and other application software(s) installed in the systems. | | |
| 15. | The proposed solution must compliance mapping with industry standards (ISO 27001, NIST, other regulatory frameworks etc.). | | |
| 16. | The proposed solution must have Customizable dashboards for different stakeholders (CISO, IT admins, and auditors). | | |
| 17. | The proposed solution must have Alerting on patch SLA breaches (e.g., critical patches not deployed within 15 days). | | |
| 18. | The proposed solution must have capability of role-based access control (RBAC) to ensure that only authorized administrators can manage patching. | | |
| 19. | The proposed solution must have capability for audit logs of all patching activities for audits and regulatory compliance. | | |
| 20. | The proposed solution should support multi-factor authentication for console login. | | |
| 21. | The proposed solution must Maintain tamper-proof logs for audit purposes. | | |
| 22. | The proposed solution must support for containerized workloads (Dockers, Kubernetes) and cloud VMs (AWS, Azure, GCP). | | |

| S. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 23. | The proposed solution must have API support for integration with automation/orchestration tools. | | |

## 13.4. Host based Data Loss Protection Solution

| Sl. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | **Content Detection & Classification** | | |
| 2. | The proposed solution should detect on patterns in binary file types | | |
| 3. | The proposed solution should detect keywords/patterns based on location (beginning/end) and proximity to each other within documents. | | |
| 4. | The proposed solution should detect on full Boolean expression for keywords and key phrases. | | |
| 5. | The proposed solution should detect on Pre-built dictionaries. | | |
| 6. | The proposed solution should detect and validate a wide range of sensitive data types | | |
| 7. | The proposed solution should detect classified Proprietary File types (types that are not predefined) and on file content not on file extensions. (eg. Document owner, authors, title etc.) | | |
| 8. | The proposed solution should detect fingerprints contents in an automated way where the user does not have to touch the files or import hashes. | | |
| 9. | The proposed solution should provide the ability to the end user to manually classify the solution on the endpoint. | | |
| 10. | The Proposed solution should provide Policy enforcement with combined automatic and manual classifications | | |
| 11. | The proposed solution DLP Discover should detect and identify automatic classifications on files set by DLP Endpoint | | |

| Sl. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 12. | The proposed solution should have single management console for data classification policies and DLP policy configuration and assignments. | | |
| 13. | The Proposed Solution should Optical Character Recognition (OCR) at the endpoint agent level | | |
| 14. | The proposed solution should have application, web and location based data tagging actions. | | |
| 15. | **DLP Policy Creation** | | |
| 16. | The proposed solution should have the ability to define a single set of policies based on content, sender/recipient, file characteristics and communications protocols once and deploy across all products. | | |
| 17. | The proposed solution should provide Out of the Box Rule Sets. | | |
| 18. | The proposed solution should create policies that support full Boolean expression for keywords/patterns (not just and/or). | | |
| 19. | The proposed solution should provide directory based policies to selectively monitor downloads based on user, business units, or directory groups, specific groups of computers and specific groups of users. | | |
| 20. | The proposed solution should provide ability to configure policies to detect on fingerprints and files from share/repository/date created etc. | | |
| 21. | **Host DLP** | | |
| 22. | The agent should Monitor content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.) & Application Access. | | |
| 23. | The proposed solution should notify the end user of a policy violation using a customizable pop-up message and should capture content that violates a policy and store it in an evidence repository. | | |
| 24. | The proposed solution should be able to enforce policies while the endpoint system is disconnected from the corporate network and the endpoint agent should log all violations and reports into the central database when a connection to the corporate network is established. | | |

| Sl. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 25. | The proposed solution should be able to Identify mass storage device by vendor specific identification numbers. | | |
| 26. | The proposed solution should be able to Identify content using regular expressions, key words, hash functions, Document Fingerprint Signatures and pattern matching. | | |
| 27. | The proposed solution should be able to Identify content based on location and allow creation of policies based on Users and Groups. | | |
| 28. | The proposed solution should provide an option of rule override which can be authorized to use an override code issued from the security administrator based on the end user's justification. | | |
| 29. | The proposed solution should support the deployment of agent, policy assignments, reporting, DLP incident management using the Central Management Console. | | |
| 30. | The agent should protect itself from unauthorized removal or service stoppage. | | |
| 31. | The solution should have an option to Quarantine/Monitor/Delete sensitive files found during endpoint discovery. | | |
| **32.** | **DLP Search Engine** | | |
| 33. | Data-in-motion | | |
| 34. | The proposed solution should conduct the following searches: | | |
| | A. Any e-mail sent from or to email addresses | | |
| | B. Any traffic sent across protocols or ports | | |
| | C. Documents leaving the network based on document type. | | |
| 35. | The proposed solution should conduct searches for content indexed during the following: | | |
| | A. Data-at-rest crawl based on keywords | | |
| | B. Data-at-rest crawl based on document type | | |
| | C. Data-at-rest crawl based on file owner, path, or age. | | |
| **36.** | **Incident Management** | | |
| 37. | The proposed solution should provide the ability to detect Policy violation which retains the source IP address, destination IP address, protocol, sender e-mail address, recipients e-mail address | | |

| Sl. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 38. | The proposed solution should provide ability by which Incidents can be assigned automatically to reviewers. | | |
| 39. | The proposed solution should provide the ability for Incidents to be sorted by severity level, sender, recipient, source, destination, protocol, and content type. | | |
| 40. | Incident views can be customized based on content pertinent to the reviewer's role and preferences. | | |
| 41. | The proposed solution should provide an inbuilt Case Management Tool. | | |
| 42. | The proposed solution should provide the ability for Case content to be exported with full content and attachments for review by an external reviewer. | | |
| **43.** | **Forensics/Investigation** | | |
| 44. | The proposed solution should have the ability to store and index the capture event data with appropriate metadata (date/time, user, protocol). | | |
| **45.** | **Architecture & Deployment** | | |
| 46. | The solution's Management System should be provided and it should be deploy in high availability mode, also support multiple hypervisor platform like (VMware esxi or Microsoft Hyper-V). | | |
| 47. | The communication channels between system components should be authenticated and encrypted | | |
| 48. | The Policy management should include the following features and options: | | |
| | A. Selection of data type(s) and user group(s) – using Active Directory. | | |
| | B. Enable exceptions - allowed users. | | |
| | C. Traffic direction - enforce on outbound or interdepartmental traffic. | | |
| | D. Pre-defined policies and content data types. | | |
| 49. | The proposed solution should be able to Configure and distribute action rules, including email notification, blocking, quarantining. | | |

| Sl. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 50. | The proposed DLP solution should provide where administrators can create a single email and web protection policy in single unified console and deploy it to endpoints and share a common classification engine that allows for a single email and web policy. | | |
| 51. | The proposed solution should support the deployment of agent for Endpoint DLP policy assignments, reporting, DLP incident management using the single Central Management Console. | | |
| **52.** | **DLP Reporting** | | |
| 53. | The proposed solution should generate reports in PDF, Excel or CSV format. | | |
| 54. | The proposed solution should develop reports built around stakeholder requirements such as top Policy Violations, Senders, Content Type, Protocol, Historical Reports etc. | | |
| **55.** | **Central Management** | | |
| 56. | 1. A separate Centralized Management / Reporting solution must be provided along with DLP software solution and must be deployed in HA mode at NDC Delhi.<br>2. Underlying ICT Infrastructure (Hardware and software) to run the DLP software must be supplied by MSP along with DLP solution.<br>3. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>4. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>5. The proposed solution must have the capability to manage minimum 200 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>6. The proposed solution should have access through GUI and user management must be based on RBAC.<br>7. The proposed solution should support API for automation<br>8. The solution must support a web-based GUI centralised management for primary and secondary instances. | | |

| Sl. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 9. The centralised management must support management of software upgrades on both primary and secondary instances. | | |
| 10. | **Support** | | |
| 11. | The proposed solution should be proposed with Premium Support i.e directly from the OEM. | | |
| 12. | The proposed solution should provide a single point of contact for account management and escalation | | |
| 13. | The OEM should provide a utility to collect product and system information to assist support in diagnosing issues | | |
| 14. | Product upgrades should be easily be downloadable from the OEM Official Website | | |
| 15. | The OEM should provide a service which delivers the latest OEM product information by email — patch and upgrade notification; and critical alerts that require immediate attention. | | |

