# Update TLS Profiles – BCP195

## SUBMITTED BY Robert Horn

Presenter’s Name

## On Behalf of Working Group 14

Security

## Introduction/Scope

The IETF has updated BCP195, Best Practices for Secure Communications. These changes affect the documentation of the secure TLS profiles. The changes may require creation of new profiles, or substantive changes to the current profiles. At this time it is not clear whether these changes can be accommodated by a CP to the existing profiles, or will need to be new profiles. The changes will be proposed as a supplement with a workitem rather than waste time by starting with a CP and then determining that a supplement is appropriate.

## Limitations of Current Standard

The current profiles reflect the previous version of BCP 195.

The new version of BCP 195 is similar to the current DICOM profile for non-downgrading BCP195. The most significant change in BCP195 is removal of the option to downgrade to TLS 1.0 or 1.1.

## Description of Proposal

Working group 14 will review BCP 195 in detail to determine what requirements changes are need to the current profile wording reflect the new contents of BCP195. If new profiles are needed or profiles need to be renamed this will be done.

## Parts of Standard Affected

This work item will affect Part 15 of the DICOM standard.

## Resources & Time Line

The members of WG14 are willing to work on this item. The editor will be Larry Tarbox. The supplement page count is expected to be under 10 pages. It will be very similar to the supplement that introduced to original BCP195 profiles.

WG-14 expects that one hour of WG-06 time will be needed on three occasions to review the document. The primary issue will be clarity of the changes to profiles and proper documentation for existing profile usage by existing products, and proper documentation of changed profile usage by existing and new products.