DR CBS CYBER SECURITY SERVICES LLP

LLP Id No. AAK-4058

CERT-In Empanelled Information Security Auditing Organization (2020-2027)
Certified ISO 9001:2015 (No. IAS0508Q2286)
Certified ISO/IEC 27001:2022 (No. IN/26314557/3260)

Tuesday, 11th August 2026

Safe to Host Certificate

Certificate Number	: 283/26-27/2659
Organization Name	: Consulate General of India, Jaffna
Address	: Consulate General of India, Jaffna
Application Name	: Official Website of Consulate General of India, Jaffna
Production URL	: https://www.cgijaffna.gov.in/
Audited URL	: https://www.cgijaffna.gov.in/
Audit Period	: 29th July 2026 to 10th August 2026
Compliance Verification Date	: 10th August 2026
Hash Value	:c4b0291c59256b9b0fc55584cb04a4b42529ee09be084877e8b7f2267a8b7b9d b90433f0f032ed3fc26fc8a8d16290ca
Path	: C:\xampp\htdocs\cgijaffna.gov.in
Certificate Validity	: 1 year (Valid till 09th August 2027)

The above web application has undergone Vulnerability Assessment & Penetration Testing, by our organization through provided production URL as per guidelines, advisories, white papers and vulnerability notes, directions issued by CERT-In. We also tested the web application against various Web Security Standards like Open Web Application Security Project (OWASP), including the OWASP Web Security Testing Guide (WSTG) and OWASP Application Security Verification Standard (ASVS), OWASP Testing Guide (OTG), Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM3), The Information Technology Act 2000, The Guidelines for Secure Application Design, Development, Implementation & Operations issued by CERT-In, Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE).
The audit was conducted on the given production environment as per auditee requirement.

Conclusion: Based on the audit outcomes, it is certified that the above application is free from any known vulnerabilities as of the audit date. However, the auditee has given a remark for Content Security Policy Bypass. The application depends on third-party services such as Google Translate and Google Analytics, which are required for translation and analytics functionality. Therefore, the CSP cannot be further restricted without affecting the intended functionality of the application.

The assessment represents the security posture of the application at the time of testing only. Any changes to application code, configuration, infrastructure, deployment architecture or security controls after the assessment period may invalidate this certificate. The certificate is valid only for the explicitly defined scope.

Other Recommendations:

1. Web Server Security and the OS hardening need to be in place for the production server.
2. Web Application should comply with Guidelines for Secure Application Design, Development, Implementation & Operations issued by CERT-In.
3. Organization must comply with the Directions issued by CERT-In (Notification No. 20(3)/2022-CERT-In) dated 28 April 2022 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
4. Auditee should also follow the Technical Guidelines on SBOM | QBOM & CBOM | AIBOM | HBOM | Version 2.0 issued by CERT-In dated 09.07.2025.

Prepared & Verified By
DRCBS-26-078 & DRCBS-17-005

Dr. CB SHARMA IPS (R)
Certified Lead Auditor ISMS (ISO/IEC 27001)
Founder & CEO
Dr. C. B. Sharma IPS R.
Founder & CEO

DR CBS CYBER SECURITY SERVICES LLP JAIPUR