## 13.5. Virtual Web Application Firewall

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| **1.** | **General Requirements:** | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| **2.** | The Proposed solution should be a Virtual software solution and must support Vmware, KVM, Hyper-V and other virtualised platforms. | | |
| 3. | The Proposed web application firewall solution should provide specialized application threat protection. | | |
| 4. | The Proposed solution should protect against application layer attacks targeted at web applications. | | |
| 5. | The Proposed solution should provide bi-directional protection against sophisticated threats like SQL injection, cross-site scripting and support OWASP application security methodology. | | |
| 6. | The Proposed solution should provide controls to prevent identity theft. | | |
| **7.** | **Performance requirements** | | |
| 8. | The Proposed solution should be able to provide a WAF or SSL throughput 2 Gbps<br>MSP has to provide all the passive components like optical fibre cables, Cat 6 cables etc. | | |
| **9.** | **Feature specifications.** | | |
| 10. | The Proposed solution should be able to perform in multiple modes such as active/passive mode, transparent mode and proxy mode. | | |
| 11. | The Proposed solution should continuously track the availability of the servers being protected. | | |
| 12. | The Proposed solution should have Data Leak Prevention functionality to analyse all outbound traffic alerting/blocking any credit card/Aadhaar. No leakage and information disclosure. | | |
| 13. | The Proposed solution should provide controls to meet PCI DSS compliance requirements for web application servers. | | |
| 14. | The Proposed solution should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 15. | The Proposed solution should support automatic signature updates to protect against known and potential application security threats. | | |
| 16. | The Proposed solution should have the ability to define different WAF policies with different settings like parameter length, URL prefix, meta characters, allowed and disallowed URL, parameter types etc. for different applications instead of one single policy or a global setting. | | |
| 17. | The Proposed solution should have the ability to create custom attack signatures or events. | | |
| 18. | The proposed solution should have the capability to protect certain hidden form fields. | | |
| 19. | The Proposed solution must provide ability to allow or deny a specific URL access/IP(s). | | |
| 20. | The Proposed solution should support normalization methods such as URL decoding, Null Byte string, termination, converting back slash to forward slash character etc. | | |
| 21. | The Proposed solution should support IP reputation service and able to provide up to date information about threatening sources. | | |
| 22. | The Proposed solution must support IPv6 for reverse proxy deployments and it should also support IPv4 to IPv6, IPv4 to IPv4,IPv6 to IPv4 and IPv6 to IPv6 communication. | | |
| 23. | The proposed solution must support communication over the IPv6 protocol on the management interface | | |
| 24. | The Proposed solution should have BOT mitigation functionality (including CAPTCHA or equivalent):<br>(a) Without having to go on internet for some cloud-based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc<br>or<br>(b) Equivalent technology for bot mitigation. | | |
| 25. | The Proposed solution should have file upload violation capabilities and should provide support for scanning of malicious content. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 26. | The proposed solution should detect and mitigate HTTP Parameter Pollution (HPP) attacks, preventing malicious manipulation of query parameters and preserving the intended behaviour of web applications | | |
| 27. | The Proposed solution should be able to employ connection pooling technology to optimize backend network operations and server resources. | | |
| 28. | The Proposed solution should have features to hide errors from server and redirect to customized page. | | |
| 29. | The Proposed solution should allow IP addresses or IP address range for bypassing applied security policy for one particular hosted application but should not bypass others. | | |
| 30. | The Proposed solution should facilitate in hiding/masking specific sensitive parameters pertaining to specific applications. | | |
| 31. | The Proposed solution should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address permanently or for a time period. | | |
| 32. | The Proposed solution should inspect Simple Object Access Protocol (SOAP) and extensible Mark-up Language (XML), in addition to HTTP (HTTP headers, form fields, and the HTTP body). | | |
| 33. | The Proposed solution should have the negative security model it should detect and protect attack based on Signature (Regular expression) and complex logic (logical AND, Logical OR) against incoming URL request and the same may be extended for all parts (i.e., URI, parameters, headers, cookies.) | | |
| 34. | The Proposed solution should have the positive security model and it should validate URLs, directories, cookies, headers, form/query parameters, HTTP methods, File upload Extensions, allowed meta characters etc. | | |
| 35. | The Proposed solution should support profiling to configure fine grained controls for each deployed web application. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 36. | The Proposed solution should support all operating systems/development frameworks and their versions including but not limited to Windows, Unix, and Linux. | | |
| 37. | The Proposed solution should provide HTML rewriting functionality (e.g., edit, add, delete request and response header, rewrite and redirect the URL in the request, rewrite response body etc.). | | |
| 38. | The Proposed solution should have the ability to generate and issue CAPTCHA or equivalent queries to challenge suspicious clients. | | |
| 39. | The Proposed solution should have the capability to auto-learn security profiles required to protect the Infrastructure. | | |
| 40. | The Proposed solution should provide a statistical view on collected application traffic. | | |
| 41. | The Proposed solution should detect and prevent brute force attack (repeated requests for the same resource) against any part of the applications. | | |
| 42. | The Proposed solution should provide protection from application layer DDOS attacks. | | |
| 43. | The Proposed solution must protect against SYN-flood type of attacks. | | |
| 44. | The Proposed solution should be able to protect cookie poisoning and cookie tampering. | | |
| 45. | The Proposed solution must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2.0 and HTTP/3.0 | | |
| 46. | The Proposed solution should support restricting/controlling the methods used. | | |
| 47. | The Proposed solution should validate header length, content length, Body length, Parameter length, body line length etc. | | |
| 48. | The Proposed solution should support hosting/terminating of SSL web applications and should allow to upload the certificates and private/public key pairs for the web servers. | | |
| 49. | The Proposed solution should work In termination mode, the backend traffic (i.e., the traffic from the WAF to the web server) can be encrypted via SSL. | | |
| 50. | The Proposed solution must support all major cipher suites. | | |
| 51. | The Proposed solution should provide protection against SSL based attacks. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 52. | The Proposed solution should support for SSL offloading. | | |
| 53. | The Proposed solution should support high availability in active/passive and active/active mode. | | |
| 54. | The Proposed solution should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers. | | |
| 55. | The Proposed solution must be integrated with third party vulnerability scanning tools to provide virtual patching with required understanding of WAF policy. | | |
| 56. | The Proposed solution should support secure administrative access using HTTPS and SSH. | | |
| 57. | The Proposed solution should support role-based access control for Management. | | |
| 58. | The Proposed solution should have ability to remotely manage appliances. | | |
| 59. | The Proposed solution should have management user interface support for both GUI and CLI access. | | |
| 60. | The Proposed solution should have separate network interface for SSH/HTTPS access. | | |
| 61. | The Proposed solution must support for trusted hosts. | | |
| 62. | The Proposed solution must have Role-based management with user authentication. | | |
| **63.** | **Central Management Solution** | | |
| 64. | 1. Must provide a dedicated central management system software for management of Virtual WAF .<br>2. The Proposed virtual WAF solution should have management console in HA for each Data Centre i.e., NDCSP Delhi, and NDC Bhubaneswar for all functionalities.<br>3. A separate Centralized Management / Reporting solution must be provided along with Virtual WAF software solution and must be deployed in HA mode.<br>4. Underlying ICT Infrastructure (Hardware and software) to run the Virtual WAF software solution must be supplied by MSP along with Virtual WAF solution.<br>5. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| | 6. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>7. The proposed solution must have the capability to manage minimum 300 Virtual WAF solution and adequate licenses for managing these assets must be supplied from Day 1.<br>8. The proposed solution should have access through GUI and user management must be based on RBAC.<br>9. The proposed solution should support API for automation<br>10. The solution must support a web-based GUI centralised management for primary and secondary instances.<br>11. The centralised management must support management of software upgrades on both primary and secondary instances. | | |
| 12. | The Proposed solution should support two factor authentication for login into the management Web GUI. | | |
| **13.** | **Logging, Reporting and Troubleshooting** | | |
| 14. | The Proposed solution should have ability to identify and notify system faults and loss of performance. | | |
| 15. | The Proposed solution should support log aggregation. | | |
| 16. | The Proposed solution should support multiple log formats such as CSV, Syslog, TXT, etc. | | |
| 17. | The Proposed solution should support reporting and sending the report via E-Mail. | | |
| 18. | Proposed solution should support report formats in PDF, HTML/WORD/RTF, etc. | | |
| 19. | The proposed solution must have facility to send all logs to separate log server/SIEM solutions as per standard norms. | | |
| 20. | The Proposed solution must have mechanism to raise alert to SOC team through Email, Syslog, SNMP Trap, Notification etc. for blocking the traced malicious IP source causing specific attack. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document / Page no) |
|---|---|---|---|
| 21. | The Proposed solution should support to generate reports like pie-chart, bar-chart based on user defined security compliance baseline. | | |
| 22. | The Proposed solution should allow commands from WAF for troubleshooting network related issues like Ping and trace route. | | |
| 23. | The Proposed solution should support to generate vulnerability reports based on standard vulnerability database like CVE, NVD etc. | | |
| 24. | The Proposed solution should support to take full secure configuration backup on a physical disk or SAN/NAS storage. | | |
| **25.** | **Service Support** | | |
| 26. | OEM should be able to deploy the Web application firewall appliance and remove it from the network with minimal impact on the existing web applications or the network architecture. | | |
| 27. | Appliance should support integration with orchestration systems and APIs if required. | | |

