DICOM Correction Proposal

STATUS	Letter Ballot
Date of Last Update	2024/01/14
Person Assigned	R Horn
Submitter Name	Lawrence Tarbox (for WG-14), LRTarbox@uams.edu
Submission Date	2023/04/04

Correction Number CP-2311
Log Summary: Make Camellia support optional
Name of Standard PS3.15
Rationale for Correction: As pointed out by early implementers (notably Marco Eichelberg), open source toolkits have sporadic support for the Camellia cipher suites in conjunction with the GCM block cipher mode. WG-14, in consultation with our Japanese participants decided to make Camellia optional rather than required.
Correction Wording:

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 may support any of the following protocols for TLS 1.2.**

- 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

Clients and Servers may support any of the following cipher suites for TLS 1.2.

- **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**

The above **server-required and optional** cipher suites are preferred for TLS 1.2. Clients that support TLS 1.2 shall support at least one of the cipher suites ~~**listed**~~ **in the server required list or the optional lists** above or below. Servers may support the following cipher suites as a fallback for TLS 1.2 but are not required to do so.

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_256_GCM_CCM_8
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_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 list above are not permitted.