CORRIGENDUM/ADDENDUM

The following are added in NIT under SOW (Scope of Work) as Annexure - A and under SLA (Service Level Agreement) as Annexure – B, which shall also be part of NIT:-

ANNEXURE-A

ADDENDUM TO SCOPE OF WORK

Agency shall ensure following:-

1. Security Audits and Compliance

- **Vulnerability Disclosure Policy:** Establish a clear policy for handling discovered vulnerabilities, including a defined timeline for patching critical and high-severity findings (e.g., critical fixes within 24 hours).
- **Vulnerability and Penetration Testing (VAPT):** Clearly define the scope of the penetration testing to include both authenticated (Admin/CMS) and unauthenticated interfaces, as well as the underlying infrastructure. Conduct VAPT of the website before go live.

2. Infrastructure and Platform Security:

- **Micro-segmentation:** Implement network security group policies on the cloud environment to restrict communication between the web, application, and database tiers to *only* what is necessary (principle of least privilege for network traffic).
- **Intrusion Detection/Prevention System (IDS/IPS):** The cloud environment or the Web Application Firewall (WAF) should be configured with IDS/IPS capabilities to monitor and block known malicious traffic patterns.
- DDoS mitigation solutions must be implemented like CDN, DNS protection and clean pipe services.
- **Secure Configuration Benchmarks:** Ensure all server components (OS, Web Server, Database) are hardened according to industry-standard benchmarks like CIS V2.0, STIG, NIST, SANS etc.

3. Application and Data Security:

- **End-to-End Encryption for Backup:** Explicitly confirm that data in transit and data at rest both are encrypted.
- **Input Sanitization:** Beyond CAPTCHA, implement rigorous **input validation and sanitization** to prevent common web attacks such as Cross-Site Scripting (XSS) and SQL Injection across all user inputs, including the CMS/Admin portal.

- **HTTP Security Headers:** Ensure the server is configured to deliver robust HTTP security headers (e.g., Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options) to mitigate client-side attacks.

4. Monitoring and Incident Response:

- All types of logging must be enabled and logs must be stored for minimum of 06 months as per Govt. guidelines.
- **Security Information and Event Management (SIEM):** Implement a SIEM solution (or a managed equivalent on the cloud platform) to aggregate and analyze security logs from the servers and application in real-time.
- **Defined Incident Response Plan:** The contractor must provide a documented and tested **Incident Response (IR) Plan** detailing:
  - Detection and Analysis (including the automatic alerts mentioned)
  - Containment, Eradication, and Recovery
  - Post-Incident Activity and Reporting to AAICLAS
- **Web Application Firewall (WAF) Logs:** WAF should be implemented and logs shall actively monitored and retained as part of the logging process.

5. Identity and Access Management (IAM):

- While two factors is the minimum technical requirement, modern security best practices recommend an Adaptive or Risk-Based approach, which may require more than two factors depending on the user profile.

Context / User Type	Recommendation	Factors Required	Example Combination
Baseline / Standard	The required minimum for all users.	2 Factors	Password (Know) + Authenticator App, SMS (Have)

- **Principle of Least Privilege:** Implement Role-Based Access Control (RBAC) across the CMS/Admin portal. Users should only have the minimum permissions necessary to perform their required tasks.

- **Regular Access Review:** Implement a process for quarterly or semi-annual review of all administrator and sub-admin accounts to ensure access remains appropriate.

ANNEXURE - B

ADDENDUM TO SLA

Agency shall comply the following:-

(a) **Secure Development Practices:**

- The Agency shall provide summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify the supplied hardware, software, and firmware.
- The agency should provide software Bill of material (SBOM) of software / applications installed in the system. It will help to track vulnerabilities and carry out patch management for the applications and third party libraries integrated with the applications supplied.
- The agency shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware).
- The agency shall identify the countries where the development, manufacturing, maintenance, and service for the product are provided.
- The agency shall provide a Quality Assurance program and validate that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities.
- The agency shall provide a contingency plan for sustaining the security of the procured product in the event the Supplier leaves the business.

