CSfC Selections for TLS Software Applications

TLS software application products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Protection Profile for Application Software (ASPP), and this validated compliance shall include the selectable requirements contained in this document.

CSfC selections for ASPP evaluations:

FCS_RBG_EXT.2.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [selection: a software-based noise source, no other noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_TLSC_EXT.1.1 The application shall [selection*: invoke platform-provided TLS 1.2, implement TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

FCS_TLSC_EXT.1.5 The application shall present the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*secp384r1*].