CSfC Selections for TLS Protected Servers

TLS Protected Server products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's collaborative Protection Profile for Network Devices (ND cPP) and this validated compliance shall include the selectable requirements contained in this document.

CSfC selections for ND cPP evaluations:

FCS_TLSS_EXT.2.1 The TSF shall implement [TLS 1.2 (RFC 5246)] supporting one or more 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

Not listed in ND cPP, but also acceptable

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288