(b) **Deployment & configuration of ICT infrastructure:** Global best practices like CIS V2.0, STIG, NIST, SANS etc may be considered for hardening and configuration of ICT devices.

- **Software / Firmware & Services:**
  - The agency shall provide documentation of software/ firmware that supports the procured hardware devices. The listing shall also include all ports and authorized services required for normal operation, emergency operation, or troubleshooting.
  - Ensure all services and/or ports in the procured product not required for normal operation, emergency operation, or troubleshooting are removed and/or disabled and documented.

- Ensure documentation of procured product's security features and security-focused instructions on product's maintenance, support, and reconfiguration of default settings.

- **Access Control:**
  - Configure each component of the procured product to operate using least privilege principle, including operating system permissions, file access, user accounts, application-to-application communication etc.
  - Modify user accounts with configurable access and security permissions with one or more user role(s) defined by CII entity. Configure these options as per the requirement of CII entity to protect against unauthorised privilege escalation.
  - The agency shall provide capabilities to prevent unauthorized changes to the Basic Input/output System (BIOS) and other firmware. If it is not technically feasible to protect the BIOS to reduce the risk of unauthorized changes, the agency shall document this case and provide mitigation recommendations.
  - Implement Multi-factor authentication (MFA) for all administrative access, including physical and remote access. Remote access shall be disabled. If required for operational purpose, it shall be provided with adequate security measures e.g. through VPN with MFA and whitelisted IP only.
  - The agency shall provide capability to identify the unauthorized installation of logging devices (e.g., key loggers, cameras, and microphones). Ensure verification and documentation for the procured product, attesting that unauthorized logging devices are not installed.
  - The agency shall deliver a product that enables CII entity to configure its components to limit access to and from specific locations (e.g., security zones, business networks, and demilitarized zones [DMZs]) on the network to which the components are attached, where appropriate, and provide CII entity with the documentation of the delivered product's configuration.

- **User Account Management**:
  - Change default account settings to CII entity specific settings (e.g. length, complexity, configuration etc.) or support the entity in these changes.

- Document all accounts that need to be active for proper operation of the procured product. Remove or disable any account that are not needed for normal or maintenance operation of the procured product.
- Accounts for emergency operations to be placed in a highly secure configuration as per CII entity requirement and documentation on their configuration to be provided to the entity.

- **Session Management**:
  - Weak or insecure system session operating practices can result in vulnerabilities in systems. Examples of insecure practices include permitting use of clear text passwords, passwords lacking requisite complexity, multiple concurrent session logins, remembered account information between logins, and auto filling fields during logins.
  - agency shall configure an appropriate level of protection for above-mentioned practices (e.g., encryption and digital signing) for the application and control system sessions, in accordance with internationally acceptable standards, commensurate with the technology platform, communications characteristics, and response time constraints.
- **Authentication/ Password Policy and Management**:
  - Deliver a product that uses secure Industry standard (internationally acceptable) authentication protocols (e.g. OAuth 2.0, OpenID Connect (OIDC), SAML, and FIDO2/WebAuthn, LDAP etc.).
  - Ensure that the procured products support implementation of multifactor authentication for remote access / control during support and maintenance activity, if needed.
  - Provide a configurable account password management system that allows for, but is not limited to, the following:
    - Changes to passwords (including default passwords)
    - Selection of password length
    - Frequency of change
    - Setting of required password complexity
    - Number of login attempts prior to lockout
    - Inactive session logout
    - Screen lock by application
    - Comparison to a library of forbidden strings
    - Derivative use of the user name
    - Denial of repeated or recycled use of the same password
    - Protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts.

