Remove the Camellia-based cipher suites from the required list and make server support optional in B.13.

Servers shall support all of the following cipher suites for TLS 1.2. Clients shall support at least one of the cipher suites defined below.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

The above cipher suites are preferred for TLS 1.2. Clients that support TLS 1.2 shall support at least one of the cipher suites listed above or below. Servers may support the following cipher suites as a fallback for TLS.
1.2 but are not required to do so. The following list of cipher suites may be used, but support is not mandatory for both servers and clients.

- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_128_CCM_8

When using TLS 1.2, cipher suites other than those listed in either the required or optional lists above are not permitted.