CSfC Selections for Enterprise Session Controllers (ESC)
(Also known as SIP Server)

Enterprise Session Controller (aka SIP Server) product-lines used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Network Device collaborative Protection Profile (NDcPP) and NDcPP Extended Package Enterprise Session Controller (ESC EP). This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for NDcPP evaluations:

FCS_TLSS_EXT.2.1 The TSF shall implement [selection: ***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support at least one of the following ciphersuites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

CSfC selections for ESC EP v1.0 evaluations:

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*selection:* ***allow the administrator to choose whether to accept the certificate in these cases****, or* ***not accept the certificate***].

Last Updated: August 21, 2018