WATER RESOURCES DEPARTMENT
GOVERNMENT OF BIHAR
OFFICE OF JOINT DIRECTOR
Flood Management Improvement Support Centre,
Jal Sansadhan Bhawan, Anisabad, Patna-02
fmiscbihar@gmail.com

Scope of Work

Bidders' Responsibilities for Storage Upgrade & Integration :
Dell SAN Storage

- Supply of additional SAN Storage with SSD (30 TB of usable space) along with necessary enclosure and accessories for Dell Unity 450F SAN Storage.
- Upgrade the existing Storage with **30 TB SSD (Usable Capacity)** and integrate the same with existing **SAN storage (Dell Unity 450F.)** as per technical Specifications.
- Configure RAID groups, storage pools, and LUNs for **30TB usable SSD storage**.
- Ensure **seamless connectivity with exiting application & virtualisation infra..**
- Verify storage **visibility and accessibility** within vSphere.
- Setup and configure backup for the entire storage.
- Implement **performance and security best practices**.
- Bidder assumes full responsibility for **data loss and any harm to SAN** during the upgrade.
- Bidder assumes full responsibility for implementation of feature such as snapshot, data replication, thin provisioning, and virtualization across the entire storage system.
- Ensure an OEM-provided comprehensive on-site warranty for 3 years, covering all hardware and software components.
- Bidder should provide 24x7 support with clear Service Level Agreements (SLAs) for response and resolution times.

Dell NAS Storage

- Supply and Upgrade and integrate **100TB usable NAS storage** consisting of **80TB SAS + 20TB SSD** into the existing **Dell NX NAS storage.**
- Ensure **seamless integration and functionality**.
- Configure RAID groups, storage pools & NFS(as applicable) **storage**.
- Setup and configure backup for the entire storage.
- Bidder assumes full responsibility for **data loss and any harm to NAS** during the upgrade.

Bidders' Responsibilities for DELL EMC Backup Appliance (DD6300 With Networker):

- Upgrade and integrate **100TB usable backup storage** into the existing **Dell EMC DD6300.**
- Ensure backup appliance functions seamlessly with existing infrastructure.
- 3 years on-site warranty supports.
- The bidder must enclose along with technical bid, OEM authorization specific to this tender and technical compliance duly approved by the OEM, failing which the bid offer will summarily be rejected.

1. Implementation & Configuration

- **Rack mounting and cabling (Fiber/iSCSI)** in the bidder's scope.
- **Power-on and initial firmware/software upgrade** (if required).
- Configure and validate **backup and replication integration.**
- Ensure the entire solution is operational and meets **stipulated performance standards.**
- 3 Years **OEM** Warranty NBD supports for new system or co-terminus with the Base storage system if existing system is upgraded.

2. Backup Software & Licensing

- Ensure **supplied licenses** match the existing **Backup software (Networker)** for seamless integration.
- The combined licenses must support **original and augmented storage.**
- Upgrade **Networker Backup software** with **capacity/socket-based licenses** to cover the entire infrastructure.

3. Ongoing Maintenance & Support

Scheduled Preventive Maintenance (Quarterly)

- Verify **RAID configurations and health.**
- Monitor **storage pools, disk utilization, and redundancy**.
- Upgrade firmware for **controllers, storage drives, and management modules.**
- Check **IOPS, latency, and throughput** metrics for performance benchmarking.

Issue Resolution & Hardware Replacement

- **OEM must replace failed components** (disks, power supplies, controllers, fans, etc.)
- Troubleshoot **hardware/software errors** affecting performance or causing downtime.
- Ensure **compatibility of replaced components** with the current system.
- Provide **onsite technical support** for critical failures within the SLA response time.

Proactive Monitoring & Performance Optimization

- Configure **alerts for critical issues** (disk failures, storage pool thresholds, performance bottlenecks).
- Identify and address **potential issues using predictive analytics.**
- Proactively replace components showing early signs of failure.
- Optimize **tiering strategies** to maximize storage resource utilization.
- Identify and resolve **performance bottlenecks in high-traffic environments.**

Security & Compliance

- Conduct **regular audits** of access controls and encryption configurations.
- Apply **security patches** to address vulnerabilities.

