Why the NSA deprecated TLS 1.0 and 1.1

Outdated protocols are unsafe by design

In 2021, the National Security Agency (NSA) issued formal guidance on encryption standards. It was unambiguous:

"NSA recommends that only TLS 1.2 or TLS 1.3 be used; and that SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 not be used."[5]

This was a direct response to known vulnerabilities that attackers routinely exploit.

Here's why the NSA—and nearly every other standards body—has moved to deprecate earlier versions of TLS.

> "NSA recommends that only TLS 1.2 or 1.3 be used..."[5]
>
> NSA Guidance on Eliminating Obsolete TLS Protocols

What's wrong with TLS 1.0 and 1.1?

1. Weak cipher suites
These protocols support encryption methods that can be cracked with modern computing power—exposing email contents to interception.

2. No protection against downgrade attacks
An attacker can trick a system into accepting a weaker connection, then eavesdrop or alter the data in transit.

3. Lacking modern cryptographic protections
TLS 1.2 and 1.3 introduced stronger authentication, forward secrecy, and resistance to known exploits.

4. Out of compliance with federal and industry standards
NIST, DHS, and multiple industry frameworks no longer consider TLS 1.0 or 1.1 acceptable for protecting sensitive or regulated data—including PHI.

If federal agencies can't use them, why can your email provider?

RFC 8996, published by the Internet Engineering Task Force (IETF) in 2021, formalized what security experts had already concluded: TLS 1.0 and 1.1 are insecure by design. The RFC explicitly states that these protocols 'MUST NOT be used,' citing their lack of support for modern cipher suites and vulnerability to downgrade attacks. It also notes that TLS 1.2 is now widely deployed, eliminating the need for backward compatibility.[6] Continued use in modern systems—especially by cloud email providers—is no longer justifiable, even for legacy interoperability.

There is broad consensus that these versions should not be used under any circumstances, yet leading email providers continue to allow or silently fall back to them.

> "Using obsolete encryption provides a false sense of security because it seems as though sensitive data is protected, even though it really is not."[5]
>
> NSA Guidance on Eliminating Obsolete TLS Protocols

That's the uncomfortable truth. Google Workspace still allows transmission using TLS 1.0 and 1.1. Microsoft 365 won't use them—but instead of rejecting the message entirely, it delivers it in cleartext.

Neither approach would be permitted in federal systems. But they're happening every day in healthcare.

For organizations that handle PHI, that gap is indefensible.

TLS PROTOCOLS: SECURE VS. DEPRECATED

Acceptable	Deprecated
TLS 1.2	TLS 1.0
TLS 1.3	TLS 1.1

CLOUD PLATFORMS' TLS DOUBLE STANDARD

Google Workspace:
Allows delivery over TLS 1.0 and 1.1, despite browser-level deprecation in Chrome

Microsoft 365:
Rejects TLS 1.0/1.1 but silently delivers in cleartext with no bounce