NIST SP 800-52 revision: what the planned TLS guideline changes mean for servers

26 November 2026 · 4 min read · blogs.iictp.org/nist-sp-800-52-revision-tls-guidelines-tls-1-2-explained

Short answer: the NIST SP 800-52 revision is a planned update to the United States guideline on selecting and configuring Transport Layer Security (TLS), announced by NIST on 19 November 2026. NIST says the new revision will say servers “may” rather than “should” support TLS 1.2, will generally not allow TLS 1.0 or 1.1, and is expected to add post-quantum algorithms and raise the minimum security strength to 128 bits. It matters because many procurement, audit and hardening baselines point to this document.

TL;DR The short version

- NIST announced on 19 November 2026 a planned revision of SP 800-52, the US guideline on selecting and configuring TLS.
- Servers would 'may' rather than 'should' support TLS 1.2, TLS 1.0 and 1.1 would generally not be allowed, and post-quantum algorithms and a 128-bit minimum strength are expected.
- Many procurement and hardening baselines cite this document, so inventory TLS versions and cipher suites now; the text is not final yet.

Read online, listen to it, or change the text size: https://blogs.iictp.org/nist-sp-800-52-revision-tls-guidelines-tls-1-2-explained

What is NIST SP 800-52?

NIST Special Publication 800-52 is titled Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. The current Revision 2 dates from 2019. NIST asked for comments on it in May 2026, said at the time that it expected to revise it, and reports that the comments agreed. It will now revise the publication and take further public comment only once a draft is released.

How the revision will work

Nothing changes in your obligations today. Revision 2 remains the published text until a final revision replaces it. NIST’s notice is a statement of direction: a draft will follow, with a comment period, then a final version. The Cryptographic Module Validation Program (CMVP) will separately define a timeline for justification requirements on older protocol versions.

What is new compared with Revision 2

- Servers “may” support TLS 1.2 instead of “should” support it.

- TLS 1.0 and TLS 1.1 will not generally be allowed.
- After a CMVP timeline, cryptographic modules will need a strong justification to include TLS 1.2 in general, and an exceptional justification to include TLS 1.0 or 1.1 in non-governmental servers.
- Alignment with the TLS 1.3 specification in RFC 9846.

Items NIST says the revision is expected to address

- Deprecate or disallow TLS 1.2 cipher suites that use SHA-1, DSA, static key exchange or RSA key exchange.
- Add support for post-quantum algorithms and explain TLS 1.3 algorithms negotiated in extensions.
- Raise the minimum bits of security to 128.
- Require authenticated encryption (AEAD) modes in the symmetric encryption guidance.
- Update guidance on certificate profiles, session resumption and early data, certificate revocation and supported extensions.

Limitations and open questions

- This is a plan, not requirement text. Wording can change in the draft and again after comments.
- The notice gives no publication date for the draft and no dates for the CMVP timeline.
- It does not say which post-quantum algorithms or parameter sets will be recommended. Sources were read on 26 November 2026. Products, rules and standards change, so check the linked originals before you rely on any detail.

How to prepare now

1. Inventory every TLS endpoint, including internal services, load balancers, mail servers and devices.
2. Scan for TLS 1.0 and 1.1 and schedule their removal.
3. List TLS 1.2 cipher suites that use SHA-1, static key exchange or RSA key exchange, and disable them where clients allow.
4. Enable TLS 1.3 by default and record which clients still need 1.2, with an owner and an end date.
5. Check certificate keys and signature algorithms against a 128-bit security floor, and ask suppliers for their post-quantum plans.

What it means for engineers and security teams

The practical risk is a long tail of old clients and appliances. Finding them takes longer than changing a server setting, so start with traffic logs that record the negotiated protocol version. Auditors may begin asking about the direction before a final text exists; answer with an inventory and a dated plan. Related background: post-quantum planning and zero trust.

Frequently asked questions

- **Is TLS 1.2 banned by the NIST SP 800-52 revision?** No. NIST plans to say servers “may” support it, with a future CMVP justification requirement for modules.

- **Is the new revision published?** No. As of 19 November 2026, NIST has announced its plans; a draft is still to come.
- **Will TLS 1.0 and 1.1 be allowed?** NIST says the revision will not generally allow them.
- **Does it cover post-quantum cryptography?** Support for post-quantum algorithms is listed among the items it is expected to address.

Related reading

- Post-quantum privacy and Q-day planning
- What is zero trust?
- What is threat modeling?
- TPBOK standard

> Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. NIST Computer Security Resource Center. NIST to Revise SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of TLS Implementations. 19 November 2026. csrc.nist.gov/News/2026/nist-will-revise-tls-guidelines

Published by IICTP, an independent technical credential body, on 26 November 2026. The current version of this post is at https://blogs.iictp.org/nist-sp-800-52-revision-tls-guidelines-tls-1-2-explained. More guides: blogs.iictp.org.