## 13.6. Database Activity Monitoring (DAM)

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 1. | The proposed solution should meet regulatory compliance such as SOX, PCI DSS, Data Privacy Law, GDPR etc. | | |
| 2. | The proposed solution must capable for creation of an inventory through auto discovery of all databases and database users, deployed across the enterprise. | | |
| 3. | The proposed DAM solution should be able to monitor in scope database without dropping any log. | | |
| 4. | Each image of DAM gateway/ collector must support up to 60K TPS and this 60K TPS support should be for all types of queries and not limited to just privilege queries. In case the TPS goes beyond 60K then the DAM gateway/collector must support horizontal scaling. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 5. | The proposed solution should provide optimum utilization of resources by using load balancing between its devices, if it is using multiple boxes/ gateways. | | |
| 6. | The proposed solution should comply and support IPv4 and IPv6 both. The Proposed solution must support IPv4 to IPv6, IPv4 to IPv4, IPv6 to IPv4 and IPv6 to IPv6 communication. | | |
| 7. | The proposed solution must have temper-proof log storage capability. | | |
| 8. | The proposed solution required monitoring should be delivered while solution is enabled and in blocking mode | | |
| 9. | The proposed solutions should support virtual patching of database for known missing patches i.e., the solution should be able to virtually patch the known vulnerabilities automatically till a patch is installed for the same. | | |
| 10. | The proposed solution should support creation of policies/rules for enforcing access control and proper rights management on databases. | | |
| 11. | The proposed solution must support reporting of deviations to the policies and access control | | |
| 12. | **Dynamic profiling –** The proposed solution should automatically examine the traffic and create profile of their structure and behaviour. | | |
| 13. | The proposed solution should continuously learn the user and application behaviour in respect of accessing database. Learning should be a continuous process and should not stop after a certain stage. | | |
| 14. | The proposed solution should provide risk score of individual databases, based on combination of security alerts, discovery results, vulnerability assessment, sensitivity and confidentiality of data stored in the database. | | |
| 15. | The proposed solution must monitor privileged user access or local SQL activity that does not cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes | | |
| 16. | The proposed DAM solution should identify abnormal server and user behaviour and providing early detection of possible attacks using outliers. For example: | | |
| | a) User accessing a table for the first time. | | |
| | b) User selecting specific data in a table that he has never selected before. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | c) Exceptional volume of errors | | |
| | d) Activity that itself is not unusual, but its volume is unusual. | | |
| | e) Activity that itself is not unusual, but the time of activity is unusual. | | |
| 17. | The solution must support filtering /hiding of the bind variables of all the SQL activities captured | | |
| 18. | The proposed  solution should not store sensitive data in plain text in logs generated by the application (e.g. passwords) | | |
| 19. | Logs and audit-trail generated by the solution should not be editable by users/ administrator and should be read-only. | | |
| 20. | The Proposed solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats. | | |
| 21. | The Proposed solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria. | | |
| 22. | The proposed solution must be able to perform  content scanning  for  regular  expression and patterns and should monitor nested queries | | |
| 23. | Communication from Agent to management server must be encrypted | | |
| 24. | The proposed solution must be able to monitor database which run on non-standard port | | |
| 25. | The proposed solution should be able to classify the database/database-objects based on sensitivity and confidentiality of data based on PII, SPDI, PCI DSS guidelines or customized parameters. | | |
| 26. | The proposed solution should be capable of auto discovering sensitive/ confidential data, like credit card Numbers, Aadhaar or any PII in the database and offers the ability for customization. | | |
| 27. | The proposed solution should be able to auto discover privilege users in the database and should support user entitlement reviews on database accounts | | |
| 28. | The proposed solution should be able to auto discover default passwords in the default DB accounts | | |
| 29. | The proposed solution tracks the dormant accounts as per defined rule. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 30. | The proposed solution should inspect both in-coming and out-going DB traffic, compare with the rules and generate alert. | | |
| 31. | The proposed solution should detect attacks on network protocols, operating systems, as well as application layer DB activity. | | |
| 32. | The proposed solution should capture and analyse all database activity, from both application user and privileged user accounts, providing detailed audit trails that shows the "Who, What, When, Where, and How" of each transaction. | | |
| 33. | The proposed solution should provide full details needed for analysis of audited events: date and time, raw SQL, parameters used, end username, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. should be capable of capturing and reporting at a very granular level. | | |
| 34. | The proposed solution should detect attacks attempting to exploit known vulnerabilities as well as common threat vectors and can be configured to issue an alert and\or terminate the session in real time | | |
| 35. | The proposed solution should discover misconfigurations in the database and its platform and suggest remedial measures. | | |
| 36. | The proposed solution should be capable of reporting missing patches and report the details of such patches and vulnerabilities associated with. | | |
| 37. | The proposed solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed. | | |
| 38. | The proposed solution should also be able to detect any change happens in stored procedure | | |
| 39. | The proposed solution should have capability to monitor local access and encrypted connections (Oracle ASO, SSL, IPsec etc.) | | |
| 40. | The proposed solution should provide full details needed for analysis of audited events:<br>Date and time, raw SQL, parameters used, end username, source IP, source application, destination database instance, schema DB objects affected, command details, results | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | generated, values affected etc. should be capable of capturing and reporting at a very granular level. | | |
| 41. | The proposed solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc. | | |
| 42. | The proposed solution support creation of different type of security and audit policies such as rule, report based on heuristic and content based. These policies should support customization. | | |
| 43. | The proposed solution  should be ability to kill sessions for accessing sensitive data/policy violations and keeping all activity in the logs | | |
| 44. | The proposed solution should be capable of blocking access real time, execution of commands which violate the rules/policies, store the events securely and report the same in real time. | | |
| 45. | The Proposed solution should support monitoring mode and blocking mode of deployment. In monitoring mode solution can generate alerts for unauthorized activity. In blocking mode solution must proactively block the queries including blocking of matching signatures for known attacks like SQL injection. | | |
| 46. | The proposed solution should support installation of agents, update of agents' configurations updates, policy updates start/ stop/restart etc., at all the databases from management server centrally. | | |
| 47. | Proposed solution should not be dependent on native configurations of the database. E.g. Solution should not require a change in the database binary | | |
| 48. | There should be no downtime of the OS or database for deployment of agents. | | |
| 49. | The   agent should not require a reboot of OS and DB after installation configuration. Only one agent to be installed, no third-party agents permitted. All agents regardless of deployment mode should be managed from the centralized management console. | | |
| | The proposed solution should not use any 3rd Party software/support for any purpose | | |
| 50. | If the agent mal-functions or uninstalled or disabled on server, immediate alert to be issued. | | |
| 51. | If the communication between agent and the console is lost, immediate alert to be issued. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 52. | The proposed solution should not use the native database audit functionality. The solution should not employ native database transaction log auditing. | | |
| 53. | The proposed solution should be able to support/monitor all database activities in Oss like – AIX, UNIX, Linux Solaris, Windows and Databases like Oracle- MS-SQL, MySQL, postgress ,IBM DB2,MariaDB at a minimum. | | |
| 54. | The proposed DAM solution should support integration with the Big Data platform and Data warehouse such as Exadata etc | | |
| 55. | The proposed solution should generate alert for any violation of security policy real time | | |
| 56. | The proposed solution should discover all the databases with details i.e., IP, type, OS etc., available in the network | | |
| 57. | The proposed solution should also discover if any new database and DB objects created within the monitored network/systems. | | |
| 58. | The proposed solution must allow administrators to add and modify policies. | | |
| 59. | The proposed solution should log the actual client IP. | | |
| 60. | The proposed solution should auto profile the activities to filter noise or known false positives and should generate alert if any violation | | |
| 61. | The proposed solution support individual user access auditing for packaged applications like SAP, PeopleSoft etc., which the buyer proposes to implement in future. | | |
| 62. | Separate policies should be applied for different databases configured in DAM | | |
| 63. | The proposed solution should have pre-built templates for well-known security and audit policies. | | |
| 64. | The resource overhead (hardware, software) for the agent should not exceed 5% of the normal requirement of the CPU. There should be only one agent. | | |
| 65. | The proposed solution should provide CPU, RAM, disk capping capabilities on agent- based solution | | |
| 66. | The proposed solution should have capability to facilitate rule creation at a very granular level. Example: Which user can connect from which source, access what objects, have which rights, at what time window etc. | | |
| 67. | Rules also should allow blocking access depending upon different parameters like above. | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| 68. | The Proposed solution should include a web based or thick client based single administration interface. | | |
| 69. | The Proposed solution should have an out-of-band management capability. | | |
| 70. | Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties. i.e., Administrator (Super-User) Manager, read only etc. | | |
| 71. | The proposed solution should support the following authentication mechanism for accessing the solution: | | |
| | (i) In-built authentication in the solution | | |
| | (ii) Kerberos authentication | | |
| | (iii) LDAP authentication | | |
| | (iv) AD | | |
| | (v) RADIUS authentication | | |
| 72. | The proposed solution must be able to operate in FIPS (Federal Information Processing Standard) 140-2 compliance mode. | | |
| 73. | **Central Management** | | |
| 74. | 1. A separate Centralized Management / Reporting solution must be provided along with DAM software solution and must be deployed in HA mode at NDC Delhi.<br>2. Underlying ICT Infrastructure (Hardware and software) to run the DAM software must be supplied by MSP along with DAM solution.<br>3. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>4. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>5. The proposed solution must have the capability to manage minimum 5000 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>6. The proposed solution should have access through GUI and user management must be based on RBAC.<br>7. The proposed solution should support API for automation | | |

| Sr. No. | Minimum Specifications | Compliance (Yes / No) | Reference (Document /Page no) |
|---|---|---|---|
| | 8. The solution must support a web-based GUI centralised management for primary and secondary instances.<br>9. The centralised management must support management of software upgrades on both primary and secondary instances. | | |
| 1. | The proposed DAM solution must be able to deploy or remove from the network with no impact on the existing databases or the network architecture. | | |
| 2. | The proposed solution must support proper reporting and logging facilities. | | |
| 3. | The proposed solution should be able to report events and alerts via standard mechanisms for example to a syslog or SNMP server or a SIEM solution. | | |
| 4. | The proposed solution must support the creation of custom log messages and provide system variable placeholders mechanism to make this use case possible. | | |
| 5. | The proposed solution must support generation both predefined as well as custom built reports as per requirements with both tabular views, pdf and data analysis graphical views. | | |
| 6. | The proposed solution should have easy option to customize report without developing or-require lot of customization/changes from scratch | | |
| 7. | Alert should be generated in case of violation of rules through SMTP (mail). | | |
| 8. | The proposed solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event violation of specific rules, user, source of origin, DB instance etc. | | |
| 9. | The solution should be able to generate the reports in HTML, PDF, Excel and CSV Excel formats | | |