- **Logging and Auditing**: following needs to be ensured by agency.
    - The agency shall provide logging capabilities. Logging capabilities provided by the Supplier shall be configurable by the entity and support the entity's security auditing requirements as per NCIIPC, CERT-In and Govt. guidelines. The procured product shall at least cover the following events:
        - Information requests and server responses
        - Successful and unsuccessful authentication and access attempts
        - Account changes
        - Privileged use
        - Application start-up and shutdown
        - Application failures
        - Major application configuration changes
    - The agency shall provide standard time synchronization in the procured product to synchronize to an authoritative time source. As per Govt. guidelines, NPL / NIC time source is recommended.
    - The agency shall ensure that the procured product provides time stamps to audit trails and log files.
    - The agency shall provide confidentiality and integrity security protection of log files.
    - The agency shall ensure that the procured product implements secure mechanism for collecting and storing (e.g., transfer or log forwarding) security log files.
    - The agency shall implement log and Security Information and Event Management (SIEM) integration (e.g., syslog).
    - The agency shall ensure that logs are generated in internationally acceptable formats for procured hardware. This list shall identify which of those logs are enabled by default.

(c) **Vulnerability and Patch Management**: To remediate discovered weaknesses and vulnerabilities, responsible system and product Supplier must regularly release updates, patches, service packages, or other fixes to their products—including third- party hardware, software, and firmware.

- agency to report the vulnerabilities throughout the life cycle of the product and need to disclose the vulnerabilities and breaches even beyond the contract period.
- agency to inform entity about compromised systems, new vulnerabilities noticed and provide documentation, which includes description of vulnerability/ breach/ cyber threat, its potential security impact, its root cause, and recommended corrective actions involving procured product.

- In cases of OEM subcontracts, the vicarious liability will remain with the OEM to ensure adequate accountability and prevention of cyber threats.
- agency shall maintain a patch management program and update process (including any third party hardware, software and firmware). This should include
  - The process for validating the integrity of the patch and upgrades prior to performing updates on production system.
  - Address zero-day vulnerabilities
  - Ensure that updates to remediate vulnerabilities or weaknesses are provided within two weeks of the vulnerability becoming public, or based on a support agreement by entity.
  - Provide all updates to remediate critical vulnerabilities within 24hrs of the critical vulnerability becoming public or within 48 hrs of notification by entity. If the Supplier cannot make updates available within this period of time, the Supplier shall provide mitigations and/or workarounds accordingly.
- **Vulnerability Reporting**: When vulnerabilities in hardware, software, or firmware configurations are discovered by entity, a process to be in place to allow users to report them. Vulnerability mitigation process also to be in place for tracking of progress of workarounds, patches, fixes. The supplier shall develop an initial action plan with 24 hours and remediate vulnerability as per timelines mentioned above.

(d) **Incident Response:** In the event of a security incident related to the deployed infrastructure, the Vendor shall adhere to the following:

- Well-defined and tested incident management processes to be in place that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise shall also in place.
- When an incident occurs the supplier team present at entity on 24/7 basis will report it to entity, NCIIPC and CERT-In as per Govt. guidelines and take immediate steps to understand its root causes and ensure appropriate remediating action is taken. Supplier shall ensure SOP regarding incident response is available.
- Clearly define roles and responsibilities in case of cybersecurity incidents.
- **Hardware Replacement / Resolution Time**: Shall be as per business requirement of the entity. This ensures that critical hardware failures are addressed swiftly to minimize downtime.

- **Reporting**: Detailed post-incident reports will be provided within 48 hours of resolution, including a comprehensive root cause analysis, a timeline of events, impact assessment, and specific corrective and preventative actions taken or recommended.
- **Telephonic Support**: Technical experts shall be available apart from team present on site for providing telephonic support with call logging mechanism on a 24×7×365 for support in incident analysis and mitigation. This ensures continuous access to expert assistance for critical security issues.