4. **Service and Support**

- **24/7 support** via email, phone, or ticketing system.
- Replacement of defective parts **at no additional cost**.
- Assist with **data migration** during hardware upgrades or transitions.
- Service provider must have necessary **maintenance tools/kits** (e.g., hoover, blower, brushes, etc.).

Scope of Work for Augmentation:-

General Overview

The selected vendor/bidder will be responsible for the deployment, installation, configuration, and integration of security solutions to enhance the organization's cybersecurity posture. This includes augmentation of the following components:

- **Web Application Firewall (WAF)**
- **Distributed Denial of Service (DDoS) Protection**
- **Security Information and Event Management (SIEM) / Log Server**
- **Network Time Protocol (NTP) Server**

The vendor must ensure seamless integration with the existing infrastructure, proper security hardening, and adherence to best practices.

Bidders' Responsibilities for WAF :

1. **Compliance and Proposal Submission:**
   a) Ensure full compliance with all technical, security, and operational requirements specified in the RFP.

b) Provide a detailed compliance statement for each specification, including the proposed make and model of the Web Application Firewall (WAF) solution.

c) Submit a comprehensive technical proposal detailing the architecture, deployment strategy, and integration approach of the WAF solution.

2. **System Design and Solution Architecture:**

   a) Propose a robust WAF solution capable of protecting web applications against common threats including OWASP Top 10, zero-day attacks, and advanced persistent threats (APTs).

   b) Ensure the solution supports both on-premises and cloud-based deployment models, providing hybrid flexibility if needed.

   c) The WAF should offer features like application layer protection, bot mitigation, API security, and web application threat intelligence.

   d) Design the architecture to include automatic threat detection, traffic analysis, SSL/TLS inspection, and integration with existing security infrastructure.

   e) Incorporate redundancy and high availability to maintain service continuity during failover scenarios.

3. **Supply, Installation, and Commissioning:**

   a) Supply all necessary hardware, software, and accessories required for a complete WAF deployment, including appliances, management software, and network components.

   b) Perform installation, configuration, and commissioning of the WAF solution, ensuring seamless integration with web servers and existing network infrastructure.

   c) Implement security rules, traffic filtering, and protection mechanisms to safeguard web applications without impacting legitimate user access.

d) Configure traffic monitoring and alerting features to provide real-time threat visibility.

4. **Configuration and Integration:**

   a) Configure security policies, virtual patching, threat signatures, and automated response mechanisms.

   b) Integrate the WAF with existing security tools, including SIEMs, firewalls, and intrusion prevention systems (IPS).

   c) Implement advanced threat protection features such as behavior-based detection, rate limiting, and session tracking.

   d) Establish API security policies, including authentication, rate limiting, and data validation.

5. **Testing and Validation:**

   a) Conduct comprehensive testing, including simulated attack scenarios to validate the WAF's detection and mitigation capabilities.

   b) Perform load testing to assess the system's ability to handle high traffic volumes without performance degradation.

   c) Provide detailed test reports, including metrics on response times, false positive rates, and the efficiency of security policies.

   d) Facilitate acceptance testing with the client's technical team to ensure compliance with performance and security standards.

6. **Warranty and Support:**

   a) Ensure a comprehensive warranty for all hardware and software components of the WAF solution.

   b) Provide 24x7 support with clear Service Level Agreements (SLAs) for incident response and resolution times.

c) Offer local service support to minimize response times and facilitate on-site assistance if needed.

d) Include software updates, threat intelligence feed subscriptions, and maintenance services as part of the warranty.

7. **Post-Implementation Support:**

   a) Provide ongoing support services, including monitoring, threat intelligence updates, and regular system health checks.

   b) Establish automated alerting and reporting mechanisms to keep the client informed of potential threats and system performance.

   c) Offer proactive maintenance, including firmware updates, patch management, and performance tuning.