### 13.7. Authentication, Authorization, and Accounting (AAA)

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| 1. | The proposed solution must support authentication, authorization, and accounting (AAA) protocols such as RADIUS, TACACS+ etc. | | |
| 2. | The proposed solution should provide authentication, user or administrator access and policy control for centralized access control. The solution must support an integrated user repository in addition to integration with existing external identity repositories such as Microsoft Active Directory servers, LDAP servers etc. | | |
| 3. | **Authentication protocols:** The proposed solution must support authentication protocols like PAP, MS-CHAP, and Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication through Secure Tunnelling (FAST), EAP-Transport Layer Security (TLS), and PEAP-TLS and other equivalent protocols. | | |
| 4. | The proposed solution must support a rules-base, attribute-guided policy model that provides access control policies, which can include authentication protocol requirements, device restrictions, time-of- day restrictions, and other access requirements.<br>The proposed solution should be support 5000 concurrent user. | | |
| 5. | **Central Management** | | |
| 6. | 1. A separate Centralized Management / Reporting solution must be provided along with software solution and must be deployed in HA mode at NDC Delhi and NDC Bhuvneshwar.<br>2. Underlying ICT Infrastructure (Hardware and software) to run the AAA software must be supplied by MSP along with AAA solution.<br>3. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>4. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>5. The proposed solution must have the capability to manage minimum 5000 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>6. The proposed solution should have access through GUI and user management must be based on RBAC.<br>7. The proposed solution should support API for automation | | |

| S. No. | Minimum Requirements | Compliance (Yes/No) | References(Document/Page No) |
|---|---|---|---|
| | 8. The solution must support a web-based GUI centralised management for primary and secondary instances.<br>9. The centralised management must support management of software upgrades on both primary and secondary instances. | | |
| 10. | The proposed solution must include monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI. | | |
| 11. | The proposed solution must support central database for all user accounts and centralized control of all user privileges, which can distribute throughout the network-to-network switches and access points | | |
| 12. | The proposed solution must be able to provide AAA services for wired and wireless LAN, and VPN and other network and network security devices in the Data centre like DDoS, NGFW, NIPS, APT, WAF, SLB, SSL off loader, APT, Server Security etc. | | |
| 13. | The proposed solution must support Lightweight Directory Access Protocol (LDAP) authentication forwarding for user profiles stored in directories from leading directory vendors. | | |
| 14. | The proposed solution must provide features to define different access levels for each administrator and the ability to group network devices to enforce and change of security policy. | | |
| 15. | The proposed solution must provide access control lists based on time-of-day, and day-of-week access restrictions | | |
| 16. | The proposed solution must be software based and should be deployable on a Virtual Machine. | | |

