Appendix B

Excerpt from 2014 Software Sector Meeting Summary
Software Sector Item 4, Software Maintenance & Reconfiguration

4. Software Maintenance and Reconfiguration

Source:
NTEP Software Sector

Background:
After the software is completed, what do the manufacturers use to secure their software? The following items were reviewed by the sector. *Note that agenda Item 3 also contains information on Verified and Traced updates and Software Log.*

1. Verify that the update process is documented (OK)
2. For traced updates, installed Software is authenticated and checked for integrity

   Technical means shall be employed to guarantee the authenticity of the loaded software (i.e. that it originates from the owner of the type approval certificate). This can be accomplished (e.g. by cryptographic means like signing). The signature is checked during loading. If the loaded software fails this test, the instrument shall discard it and either use the previous version of the software **or become inoperative**.

   Technical means shall be employed to guarantee the integrity of the loaded software i.e. that it has not been inadmissibly changed before loading. This can be accomplished e.g. by adding a checksum or hash code of the loaded software and verifying it during the loading procedure. If the loaded software fails this test, the instrument shall discard it and either use the previous version of the software **or become inoperative**.

   Examples are not limiting or exclusive.

3. Verify that the sealing requirements are met

   The sector asked, What sealing requirements are we talking about?

   This item is **only** addressing the **software update**, it can be either verified or traced. It is possible that there are two different security means, one for protecting software updates (software log) and one for protecting the other metrological parameters (Category I II or III method of sealing). Some examples provided by the sector members include but are not limited to:

   - Physical Seal, software log
   - Category III method of sealing can contain both means of security

4. Verify that if the upgrade process fails, the device is inoperable or the original software is restored

   The question before the group is, Can this be made mandatory?

   The manufacturer shall ensure by appropriate technical means (e.g. an audit trail) that traced updates of metrologically significant software are adequately traceable within the instrument for subsequent verification and surveillance or inspection. This requirement enables inspection authorities, which are responsible for the metrological surveillance of legally controlled instruments, to back-trace traced updates of metrologically significant software over an adequate period of time (that depends on national legislation). The statement in italics will need to be reworded to comply with US weights and measures requirements.

The sector **agreed** that the two definitions below for Verified update and Traced update were acceptable.

Verified Update
A verified update is the process of installing new software where the security is broken and the device must be re-verified. Checking for authenticity and integrity is the responsibility of the owner/user.

Traced Update
A traced update is the process of installing new software where the software is automatically checked for authenticity and integrity, and the update is recorded in a software update log or audit trail.

Note: It's possible that the Philosophy of Sealing section of NCWM Publication 14 may already address the above IF the definitions of Verified and Traced Updates (and the statement below) were to be added. The contrary argument was that it may be better to be explicit).

Use of a Category 3 audit trail is required for a Traced Update. A log entry representing a traced software update shall include the software identification of the newly installed version.

The sector recommended consolidating the definitions with the above statement thus:

Verified Update
A verified update is the process of installing new software where the security is broken and the device must be re-verified. Checking for authenticity and integrity is the responsibility of the owner/user.

Traced Update
A traced update is the process of installing new software where the software is automatically checked for authenticity and integrity, and the update is recorded in a ~~**software update log or**~~ Category 3 audit trail. The audit trail entry shall include the software identification of the newly installed version.

The sector recommended that as a first step, the following be added to *NCWM Publication 14*:

The updating of metrologically significant software, including software that checks the authenticity and integrity of the updates, shall be considered a sealable event.

Mr. Truex, NTEP Administrator, believes the above sentence is unnecessary since it's self-evident. It was agreed to ask the other sectors for feedback on the value of this addition.

Though the sector is currently recommending only the single sentence be incorporated into *NCWM Publication 14* for the time being, ultimately, the sector may wish to advance the remaining language of the original item submission.

At the 2013 meeting, the Sector had no information indicating that the other sectors had yet been approached for feedback on the value of the addition of the proposed sentence. This sector would still like the other sectors to evaluate this for inclusion in Pub. 14. We'd also like to include some description indicating that an existing audit trail should be protected during a software update, though that may already be a requirement. This does appear to be addressed in the Requirements for Metrological Audit Trails Appendices in Pub. 14.

Discussion:
In 2010 the Software Sector had considered the following:

G-S.9. Metrologically Significant Software Updates
The updating of metrologically significant software shall be considered a sealable event.
Metrologically significant software that does not conform to the approved type is not allowed for use.

Ambler Thompson suggested that the notes under G-S.8. could be amended to include software updates as a new example. Rick Harshman recommended having it as a stand-alone item, such as discussed in 2010.

This could possibly be tied back to G-S.2.

What is the sealable parameter? Is it the software version / revision? Currently all of the parameters are user-selectable, which would make this unique.

If the general code in Handbook 44 is amended to include this in some form, it applies to everything. The various sectors don't need to add to their specific sections of Handbook 44.

Darrell Flocken suggested that we try to come up with a declaration of intent and see how the sectors respond. Doug Bliss will add it to the existing presentation. Jim Truex thought it might be valuable to obtain the opinion of the S&T Committee. The Legal Metrology group should be asked, "Is a software change that updates metrologically significant software a sealable event?" Rick Harshman can obtain an answer from them.

Ambler Thompson raised a concern about the fact that at this point none of the suggested wording requires that the software identifier be unique, i.e. a change to the metrologically significant software should require a change to the software identifier. You could perhaps infer it from the requirement that it be inextricably linked to the software, but that isn't clear. Jim Truex thinks this will eventually need to be addressed, but not right now.

We reviewed the presentation that Doug Bliss had revised and tweaked it a bit. This sparked more discussion about the difficulty of convincing NIST. There seems to be a fundamental difference in how they understand changes of parameters and/or software. People don't seem to understand the difference between software and data. Adding a slide that explains the difference may help.

Last year's Weighing Sector feedback (Jim Truex will provide their wording) – they were opposed because:

1. It would change the methods of sealing (category 1, 2, and 3 audit trails) and require a change to Handbook 44.
2. It's not clear that the requirement for authenticity and integrity of the updates is limited to metrologically significant software.

The other sectors were concerned about this as well.

Legacy equipment that's still being manufactured might need to be changed to meet this obligation since their audit trails wouldn't necessarily indicate that the software has been updated.

Reference G-S.8., which is rather loose. Pub. 14 goes into much more detail about what is metrologically significant.

Darrell Flocken referred to Handbook 44, the Scales code – the event logger category 3 – the software is not a parameter. It's not so much that the software would be tracked, as the fact that it has not been in the list of sealable parameters is the concern. It sounds like this may be a procedural issue – sections of Handbook 44 may need to be altered before the sectors can add this suggestion to Pub. 14.

Conclusion:
After the discussion during the 2014 joint meeting, we revised the wording of the proposed G-S.9 to reflect some of the concerns heard from the other Sectors and interested parties:

G-S.9. Metrologically Significant Software Updates

A software update that changes the metrologically significant software shall be considered a sealable event.

The Sector still feels that explicitly requiring the metrologically significant software to be given at least the same level of protection as metrologically significant parameters is the best approach. We look forward to feedback from the S&T Committee and other Sectors on this proposed change. The Software Sector still would like to consider the issue of audit trail protection; there is some doubt as to whether the existing language is sufficient as it does not address the integrity of the audit trail during a software update, etc.