This **DRAFT SPECIAL PUBLICATION (SP)** (Draft SP 800-52, Revision 1) document has been approved as **FINAL**, and has been superseded by the following publication:

Publication Number:	**Special Publication 800-52 Revision 1**
Title:	**Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations**
Publication Date:	**April 2014**

- Final Publication:
  NIST Publication Portal
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
  DOI URL (note: The DOI actually redirects to the URL above):
  http://dx.doi.org/10.6028/NIST.SP.800-52r1

- *Link to NIST SP 800-52 Revision 1 can be found on the CSRC Special Publications page at:*
  http://csrc.nist.gov/publications/PubsSPs.html#800-52

- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following information was posted to CSRC announcing release of this document:

April 29, 2014:

NIST Announces the Release of Special Publication (SP) 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

NIST has released Special Publication 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. 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.