## 13.8. Vulnerability Assessment (VA) Solution

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 1. | Category | Software | | |
| 2. | VA Scanner based on | Software | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 3. | VA Scanner Deployment modes | 1. Active-Active<br>2. Active-Passive<br>3. Standalone<br>4. Manual<br>5. Multi Tenancy<br>6. Zero Touch Deployment<br>7. Scanner Proxy for VPC Environment | | |
| 4. | Scope of Installation | 1. Installation<br>2. Support Integration- with SIEM and open stack and Parichay.<br>3. End to End Vulnerability Management Work flow creation<br>4. User Acceptance Testing of offered  modules | | |
| 5. | Automation/Management Support | 1. Terraform<br>2. Ansible<br>3. Heat Template<br>4. AWS Lambda<br>5. Azure ARM<br>6. Elastic Beanstalk<br>7. CLI<br>8. SSH<br>9. GUI | | |
| 6. | VA Scanner Functioning | Load balancing, Task peering, Automatic failover | | |
| 7. | Centralized Management Module Based on | Hardware, Software | | |
| 8. | Type of License | Subscription | | |
| 9. | Type of IP Scanning | Firmware, OS, Application, Database | | |
| 10. | Licence Model for VA Scanner | 1. Host Based<br>2. IP Based<br>3. Container Image Based<br>4- Container Host/POD | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 11. | Number of Licences for Host Based/IP based Scanning | 45,000 | | |
| 12. | Number of Licences for container images and running containers scanning | 1000 | | |
| 13. | Installation and Demonstration | Yes | | |
| 14. | No. of days of Training Provided at Client Site by OEM | 5 | | |
| 15. | OEM Support Features | 1. 24 x 7 x 365 Support by respective OEM from India<br>2. OEM office in India<br>3. Support offices Pan India<br>4. To Provides direct & its own payroll employee based onsite professional services for installations, configuration, validations, support etc.<br>5. Updating for Patches and Bug fixes within support period<br>6. Upgradation of version within support period<br>7. Fine tune the Vulnerability signatures in case of false positive | | |
| 16. | IPv6 support and scan by hostname/IP supported | Yes | | |
| 17. | Capability of creating users in the offered product | 1000+ | | |
| 18. | Global Threat Intelligence support | DBIR (Data Breach Investigations Report), SANS TOP20 | | |
| 19. | Agents Size in MB | Less than 100 MB | | |
| 20. | | **MAX CAPACITY OF ASSET TO BE SCANNED** | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 21. | Hard disk capacity (in TB) (Hint :- Select '0' if not applicable) | Unrestricted | | |
| 22. | RAM size (in GB) (Hint :- Select '0' if not applicable) | Unrestricted | | |
| 23. | Physical CPU Cores | Unrestricted | | |
| 24. | **Asset Inventory, Categorization and Management** | | | |
| 25. | Asset Inventory, Categorization and Management | Assess complex IT infrastructure and quickly identify the risk | | |
| 26. | | Collect and analyse data about assets across hybrid environments, and delivers up-to-date, comprehensive and continuous information about those assets as well as their security and compliance posture | | |
| 27. | | Find unauthorized software which are blacklisted in the environment but are installed in the environment, also including assets that are running unsanctioned ports and take the necessary actions | | |
| 28. | | Track EOS/EOL Software, Hardware, OS that reduces tech debt by uncovering outdated or unsupported applications, missing required software, and unauthorized or missing titles. Solution should also give the visibility into the list of software which will be EOL in the upcoming 3, 6, 9 and 12 months. | | |
| 29. | | Able to tag software as per requirement of the Purchaser | | |
| 30. | | Bridge the IT-Security Gap: Integration with CMDB, tracking 150k+ vulnerabilities from over 25+ threat sources – plus support for ITSM ticketing resulting in a faster MTTR across teams | | |
| 31. | | Identify the assets which are missing the Mandatory/Approved software as per organization’s policy and plan to roll them out in phase wise manner | | |
| 32. | | Keep the CMDB up to date via bi-directional integration which will aid in baselining & improving the CMDB and ensure compliance with industry standards and regulatory requirements | | |
| 33. | | Able to ingest the asset date from 3rd party sources | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 34. | | Expand the Internal attack surface coverage with network discovery including unmanaged devices connected to the network in real time without compromising on performance of running VMs/containers. | | |
| 35. | | Risk Scoring giving the solution the power to analyse vulnerabilities and misconfigurations in real time with six-sigma accuracy to prioritize remediation based on criticality and potential business impact | | |
| 36. | | Provide Context-relevant Prioritization that allows security teams to assign risk profiles that prioritize security efforts by tagging assets according to function, environment, service and business relevance | | |
| 37. | | Asset Management and Vulnerability Management modules should be integrated within the platform for data enrichment | | |
| 38. | | Give the visibility into Asset, Software, Web applications, open ports, certificates details on the same UI | | |
| 39. | | Give the user the flexibility to create dynamic tags basis on "asset name", "asset inventory", IP address and range, open ports, vulnerability, etc. | | |
| 40. | | Have the response capability to send the emails to required stakeholders | | |
| 41. | | Given the option to users to create rules for Software, Ports, Asset Purge (basis on IP scanned date, agent reporting to the platform, cloud meta data) | | |
| 42. | | The solution must provide functionality for creating and enforcing rules to categorize software as Authorized, Unauthorized, or Under Review. The system should allow administrators to define, manage, and enforce policies for each category to ensure only approved software is permitted, unapproved software is blocked or flagged, and software requiring review is logged for further assessment | | |
| 43. | | Proposed solution should be able to create asset, software, certificate, missing software, open ports, compliance dashboard/reports | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 44. | | Proposed solution must able to Identify unmanaged devices connected to your network in real time, including IoT and rogue devices. Quickly add them to your VM program for risk assessment | | |
| 45. | | Discover assets from Service Now, BMC Helix, Active Directory, Web hook, and more to add coverage and business context to your security program. Extract data such as asset criticality, device ownership, and assigned support group to drive risk prioritization | | |
| 46. | | The proposed solution should go beyond vulnerabilities to measure cyber risk - add risk factors such as EoL/EoS software, missing agents and security tools, unsanctioned ports, and expired SSL certificates to risk scoring to prioritize and eliminate business risk | | |
| 47. | | To be customized based on a Asset search query & tool able to convert  clicks to search query | | |
| 48. | | Allow user to customize the dashboard | | |
| 49. | | Widgets to be color coded so that user  can measure risk appetite | | |
| 50. | | Drilldown capability from the UI (User Interface) | | |
| 51. | | Must allow daily trending within a widget | | |
| 52. | | Flexible widgets like Pie chart, Bar chart, value based and list based | | |
| 53. | | Inventory visibility with search like querying | | |
| 54. | | query based asset and vulnerability search | | |
| 55. | | Must allow saving a query so that it can be re-used | | |
| 56. | | Able to provide asset details like bios, driver details, hostname etc. in the central dashboard. | | |
| 57. | | Should be able to convert a query into a widget | | |
| 58. | | Single Management Console with RBAC (Role Based Access Control) . User site / project/ asset group to be able to handle scanning reporting querying, asset group creation and deletion independently | | |
| 59. | | Easy deployment, Scalable and extendable | | |
| 60. | | Minimal impact on systems and networks | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 61. | | Ability to handle virtualized environments and Complete coverage for Container host, image and registry | | |
| 62. | | Provision to engine pooling with multiple engines grouped together to run any single scan to reduce and improve scanning time by load sharing | | |
| 63. | | Ability of Database queries to run against reporting data model. | | |
| 64. | | Scanning engine to be able to scan IPs simultaneously and the rest of the IP's /asset scheduled for scanning (in any site) to be able to put in the scanning queue and run automatically | | |
| 65. | | Solution should to be able to scan duplicate or overlapping IP ranges | | |
| 66. | | Minimum volume of 10 IP scan be scanned simultaneously by each scan engine | | |
| 67. | | Solution should monitor networks for unmanaged and unauthorized devices. | | |
| 68. | **Container Security** | | | |
| 69. | **Container Security** | The proposed solution must have container security for runtime protection by scanning containers for vulnerabilities. | | |
| 70. | | The proposed solution should support CI/CD build pipelines, container registry and running containers without compromising on performance of running containers | | |
| 71. | | The proposed solution should support clustered container orchestration environments like Kubernetes, OpenShift, Docker Swarm and managed services like AKS, ECS, EKS etc. | | |
| 72. | | The Proposed solution should support registry scanning of container images in registries like JFrog, Docker Private, ACR, ECR, GCR, GAR, Docker Hub, Quay etc. | | |
| 73. | | The Proposed solution should support multiple container runtime docker, container, cri-o. | | |
| 74. | | The Proposed solution should support integration with CICD tools like Jenkins, Bamboo, Azure DevOps, GitLab etc. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 75. | | The Proposed solution should support container scanning on standalone container hosts. | | |
| 76. | | The Proposed solution must have comprehensive APIs to manage containers. | | |
| 77. | | The Proposed solution should have the ability to do automatic discovery, Inventory of all the containers and images with all metadata. | | |
| 78. | | The Proposed solution should be able to create and view unified dashboard for container security. | | |
| 79. | | The Proposed solution should be able to view the issue in a dashboard and follow the remediation recommendations. | | |
| 80. | | The solution should have the ability to search for custom queries for filtering vulnerabilities in containers, images, Kubernetes labels and other metadata. | | |
| 81. | | The solution must show the association between discovered assets. | | |
| 82. | | The solution must provide drift detection between running containers and container images for vulnerabilities. | | |
| 83. | | The solution must provide drift detection between running containers and container images for software. | | |
| 84. | | The solution should give the remediation/fixes for vulnerabilities in containers. | | |
| 85. | | The solution should support dynamic scanning of containers with option to do static scanning. | | |
| 86. | | The solution must have container security which can detect secrets within container images. | | |
| 87. | | The solution should have container security which can detect malware threats within container images. | | |
| 88. | | The solution must have support for Software Composition Analysis (SCA) scanning<br>of container images for software like Java, Python, Go, Node.js, .NET, PHP, Ruby, Rust etc. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 89. | | The solution must have ability to detect all known vulnerabilities for image scans. | | |
| 90. | | The solution should support continuous vulnerability management for running container without need to manually trigger any scans. | | |
| 91. | | The solution must support scan on schedule functionality | | |
| 92. | | The solution must have option to scan all the images in all repositories of the registry. | | |
| 93. | | The solution must have option to scan images either on-demand or scheduled. | | |
| 94. | | The solution should have compliance checks for running containers. | | |
| 95. | | The solution must provide remediation for failed compliance checks. | | |
| 96. | | The solution should have ability to manage configurations, vulnerability management, compliance, access, and auditing in containerized environments. | | |
| 97. | | The solution must be able to create exceptions for required vulnerabilities, for specific images and containers. | | |
| 98. | | The solution should have comprehensive accessible vulnerabilities knowledgebase. | | |
| 99. | | The solution must have command line utility to scan the containers | | |
| 100. | | The solution should have integration in to major CICD tools like Jenkins, Azure DevOps, Bamboo, GitLab etc. | | |
| 101. | | The solution should have integrations into SIEMs, ticketing, even extensions into logging tools. | | |
| 102. | | Ability to automatically block builds based on policy violations | | |
| 103. | | The solution must have customizable data retention policy for container security agents, containers and images. | | |
| 104. | | The solution must have reporting functionality with on-demand or on schedule and possibility to use API. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 105. | | The solution must deliver detailed vulnerability information and environment context, including CVSS score, remediation steps, attack vector, attack complexity, listening ports etc. | | |
| 106. | | Same container sensor can be used for CICD, registry & general purpose | | |
| 107. | | The solution should support encryption: Strong encryption for data at rest and data in transit. | | |
| 108. | | The solution should provide a robust RBAC access to the portal for administrative and functional roles | | |
| 109. | **Vulnerability Management** | | | |
| 110. | Vulnerability Management | The proposed solution Should bring together all the key elements of an effective vulnerability management program into a single app unified by powerful out-of-the-box orchestration workflows | | |