(e) **Deployment and Operation of Security Information and Event Management (SIEM) solution**: Following shall be done by the supplier:

- **Discovery and Assessment:** Understanding existing IT / OT infrastructure, security needs, compliance requirements and data sources for log collection.
- **Architecture Design and Planning:** Development of the SIEM architecture, capacity planning, and a detailed deployment roadmap.
- **Installation and Configuration:** Deployment of the SIEM solution (on-premises), initial system configuration, and integration with specified log sources (e.g., firewalls, servers, endpoints etc.). Ensure all the log sources are integrated into the SIEM and it is correctly integrated, configured, and tuned. Threat models in SIEM should be developed based on MITRE ATT&CK framework as relevant to the infrastructure. Logs should be retained as per Govt. of India guidelines.
- **Monitoring and Alert:** Creation and customization of correlation rules, alerts, and dashboards based on identified use cases to detect known threats.
    - Ensure adequate number of use cases are configured (e.g., brute-force detection, anomalous login, unauthorised software installation, data exfiltration attempts etc.) successfully and operationalized.
    - SIEM should generate alerts for configured use cases and security team will respond to these immediately as soon as alert is generated.
    - SIEM's configuration, rules, and logs shall be reviewed periodically to ensure it is functioning correctly and effectively.
- **Testing and Tuning:** Thorough testing of the SIEM's functionality, alert accuracy, and performance, followed by fine-tuning to reduce false positives and optimize detection.
- **Documentation:** Comprehensive documentation, including architecture diagrams, configuration details, and operational procedures.

- **Training:** Training for the entity's security team on how to use, manage, and maintain the SIEM solution.
- **Operation and Maintenance:** Supplier shall ensure following.
  - Providing qualified personnel for deployment.
  - Adhering to agreed-upon timelines and quality standards.
  - Since SIEM handles sensitive security data, the supplier must ensure data privacy, protection, and integrity.
  - Principle of least privilege and MFA shall be implemented for access control in SIEM.

(f) **Training & Capacity Building**: Supplier shall provide training and knowledge transfer to entity officers for sustainable and effective management of the new security infrastructure as per requirement of the entity.

(g) **Supplier/Agency Personnel Management:**

- Ensure appropriate security checks are performed for their personnel with access to the procured product.
- Ensure their personnel have awareness of cyber security risk, and capability as appropriate to their role and can provide records of their training.
- Agree and adhere to the entity’s information security policy, latest cyber security guidelines of statutory security agencies (e.g. NCIIPC, CERT-In etc.).

(h) **Reporting & Auditing:** The Vendor shall provide regular reports and support auditing requirements:

- **Monthly Performance Report**: A comprehensive report detailing service availability, performance metrics, incident summaries, and patch management activities, to be submitted by the 5th business day of the following month.
- **Security Audit Support**: Vendor shall provide necessary logs, configurations, and documentation to support entity’s internal and external security audits within 48 hours of request.
- **Compliance Reporting**: Assist in generating reports required for compliance with relevant regulations.

(i) **Additional Considerations:**

- Notify the entity of potential security incidents or relevant risk, such as breaches affecting agreed data connections, personnel issues or compromise of information (physical or electronic) in supplier organisation and identified vulnerabilities that may affect the entity's systems whether considered a cyber-security risk by the vendor or not.
- The vendor to have the responsibility to provide an inventory of all assets included in the delivery of procured products. The inventory contains appropriate information for asset management and identifies critical or operationally important assets where possible. The contractor to identify and document system interfaces and dependencies for the procured product. Ensure any changes to the System are updated in inventory or a record is provided to the entity.
- **Non-Disclosure Agreement**: Ensure that the any type of Information related to procured product not to be discussed or disclosed to any third party without the express written consent of entity.

(j) **Review and Escalation:**

- **SLA Review**: It shall be reviewed half yearly / annually by entity and Supplier to ensure its continued relevance and effectiveness. The reviews will assess performance against SLA targets, discuss any challenges, and make necessary adjustments.
- **Escalation Matrix**: The Vendor will provide an escalation matrix, detailing contact information and escalation paths for different levels of issues and concerns. This ensures that critical issues are promptly escalated to appropriate management levels for swift resolution.