The bidder must take full responsibility for delivering a robust, scalable, and reliable WAF solution that ensures the security of web applications, minimizes risks of data breaches, and enhances the client's overall cybersecurity posture.

Bidders' Responsibilities for DDoS Protection :

1. **Compliance and Proposal Submission:**

   a) Ensure complete compliance with all technical, functional, and security requirements specified in the RFP.

   b) Provide a detailed compliance statement (Yes/No) against each specification, including the proposed make and model of the offered DDoS mitigation solution.

   c) Submit a comprehensive technical proposal outlining the architecture, deployment strategy, and integration approach for the proposed DDoS solution.

   d) Include a detailed risk assessment, mitigation strategies, and a project execution timeline.

2. **System Design and Solution Architecture:**
   a) Propose a robust DDoS mitigation solution capable of detecting and mitigating all types of DDoS attacks, including volumetric, protocol, and application layer attacks.
   b) Ensure the solution supports both on-premises and cloud-based deployment models, offering hybrid protection if required.
   c) Provide an architecture that includes automatic attack detection, traffic analysis, and threat intelligence integration.
   d) Include redundancy and high availability features to maintain service continuity during attack scenarios.
   e) Design the solution with scalability in mind to handle future increases in traffic and potential attack sizes.

3. **Supply, Installation, and Commissioning:**
   a) Deliver all necessary hardware, software, and accessories required for a complete DDoS protection setup, including network appliances, management software, and cabling.
   b) Perform installation, configuration, and commissioning of the DDoS solution, ensuring seamless integration with the existing network infrastructure.
   c) Configure network traffic redirection, filtering, and scrubbing mechanisms to ensure legitimate traffic is not impacted during mitigation.
   d) Implement traffic monitoring and alerting features for real-time threat visibility.

4. **Configuration and Integration:**
   a) Configure attack detection thresholds, traffic baselining, and automated response mechanisms.

b) Integrate the DDoS solution with existing security tools, including firewalls, intrusion detection/prevention systems (IDS/IPS), and security information and event management (SIEM) systems.

c) Establish automated traffic analysis and anomaly detection to proactively identify potential threats.

d) Implement multi-vector attack defense capabilities, including rate limiting, connection tracking, and behavioral analysis.

5. **Testing and Validation:**

a) Conduct comprehensive testing, including simulation of DDoS attack scenarios to validate detection and mitigation capabilities.

b) Perform load testing to assess the system’s ability to handle peak traffic loads and maintain performance.

c) Provide detailed test reports, including metrics on response times, false positive rates, and effectiveness of mitigation strategies.

d) Facilitate acceptance testing with the client's technical team to ensure compliance with performance and security requirements.

6. **Warranty and Support:**

a) Ensure a comprehensive warranty for all hardware and software components of the DDoS solution.

b) Provide 24x7 support with clear Service Level Agreements (SLAs) for incident response and resolution times.

c) Offer local service support to minimize response times and facilitate on-site assistance if needed.

d) Include software updates, threat intelligence feed subscriptions, and maintenance services as part of the warranty.

7. **Post-Implementation Support:**
   a) Provide ongoing support services, including monitoring, threat intelligence updates, and regular system health checks.
   b) Establish automated alerting and reporting mechanisms to keep the client informed of potential threats and system performance.
   c) Offer proactive maintenance, including firmware updates, patch management, and performance tuning.

The bidder must take full responsibility for delivering a robust, scalable, and reliable DDoS mitigation solution that ensures business continuity, minimizes service disruptions, and enhances the client's overall security posture.

Bidders' Responsibilities for Security Information and Event Management (SIEM) / Log Server Augmentation :

1. **System Design and Solution Architecture:**
   a) Propose a robust SIEM solution that provides secure and seamless access management across the enterprise network, ensuring compliance with security protocols and data governance policies.
   b) Design an architecture that includes identity and access management (IAM), single sign-on (SSO), multi-factor authentication (MFA), and role-based access controls (RBAC).
   c) Ensure support for integration with existing directory services like Active Directory, LDAP, and cloud-based identity providers.
   d) Propose a solution that includes advanced threat detection, behavioral analytics, and zero-trust security principles.
   e) Incorporate high availability and redundancy features to ensure uninterrupted network access and authentication services.