| 111. | | The proposed solution Should enable organizations to automatically discover every asset in their environment, including unmanaged assets appearing on the network, inventory all hardware and software, and classify and tag critical assets. | | |
| 112. | | The proposed solution Should Continuously assesses these assets for the latest vulnerabilities and applies the latest threat intel analysis to prioritize actively exploitable vulnerabilities | | |
| 113. | | The proposed solution should detect and inventory all known and unknown assets that connect to global hybrid-IT environment – including, on-premises devices, mobile, endpoints, clouds, containers. | | |
| 114. | | The proposed solution should gather detailed information, such as an asset’s details, running services, installed software, and more and eliminate the variations in product and vendor names and categorize them by product families on all assets | | |
| 115. | | The proposed solution should analyse vulnerabilities and misconfigurations with six sigma accuracy | | |
| 116. | | The proposed solution should have CVE-to-detection mapping | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 117. | | The proposed solution should support CVSSv2 and CVSSv3 base scores. | | |
| 118. | | The proposed solution vulnerability knowledgebase should have at least 150+ detection logics | | |
| 119. | | The proposed solution should use advanced correlation and machine learning, automatically prioritize the riskiest vulnerabilities on the most critical assets | | |
| 120. | | The proposed solution should leverage MITRE ATT&CK Insights to identify. Leveraging MITRE ATT&CK involves, providing MITRE ATT&CK-based mappings, techniques, or visualizations where applicable. | | |
| 121. | | The proposed solution Should append real-time threat indicators (RTIs) to vulnerabilities, tapping findings from the solution and external sources | | |
| 122. | | The proposed solution should have Public Exploit, Actively Exploited, Actively Attacked, High Lateral Movement, EASY EXPLOIT, HIGH DATA LOSS, DENIAL OF SERVICE, NO PATCH, MALWARE, EXPLOIT KIT, Zero day and many more real-time threat indicators | | |
| 123. | | The proposed solution should have Live Threat Intelligence Feed and threat categorization | | |
| 124. | | The proposed solution should displays entire threat posture at a glance | | |
| 125. | | The proposed solution should group vulnerabilities that have public exploit available, can result in DoS and can propagate via lateral movement | | |
| 126. | | The proposed solution must have provision for search results to be further sorted, filtered and refined | | |
| 127. | | The proposed solution should make configurable dashboard with widgets from threat and asset query results | | |
| 128. | | The proposed solution should provide dynamic, customizable views with specific stats, such as assets with active zero-day vulnerabilities | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 129. | | The proposed solution should have shareable dashboards allow import / Export for reuse and sharing in open standard | | |
| 130. | | The proposed solution should Craft ad-hoc queries with multiple variables and asset criteria | | |
| 131. | | The proposed solution should support unlimited multiple sensors for inventory - virtual scanners, agents, container sensors etc for asset inventory | | |
| 132. | | The proposed solution should have an automated way to "Ignore" vulnerabilities with easy tracking for exception management and/or false positives | | |
| 133. | | The proposed solution should support authentication support for Linux, Windows, Network and Security devices (Checkpoint FW, Fotinet FW,CISCO FW, Palo Alto FW , Cisco APIC Infoblox, Network SSH, , SNMP), Applications (Apache, BIND, Docker, HTTP, Jboss, MS IIS, Kubernetes, NGINX, Tomcat, Oracle Weblogic etc.), Databases ( Azure MS SQL, Cassandra, IBM DB2, MariaDB, MongoDB, MS SQL, MySQL, Oracle, SAP HANA, PostgreSQL etc.), VMware for authentication | | |
| 134. | | The proposed solution should support integration with authentication vaults/PIM,PAM. | | |
| 135. | | The proposed solution support static and dynamic tagging for asset management, scanning and reporting | | |
| 136. | | The proposed solution should support API tier for SIEM, Risk Assessment solution, SNOW SecOps, ITSM & many more | | |
| 137. | | The proposed solution should have the capability for Automatic correlation between CVE and Patch KB | | |
| 138. | | The proposed solution should be able to assess the digital certificates (internal and external) and TLS configurations for certificate issues and vulnerabilities | | |
| 139. | | The proposed solution should give the visibility of risk reduction trend for last 90 days, contributing factors and overall risk score | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 140. | | The proposed solution should quantify the risk against the vulnerability and associated attributes like cvss, vulnerability trend, malware, threat actors, RTIs, associated CVE IDs, | | |
| 141. | | The proposed solution should support out of box query/token for assets and vulnerabilities like threat hunting any asset with vulnerability having remote code execution or ransomware associated to it | | |
| 142. | | The proposed solution should have the capability to assign business context/criticality to the asset which should give overall risk score on the asset and organization | | |
| 143. | | The proposed solution should be transparent in showcasing the formula which is being used for risk calculation | | |
| 144. | | The proposed solution should have option to group the vulnerabilities basis on name, age, severity, cvss rating, vendor, vendor product name, OS, status, malware name, RTIs, Public exploit, exploit kit etc. | | |
| 145. | | The proposed solution should have Option to group the assets basis on OS, software, tags, last logged in user, created, last seen etc. | | |
| 146. | | The proposed solution should have visibility and transparency into proprietary and open-source dependencies within the software supply chain. | | |
| 147. | | The proposed solution should have option to users to exclude vulnerabilities related to Information gathered, Fixed, non-running kernel, 3rd party detections, etc. from the UI and reports. | | |
| 148. | | The proposed solution should have capability to prioritize the vulnerabilities basis on vulnerability age, real-time-threat indicators and attack surface | | |
| 149. | | The proposed solution should have Option to generate the reports for the prioritized vulnerabilities and should be able to add it in the dashboard for tracking | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 150. | | The proposed solution should have ability to automatically co-relate the asset to vulnerability to patch details | | |
| 151. | | The proposed solution should perform discovery/map scan, EC2 scan, cloud perimeter scan, debug scan, vulnerability scans etc. | | |
| 152. | | The proposed solution should have the list of approved, scannable, live host as on outcome of discovery/map scan | | |
| 153. | | The proposed solution should have ability to schedule discovery/map scans and vulnerability scans and sent the notifications. | | |
| 154. | | The proposed solution should have ability to configure the profiles for discovery/map and vulnerability scans | | |
| 155. | | The proposed solution should have ability to create custom lists of vulnerabilities that can be saved and used in order to customize vulnerability scans, reports and ticket creation | | |
| 156. | | The proposed solution should have ability to discover and assess the risk of embedded open-source software (OSS) vulnerabilities. It should also identify, prioritize & respond to vulnerabilities in open-source embedded packages in production from day zero | | |
| 157. | | The proposed solution should  leverage insights from over 25+ threat sources to receive pre-emptive alerts on potential attacks with the product's Thread DB | | |
| 158. | | The proposed solution should have ability to generate detailed, easy-to-comprehend customizable reports which may be exported to HTML, MHT, PDF, CSV, and XML formats. | | |
| 159. | | Reports should able to provide:<br>- detailed vulnerability assessment with complete view of new, existing, and fixed vulnerabilities.<br>- most current information about remediation progress and vulnerability status<br>- overall security status of your hosts and many more | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 160. | | There should be multiple pre-defined scan reports that simplify report generation and provide immediate access to your most critical vulnerability information. These reports are available to you at any time:<br>- SANS Top 20 Report<br>- Real Vulnerabilities Top 10<br>- Executive Report<br>- Technical Report<br>- PCI Technical and Executive Reports<br>- High Severity Report | | |
| 161. | | The proposed solution should have ability to scan a host (wherever applicable) with agent and scanner both consuming only single license | | |
| 162. | | The proposed solution should have ability  to provide exhaustive RBAC and give flexibility to users to create custom roles | | |
| 163. | | The proposed solution should have ability to provide remediation suggestion in the scan reports | | |
| 164. | | The proposed solution should have ability to suffice the requirement to conduct agent and scanner based scans to cover the complete detections supported in the product | | |
| 165. | | The proposed solution should  support:<br>Agent-based detection (On prem)<br>Agentless detection (On prem)<br>Agent Support Windows (client and server versions)<br>Agent Support Linux and Unix | | |
| 166. | | The proposed solution should have configurable monitoring and alerting features | | |
| 167. | | The proposed solution should have support Cloud Workloads in Azure/VMware/OpenStack PaaS on premises | | |
| 168. | | The proposed solution should  support CI-CD pipelines for build tools like Bamboo, Jenkin, GitLabs, etc. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 169. | | The proposed solution’s agent and scanner should communicate directly with Management server over encryption | | |
| 170. | | The proposed solution should  allow defining policy for console access with IP whitelisting | | |
| 171. | | The proposed solution should have ability to track the status of vulnerability with each iterative scan | | |
| 172. | | The proposed solution should have auto updating & self-managing scanners and agents | | |
| 173. | | The proposed solution should have  ability to auto-eliminate superseding patches | | |
| 174. | | The proposed solution should have APIs, Scripts/Tools and zero touch deployment of scanner and agent | | |
| 175. | | The proposed solution should  provide information if the vulnerability has a patch or virtual patch available | | |
| 176. | | Report generation through API | | |
| 177. | | User login should supported with 2 factor authentication (in built in product) or domain credentials/SAML (organization's policy) | | |
| 178. | | Scan result database should be encrypted | | |
| 179. | | VA Scanners running on hardened OS | | |
| 180. | | The proposed solution should have ability to track ongoing progress against vulnerability management objectives | | |
| 181. | | The proposed solution agent should be able to use a proxy and do data compression | | |
| 182. | | The proposed solution VA Scanner should be able to check credentials authentication before launching scan | | |
| 183. | | The proposed solution scanner should have password less key communication to run agent and communicate between them, no physical password should be shared from user | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 184. | | User should be alerted right away about vulnerabilities, misconfigurations and other issues that can put you at risk of breaches, including:<br>1. Unexpected hosts/OSes<br>2. Expiring SSL certificates<br>3. Inadvertently open ports<br>4. Severe vulnerabilities<br>5. Remediation tickets<br>6. Undesired software and many more use cases | | |
| 185. | | The proposed solution should have monitoring features for:<br>1. Provision to detect and alert new assets in the network<br>2. Provision to targeted alerts based on a security policy<br>3. Certificate data insight and certificate based vulnerabilities<br>4. Provide alerts based on threat intelligence<br>5. Provision to monitor SSL certificates and alert on expiring SSL certificate | | |
| 186. | | The proposed solution should have generic features of monitoring:<br>1. Target alerts for each issue to the people responsible for fixing them<br>2. Provision of calendar based alerts dashboard<br>3. Provide alert rule creation using AND / OR / ONLY-IF kind of logic<br>4. Reduced risk of system changes going unnoticed<br>5. Provide alerts via email and CEF(Common Event Format)/Syslog<br>6. Provide alerting for both External and Internal IPs | | |
| 187. | Agent Specific Features | Proposed agent should enable instant, global visibility of IT assets – even occasionally connected virtual devices, with up-to-date asset configuration data for security and compliance. | | |
| 188. | | Proposed Agent should provide a continuous view of assets for vulnerability management, policy compliance, and asset inventory | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| | | without the need for credential management, and firewall changes required by network scanner deployments. | | |
| 189. | | Proposed agent should deliver visibility and security solutions for assets that are not able or not easily scanned from the network including remote/roaming users, distributed offices, and cloud server instances. | | |
| 190. | | Proposed agent should be lightweight and designed to minimize resource consumption, ensuring that performance of applications and virtual machines is not adversely impacted. | | |
| 191. | | Proposed agent should be light weight, have a low-footprint which should bring the high-performance functionality of the platform, built in configurations for central management | | |
