NeSL®
National E-Governance Services Ltd.

Communiqué to ALL Users (#215)

Circular No.: NeSL/FC/2025/0215 Date: 23rd September 2025

Discontinuation of Obsolete Cipher Suites in Transport Layer Security (TLS)

Kind Attention: All Clients/Service providers

Please be advised that NeSL is enhancing the security of its TLS connections by discontinuing support for several outdated and less secure cipher suites for Web/API applications (IU Data, DDE, e-BG).

Effective October 15, 2025, the following cipher suites will no longer be supported in the production environment:

- Cipher Block Chaining (CBC) cipher suites.
- Ciphers that do not support Perfect Forward Secrecy (PFS) in RSA Key Exchange.
- Obsolete CAMELLIA ciphers.

To ensure uninterrupted service and maintain secure communication with NeSL platforms, all clients and service providers currently using these configurations are required to migrate with secure alternatives, such as Galois/Counter Mode (GCM).

UAT/Staging Environment Update

Please note that the discontinuation of these ciphers will be implemented earlier in the UAT/Staging environment, effective October 1, 2025. We encourage all affected parties to complete their testing and transition processes before this date.

Your feedback is important to us, and we welcome any suggestions to improve our services on a continuous basis. Please write to us at suggestions@nesl.co.in with your suggestions, if any.

Sd/
Team NeSL

CLICK HERE- For all previous communiques