QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Transport Layer Security (TLS) provides mechanisms to protect sensitive data during electronic dissemination across networks. This special publication provides guidance to the selection and configuration of TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms. The revised guidelines include the required support of TLS version 1.1, recommended support of TLS version 1.2, guidance on certificate profiles and validation methods, TLS extension recommendations, and support for a greater variety of FIPS-based cipher suites.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- NISTSP800-52r1.pdf