| 192. | | Proposed agent should have real-time actionable data collection with customizable configuration profile. This requirement can provided by the solution suite that delivers the intended functionality. | | |
| 193. | | Proposed solution must have continuous evaluation and data enrichment on platform for comprehensive security and compliance, seamless API integration | | |
| 194. | | Proposed Agents must be designed to capture OS and application metadata, including installed applications, registry keys, running processes, and system configurations. | | |
| 195. | | The agent should perform continuous monitoring/assessment. The agent shouldn't consume excessive resources, ensuring that the performance of running applications/VMs is not compromised. The resource overhead (hardware, software) for the agent should not exceed 5% of the normal requirement of the CPU. There should be only one agent. Proposed agent utilization must be configurable. | | |
| 196. | | Agent data should be uploaded to the solution's Platform for assessment, analysis, correlation, reporting, and alerting. Data | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| | | “snapshot” transmissions to the platform focus on detected changes (deltas) | | |
| 197. | | Agent should serve primarily as a “data collector” for all the supported applications. Assessment testing and data enrichment should be performed on the product's platform. | | |
| 198. | | Agent's design should focus on "One Agent - Multiple Capabilities" which means same agent should be performing inventory, vulnerability, compliance, asset management (including security use cases), Software Composition Analysis (SwCA), Passive Sensing etc. (assuming required licenses/modules are procured) | | |
| 199. | | The proposed solution should provide the option to deploy a virtual appliance which should act as a forward proxy for the agents. | | |
| 200. | | Agent communication is optimized to support large scale agent deployments while providing flexible and granular performance configuration controls allowing organizations to tune agent performance and bandwidth usage for their specific environment requirements | | |
| 201. | | All communications should be initiated by the agent outbound from the agent to the platform using REST over HTTPS/TLS on configurable intervals. | | |
| 202. | | Performance parameters should be configurable in the profiles and should be assigned to assets by direct assignment or tags. | | |
| 203. | | The agent should support techniques for CPU performance management. | | |
| 204. | | The agent should support CPU Throttle/CPU Limit to insert a sleep delay between subsequent metadata collection commands executed by the agent. | | |
| 205. | | Agent should be able to auto-upgrade itself whenever a new version is made available | | |
| 206. | | Agent should support communication suppression /blackout windows either manually or scheduled. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 207. | | The proposed solution should have a separate UI on the same platform to track agent based assets and associated details | | |
| 208. | | The proposed solution must have ability Enabling and disabling the modules done swiftly from the UI itself | | |
| 209. | | Users should have the liberty to generate unlimited "keys" for segregation and effective tracking | | |
| 210. | | Agent's profile should have the option to prevent auto upgradation | | |
| 211. | | Agent's profile should have the option to configure - Scan Performances ( Data Collection Interval, Scan Delay, Scan Randomize) | | |
| 212. | | Agent's profile should have the option to configure performances and customize parameters - Agent Status Interval, Delta Upload Interval, Chunk Size for File Fragment Uploads, Logging Level for Agent, CPU Limit (for Windows) , CPU Throttle (for Unix/ Linux) | | |
| 213. | | The proposed solution should be able to merge the scan data from agent and scanner and provide a single instance for the vulnerability. | | |
| 214. | | Agent should be activated/deactivated from the central management console through UI, provisioned by the bidder. | | |
| 215. | | Agent module should be able to enable/disable self-protection feature to prevent it from tampering | | |
| 216. | | The proposed solution should be able to perform on-demand scans - inventory, vulnerability, policy compliance, SCA etc. | | |
| 217. | | Users should be able to uninstall the agents which are not reporting to the platform automatically or manually from the UI | | |
| 218. | | Agent should be self updating and tamper resistant | | |
| 219. | **Policy Compliance** | | | |
| 220. | Hardening & Compliance | Technology Coverage:<br>1. Host<br>2. OS<br>3. Network Device<br>4. Security Device | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| | | 5. Storage Device<br>6. Database<br>7. Application<br>8. Containers<br>9. Mobile OS | | |
| 221. | | The proposed solution should provide database scanning coverage for at least following database platforms: MS-SQL, MySQL, Oracle, PostgreSQL, MongoDB, MariaDB. | | |
| 222. | | The proposed solution should support the following reporting but not limited to<br>1. Customizable reports<br>2. Scheduled Reports<br>3. CIS (Centre For Internet Security) | | |
| 223. | | Support Reporting Formats<br>1. PDF<br>2. CSV | | |
| 224. | | The proposed solution should supports CIS Benchmark for:<br>1. Databases<br>2. Network Firewalls<br>3. UTM Device<br>3. IPS (Intrusion prevention system)<br>4. DDOS (Distributed denial of service)<br>5. Routers<br>6. Switches<br>7. WAF (Web Application Firewall)<br>8. Load Balancer | | |
| 225. | | The proposed solution should be a next-generation cloud solution for continuous risk reduction and compliance with internal policies and external regulations. | | |
| 226. | | The proposed solution should allow the users to leverage out-of-the-box library content to fast-track compliance assessments using | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| | | industry-recommended best practices such as CIS Benchmarks, DISA, STIG, vendor specific, mandates etc. covering 700+ Policies, 18000+ Controls, Over 200 technologies, 70+ mandates for configuration management | | |
| 227. | | The proposed Solution should automate the evaluation of requirements against multiple standards for OSes, network devices, and applications, PC lets you identify issues quickly and prevent configuration drift | | |
| 228. | | The proposed solution should able to auto-discover running middleware & databases even from their custom locations, for multiple instances, with meta data ranging from versions to execution paths and assess them for their security and compliance posture. | | |
| 229. | | The proposed solution should able to provide "At-a-glance" view of security and compliance posture of the assets based on control criticality, CVE detection, CIS IG, as well as the MITRE ATT&CK tactics and techniques | | |
| 230. | | The proposed solution should provide mandate-based reporting (CIS, ISO/IEC, National Information Assurance Policy, NIST, PCI, RBI, NIST CSF, CMMC etc.) to simplify the process of reporting on the compliance posture of the organization across regulations, standards, and guidelines. | | |
| 231. | | The proposed Solution should support User Defined Controls and Customization of Policies. It should ease to use wizard driven process to create custom controls and policy editor to quickly tailor pre-defined policies from the library to organizational needs. | | |
| 232. | | The proposed solution should support Centralized Exception Management to provides a documented, repeatable workflow for requesting, evaluating. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 233. | | The proposed solution should offer own security hardening policies for technologies for which no benchmark or vendor security guidelines are available | | |
| 234. | | The wide range of support should also include web servers such as IBM WebSphere, Apache Tomcat, Apache HTTP Server, WebLogic, IBM HTTP Server, and JBoss EAP etc. | | |
| 235. | | The support should also extend browsers and productivity tools such as Microsoft Office applications, which are the most used applications in any organization. | | |
| 236. | | The proposed solution should allow users to create their own controls dynamically, as needed, without having to submit control requests to solution's development team | | |
| 237. | | The proposed solution should support at least following scripting languages — Perl, Shell, Python, PowerShell, VBScript — with no vendor-specific syntax or restrictions. | | |
| 238. | | Accelerated compliance audits and assessments for FedRAMP, PCI, SOX, HIPAA, FINRA, GDPR, NYDFS, CCPA, and many other regulations | | |
| 239. | | The proposed solution should provide Real-time, dynamic dashboards showing true compliance picture, Executive Reporting - View overall compliance Posture and download reports from Posture tab. | | |
| 240. | | The proposed solution should prioritize based on criticality and other factors for quick remediation of the highest risk asset. | | |
| 241. | | The proposed solution should integrate with the VM solution to prioritize configurations as compensatory controls, where vulnerability cannot be patched immediately, to reduce vulnerability risks | | |
| 242. | | The proposed solution should provide a centralized console to perform threat hunting via multiple Asset and Controls tokens | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 243. | | The proposed solution’s components should be able to give compliance visibility without adversely impacting the performance of applications or virtual machines | | |
| 244. | | Same set of authentication record (admin/root) which is created for VM scans should suffice ask for compliance scans | | |
| 245. | | The proposed solution should be able to provide option to schedule scans and reporting | | |
| 246. | | The proposed solution should be able to provide policy summary on the UI giving visibly into controls evaluated, pass/fail controls, control severity, top failing hosts and controls. | | |
| 247. | | The proposed solution should be able to raise exceptions and track the exceptions on the UI | | |
| 248. | | The proposed solution should be able to provide exhaustive RBAC and give flexibility to users to create custom roles. | | |
| 249. | | The proposed solution should able to integrate with other 3rd party solution via API | | |
| 250. | | Easily define configuration policies required for different environments and assets | | |
| 251. | | Use SCAP content streams | | |
| 252. | | Create custom policies | | |
| 253. | | Leverage custom controls in library policies | | |
| 254. | | Scan on demand or on a schedule | | |
| 255. | | Report anytime and in any way required, without rescanning systems | | |
| 256. | | Compare compliance rates across policies, technologies and assets | | |
| 257. | | Create different reports for different audiences | | |
| 258. | | Enable data-driven risk & compliance management | | |
| 259. | | Share data with GRC systems & other enterprise applications | | |
| 260. | | Tool should be able to convert running golden image of hardened OS into policy template | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| 261. | | | | |
| 262. | HARDWARE AND SYSTEM SOFTWARE REQUIREMENT FOR VA SCANNER AND CENTRAL MANAGEMENT | | | |
| 263. | Hard Disk Space Required | As Required | | |
| 264. | RAM Size required | As Required | | |
| 265. | CPU required | As Required | | |
| 266. | Supported Operating Systems | As Required | | |
| 267. | **GENERIC PARAMETERS** | | | |
| 268. | Free Upgradation to Higher Version within support period including API, Firmware, Signatures, etc. | YES | | |
| 269. | OEM to provide Certification on-site | Yes | | |
| 270. | If yes, no. of users to certify | 5 | | |
| 271. | **ATC Clauses** | | | |
| 272. | **ATC Clauses** | Agent Support Windows (all client and server versions) | | |
| 273. | | Agent Support Linux and Unix | | |
| 274. | | Agent Support Mac OS | | |
| 275. | | 1. Bidder must establish complete VA scan setup at the premises of the Purchaser/NIC Data Centre. The complete VA scan setup should include:<br>2. Required software and other prerequisites like Software scanner and Central management console.<br>Note: a. Required Infra (VMs, Networking equipment, Storage, backup hardware etc.) shall be provided by the MSP on premise)<br>b. The bidder should establish their scanner on premise at NIC Data | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| | | Centre for VA scan of the servers deployed at Data centre for 50,000 host based/IP based scanning and for 1000 container image/ host.<br>c. The bidder should establish and provide complete solution for achieving the scanning and other functionalities which shall include but not limited to, required prerequisite like Software scanner, Central management for correlating the vulnerabilities with threat and generating the reports and storage for the Vulnerabilities must be provided<br>d. The bidder should be responsible for management, monitoring and administrative activities of entire solution for which, onsite and/or remote support shall be provided by the bidder as per requirement. Also day to day VA scan activities shall be done by MSP. | | |
| 276. | | **Central Management** | | |
| 277. | | 1. Must provide a dedicated central management solution for management of VA solution in HA at NDC New Delhi.<br>2. Virtual scanner must be provided at NDCSP Delhi, and NDC Bhubaneswar, NDC Pune and NDC Hyderabad along with underlying Hardware.<br>3. Underlying ICT Infrastructure (Hardware and software) to run the VA software must be supplied by MSP along with VA solution.<br>4. All software, licenses etc. to be supplied for establishing complete solution by the bidder on premise.<br>5. The Management solution must have the capability to store and analyse logs for a minimum period of 90 Days.<br>6. The proposed solution must have the capability to manage minimum 50,000 assets and adequate licenses for managing these assets must be supplied from Day 1.<br>7. The proposed solution should have access through GUI and user management must be based on RBAC. | | |