2. **Supply, Installation, and Commissioning:**

a) Provide all necessary hardware, software, and accessories required for a fully functional SIEM Network deployment, including servers, software licenses, and security appliances.

b) Perform end-to-end installation, configuration, and commissioning of the SIEM Network components.

c) Integrate the SEAM solution with the organization's existing IT infrastructure, including network devices, servers, applications, and cloud services.

d) Configure network policies, security rules, and authentication mechanisms to ensure a secure and efficient access management framework.

3. **Configuration and Integration:**

   a) Configure authentication and authorization policies, user provisioning workflows, and access control lists (ACLs).

   b) Integrate the SIEM solution with Security Information and Event Management (SIEM) systems for real-time monitoring and incident management.

   c) Establish automated processes for user lifecycle management, including onboarding, offboarding, and role changes.

   d) Implement API-based integration with third-party applications and services to enhance security and usability.

4. **Testing and Validation:**

   a) Conduct rigorous testing of all SIEM Network components to validate security, performance, and compatibility with the existing network environment.

   b) Perform security assessments, including vulnerability scanning and penetration testing, to ensure the integrity of the access management framework.

c) Validate the effectiveness of access control policies, authentication methods, and network segmentation.

d) Provide test reports demonstrating compliance with performance metrics and security benchmarks.

5. **Warranty and Support:**
   a) Provide a comprehensive warranty for all hardware and software components of the SIEM solution.

   b) Ensure 24x7 support with well-defined Service Level Agreements (SLAs) for incident response and resolution.

   c) Offer on-site and remote support to address any technical issues and maintain system availability.

   d) Include software updates, patches, and maintenance services as part of the support package.

6. **Post-Implementation Support:**
   a) Provide ongoing support, including system monitoring, regular health checks, and performance optimization.

   b) Implement a proactive maintenance approach with automated alerts, incident management, and preventive measures.

   c) Ensure the SIEM Network solution remains updated with the latest security patches and compliance requirements.

The bidder must assume full responsibility for delivering a scalable, secure, and reliable SIEM Network solution that enhances access management, strengthens security, and supports the client's organizational objectives efficiently

Bidders' Responsibilities for Network Time Protocol (NTP) Server:

- **Installation & Configuration:**
  Deploy and configure a secure NTP server.

Integrate with internal network devices, servers, and security appliances.

- **Time Synchronization:**
  Ensure accurate timekeeping across all connected systems.
  Synchronize with reliable external time sources.

- **Security & Hardening:**
  Implement authentication and access control for time synchronization requests.
  Prevent unauthorized time changes and spoofing attacks.

Bidders' Responsibilities for Database Management System:

- Bidder should supply and install latest version of Oracle Database Enterprise Edition perpetual licenses with ATS for three years

- The Oracle Licenses will be in name of The Joint Director, FMISC, Patna, Bihar.

- Bidder shall migrate the existing data from current databases (if any) to the new setup and ensure data consistency.

- Bidder to coordinate for any troubleshooting and ticketing as and when required during the service period.

- Bidder to ensure proper backup methodology of the installed database.

- Bidder to implement the Database security component **(Audit Vault and Database Firewall)** as per the scope of work and customer's security policy.

Bidder to ensure proper database management and overall database health management during the service period.

Deliverables

1. **Fully deployed and configured solutions** for Storage, Software, WAF, DDoS, SIEM, and NTP Server..etc.
2. **Technical documentation** covering installation, configurations, and policies.

3. **User training and knowledge transfer** for IT/security teams.
4. **Testing and validation reports** ensuring security effectiveness.
5. **Post-deployment support** and troubleshooting assistance.
6. Maintain local service support in Patna to facilitate quick response times and minimize downtime.

Vendor Responsibilities

- Provide qualified professionals for deployment and configuration.
- Ensure minimal downtime and disruption to existing services.
- Follow security best practices and compliance guidelines.
- Perform system validation and performance testing.
- Offer post-deployment support for a defined period