| Sr. No | KEY | Minimum Specification | Compliance (Yes/No) | References(Document/ Page No) |
|---|---|---|---|---|
| | | 8. The proposed solution should support API for automation<br>9. The solution must support a web-based GUI centralised management for primary and secondary instances.<br>10. The centralised management must support management of software upgrades on both primary and secondary instances. | | |

## 14. Annexure: Format for 'Malicious Code Free' Certificate

**Format for Bidder**

(To be provided on Bidder letter head)

Tender Ref. No.: ________________________________ Date: ___________

To,
Tender Division,
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 trojan 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 and Seal:

**Format for OEM**

(To be provided on OEM letter head)

Tender Ref. No.: ________________________________ Date: ___________

To,
Tender Division,
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 trojan 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: | Authorised Signatory: |
| Place: | Name of the Person: |
| | Designation: |
| | Firm Name and Seal: |

## 15. Annexure: Undertaking to be submitted by OEM

**OEM UNDERTAKING**

This is to certify that 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 Enterprise support for **Seven Years** from the date of delivery to the Purchaser.

Submitted on behalf OEM Name:

Name of Authorised Signatory:

Designation of Authorised Signatory:

Signature and Seal of the OEM Authorised person:

Place:

Date:

Note:
*The letter shall be submitted on the letter head of the manufacturer / OEM and shall be signed by the authorised signatory*

## 16. **Annexure: 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 Centre. (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 Selection of Managed Service Provider for setting up Cyber security solutions for National Data Centres (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 and 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. Sanctions for Violations**

5.1 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 (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.

5.2 The Purchaser will be entitled to take all or any of the actions mentioned at para 5.1 (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.

5.3 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.

**6. Fall Clause**

6.1 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.

**7. Independent Monitors**

7.1 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>

7.2 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.

7.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

7.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

7.5 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.

7.6 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.

7.7 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.

7.8 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.

**8. 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.

**9. Law and Place of Jurisdiction**

This Pact is subject to Indian Law. The place of performance and jurisdiction is New Delhi.

**10. 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.

**11. Validity**

11.1 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. The validity of this Integrity Pact shall be from date of its signing and extend up to ___ 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.

11.2 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.

**12. The parties hereby sign this Integrity Pact at on**

| | |
|---|---|
| Bidder | |
| Name of Officer | |
| Designation | |

| WITNESS | WITNESS |
|---|---|
| 1. | 1. |
| 2. | 2. |

Note:-

1. 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.

2. The MSP shall submit the integrity pact along with the technical bid.

## 17. **Annexure: Format for Change Control Note**

| | | | | |
|---|---|---|---|---|
| Please attach any paper required to support this Change Request | | | | |
| RFP Reference | | | | |
| Subject | | | | |
| Change No. | Change Requested By | Request Date | Required by Date | Proposed Implementation Date |
| | | | | |
| Justification | Type of Change | | | |
| | Requested Change | | | |
| | Reason for Change | | | |
| | | | | |
| CR Classification | | | | |
| Priority: (Choose P1 TO P3) | Severity | Component name: | | |
| | High | | | |
| | Medium | Details (if any): | | |
| | Low | | | |
| Area | Impact of Proposed Change | | | |
| | Note: If possible, provide details of impact in terms of days/INR | | | |
| Impact | Impact on Cost (Estimated cost for each component and justification for the same) | | | |
| | Impact on Data centre operations including risks and issues | | | |
| | Impact on Schedule | Schedule Date | Proposed New Date | |
| | | | | |
| Conclusion for consideration of NIC: | | | | |

## 18. **Annexure: Covering Letter**

<To be submitted on the letter head of the Bidder>
<Place>
<Date>

To,
Tender Division,
National Informatics Centr,
1st Floor, NBCC Tower,
15 Bhikaji Cama Place,
New Delhi -110066
Tel: 011-22900534/35

**Subjec**t: Submission of Bid Request  Proposal for Selection of Managed Service Provider for setting up Cyber security solutions for National Data Centres( Tender ID: _________)

Dear Madam/Sir,

This is to notify that our company is submitting technical Bid in response to Tender No…………….for RFP………………………………………….
Primary and 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 Purchaser on time.
2. We are submitting our Bid for RFP for ……………………………., 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 Purchaser 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 and S/W, Cost for comprehensive security Audit of entire supplied and deployed components, Cost incurred for Training and 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 and 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.
   iii. 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.
b. We certify that we fulfil any other additional eligibility condition if prescribed in Tender Document.
c. 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:
   ii. we are not from such a country or, if from such a country, we are registered with the Competent Authority (copy enclosed) and;
   iii. 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 and Title of signatory:
Name of Firm:
Address:
Seal/Stamp of the Bidder:
Place:
Date:

# Form 1.2: Eligibility Declarations

(To be submitted as part of Technical bid)

(On Company Letter-head)

(Along with supporting documents, if any)

Tender Document No. Tend No./ xxxx; Tender Title: --------------
Bidder's Name__________________________
[Address and Contact Details]
Bidder's Reference No.____________________________ Date……….

Note: The list below is indicative only. You may attach more documents as required to confirm your eligibility criteria.

## Eligibility Declarations

(Please tick appropriate boxes or cross out any declaration not applicable to the Bidder)

We hereby confirm that we are comply with

The Bidder, unless otherwise

1) **Legal Entity of Bidder: ___________________________**
2) **OEM/ Manufacturer/ Agent/ Dealership Status:**
3) **We ¨ are/ ¨ are not a JV________________________________________**

4) **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

b) (including our Contractors/ subcontractors for any part of the contract):

   a. Do not stand declared ineligible/ blacklisted/ banned/ debarred by the Procuring Organisation or its Ministry/ Department from participation in its Tender Processes; and/ or

   b. 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.
   c. Do not have any association (as bidder/ partner/ Director/ employee in any capacity) with such retired public official or near relations of such officials of Procuring Entity, as counter-indicated, in the Tender Document.
   d. We certify that we fulfil any other additional eligibility condition if prescribed in Tender Document.
   e. 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.

5) **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:**

We certify as under:

"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:

a. we are not from such a country or, if from such a country, we are registered with the Competent Authority (copy enclosed). and;

b. we shall not subcontract any work to a contractor from such countries unless such contractor is registered with the Competent Authority.

**6) MSME Status:**

Having read and understood the Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 (as amended and revised till date), and solemnly declare the following:

a. We are - Micro/ Small/ Medium Enterprise/ SSI/ Govt. Deptt. / PSU/ Others:…………..
b. We attach herewith, Udhyam Registration Certificate with the Udhyam Registration Number as proof of our being MSE registered on the Udhyam Registration Portal. The certificate is the latest up to the deadline for submission of the bid. Whether Proprietor/ Partner belongs to SC/ ST or Women category. (Please specify names and percentage of shares held by SC/ ST Partners):…………….

**7) Start-up Status**

we confirm that we ¨ are/ ¨ are not a Start-up entity as per the definition of the Department of Promotion of Industrial and Internal Trade – DPIIT.

8) **Make in India Status:** Having read and understood the Public Procurement (Preference to Make in India PPP - MII) Order, 2017 (as amended and revised till date) and related notifications from the relevant Nodal Ministry/ Department, and solemnly declare the following:

**9) Self-Certification for the category of suppliers:**

(Provide a certificate from statutory auditors/ cost accountant in case of Tenders above Rs 10 Crore for Class-I or Class-II Local Suppliers). Details of local content and location(s) at which value addition is made are as follows:

| | |
|---|---|
| Local Content and %age | |
| Location(s) of value addition | |

Therefore, we certify that we qualify for the following category of the supplier (tick the appropriate category):

Class-I Local Supplier/
Class-II Local Supplier/
Non-Local Supplier.

a) We also declare that

I. There is no country whose bidders have been notified as ineligible on a reciprocal basis under this order for an offered Goods, or

II. We do not belong to any Country whose bidders are notified as ineligible on a reciprocal basis under this order for the offered Goods.

a. Self-Declaration by Indian Agents/ Associates of Foreign Principals

a. Self-attested documentary evidence about their identity (PAN, Aadhar Card, GSTIN registration, proof of address, etc.), business details (ownership pattern and documents, type of firm, year of establishment, sister concerns etc.) to establish that they are a bonafide business as per Indian Laws – are submitted as part of Company profile.

b. Agency Agreement shall be submitted with Form 1.4. It shall cover (i) the precise relationship, services to be rendered, mutual interests in business - generally and/ or specifically for the tender and

(ii) any payment the agent or associate receives in India or abroad from the foreign OEM/ principal, whether a commission or a general retainer fee.

c. Our Foreign principals, explicitly authorizing us to make an offer in response

to the tender, either directly or in association with them, are listed in **OEM Authorization** and **Declaration by Agents/ Associates of Foreign Principals** annexed herewith. That also indicates their name, address, nationality, status (i.e., whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal).

d. The amount of commission/ remuneration included in the price (s) quoted by Bidder for agents or associated bidder is detailed in **Declaration by Agents/ Associates of Foreign Principals** Confirmation is given in **Declaration by Agents/ Associates of Foreign Principals** annexed herewith from the foreign principals that the commission/ remuneration, reserved for Bidder in the quoted price(s), if any, shall be paid by the Procuring Entity in India, in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Goods and Spares.

**10) Penalties for false or misleading declarations:**

We hereby confirm that the particulars given above are factually correct and nothing is concealed and undertake to advise any future changes to the above details. We understand that any wrong or misleading self-declaration would violate the Code of Integrity and attract penalties as mentioned in this Tender Document.

…………………..

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of

……………………………………….
……………………………………….
[name & address of Bidder and seal of company]
DA: As in Sr 9 to 14 above, as applicable