Appendix E

National Type Evaluation Program (NTEP)
Software Sector Meeting Summary

September 14, 2016
Kansas City, Missouri

5200-2   INTRODUCTION

The charge of the NTEP Software Sector is important in providing appropriate type evaluation criteria for software based weighing or measuring device based on specifications, tolerances, and technical requirements of NIST Handbook 44, *"Specifications, Tolerances, and Other Technical Requirements for Weighing and Measuring Devices*," Section 1.10. General Code, Section 2 for weighing devices, Section 3 for liquid and vapor measuring devices, and Section 5 for taximeters, grain analyzers, and multiple dimension measuring devices. The Sector's recommendations are presented to the National Type Evaluation Program (NTEP) Committee each January for approval and inclusion in NCWM Publication 14, "Technical Policy, Checklists, and Test Procedures," for national type evaluation.

The Sector is also called upon occasionally for technical expertise in addressing difficult NIST Handbook 44 issues on the agenda of the National Conference on Weights and Measures (NCWM) Specifications and Tolerances (S&T) Committee. Sector membership includes industry, NTEP laboratory representatives, technical advisors, and the NTEP Administrator. Meetings are held annually, or as needed and are open to all NCWM members and other registered parties.

Proposed revisions to the handbook(s) are shown as follows: 1) deleted language is indicated with a **bold face font using ~~strikeouts~~** (e.g., **~~this report~~**), 2) proposed new language is indicated with an **underscored bold-faced font** (e.g., **new items**), and 3) nonretroactive items are identified in *italics*. There are instances where the Sector will use red text and/or highlighted text to bring emphasis to text that requires additional attention. When used in this report, the term "weight" means "mass."

Note: It is the policy of the National Institute of Standards and Technology (NIST) to use metric units of measurement in all its publications; however, recommendations received by NCWM technical committees and regional weights and measures associations have been printed in this publication as submitted. Therefore, the report may contain references U.S. customary units.

Table A
Table of Contents

Table B
Glossary of Acronyms and Terms

Acronym	Term	Acronym	Term
BIML	International Bureau of Legal Metrology	OIML	International Organization of Legal Metrology
CC	Certificate of Conformance	OWM	Office of Weights and Measures
EPO	Examination Procedure Outline	PDC	Professional Development Committee
NCWM	National Conference on Weights and Measures	S&T	Specifications and Tolerances Committee
NIST	National Institute of Standards and Technology	SMA	Scale Manufacturers Association
NTEP	National Type Evaluation Program	WELMEC	European Cooperation in Legal Metrology

---

Details of All Items
(In order by Reference Key)

I. SOFTWARE SECTOR PRESENTATION

Technical Advisor, Mr. Doug Bliss gave a presentation from the Software Sector for the benefit of those Grain Analyzer Sector members who may not have been familiar with the agenda items and the background behind them. The presentation can be found on the NCWM.net website (**www.ncwm.net**) for those interested in reviewing the background.

II. 2016 NCWM INTERIM AND ANNUAL MEETING REPORT

Darrell Flocken reported that the two Voting items from our Sector were passed by the Conference at the July meeting.

The marking requirement for Not Built for Purpose instruments begins January 1, 2017, and will begin to be required for Built for Purpose instruments in 2022. Ms. Diane Lee relayed Ms. Cathy Brenner's comment that she is only aware of one Certificate of Conformance (CC) with the software revision on it. One of the labs (GIPSA) checked the meters, and two out of eight had the software revision on the label. Since built-for-purpose devices don't need to be able to indicate software revision until 2022, it is expected that the addition of this requirement will not pose a problem for grain analyzer manufacturers.

Also, in August, NCWM Publication 14 was revised by the Weighing Sector to include the requirement that changing software is a metrologically significant event.

III. 2016 INTERNATIONAL ACTIVITY REPORT

At the Berlin, Germany, OIML TC 5-SC 2 meeting, Dr. Thompson met with Mr. Ulrich Grottker, who revealed a proposal to revise OIML D 31. He estimates it will take three to five years for the revision to be completed. Dr. Thompson suggested that the United States would volunteer to act as Secretariat for the document review process.Carry-over Items

1. Software Identification/Markings

Source:
NTEP Software Sector

Background:
See the 2015 Software Sector Meeting Summary and the 2015 Interim Meeting S&T Agenda Item 310-1 for more background on this item.

Since its inception the Sector has wrestled with the issue of software identification and marking requirements. At the 2014 meeting, significant work was done to make the recommendation to modify GS-1. Identification more palatable to the Conference. The new approach was a less invasive modification with effective dates set in the future for compliance to new requirements.

Mr. Darrell Flocken reported on the discussions during the 2015 Interim Meeting S&T Committee sessions. The item was left as a Developing item and was not officially commented upon during the session; the Committee indicated they were waiting for the outcome from the joint meetings with the other sectors, especially this one, to move forward.

In 2015, in conjunction with the Measuring Sector, some additional fine tuning was done. The current recommendation is below.

Amend NIST Handbook 44: G-S.1. Identification as follows:

G-S.1. Identification. – All equipment, except weights and separate parts necessary to the measurement process but not having any metrological effect**,** shall be clearly and permanently marked for the purposes of identification with the following information:

(a) the name, initials, or trademark of the manufacturer or distributor;

(b) a model identifier that positively identifies the pattern or design of the device;

   (1) The model identifier shall be prefaced by the word "Model," "Type," or "Pattern." These terms may be followed by the word "Number" or an abbreviation of that word. The abbreviation for the word "Number" shall, as a minimum, begin with the letter "N" (e.g., No or No.). The abbreviation for the word "Model" shall be "Mod" or "Mod." Prefix lettering may be initial capitals, all capitals, or all lowercase.
   [Nonretroactive as of January 1, 2003]
   (Added 2000) (Amended 2001)

(c) *a nonrepetitive serial number, except for equipment with no moving or electronic component parts and* ~~not-built-for-purpose software-based software devices~~ <u>software</u>;
   [Nonretroactive as of January 1, 1968]

   (Amended 2003 and 2016)

---

(1) The serial number shall be prefaced by words, an abbreviation, or a symbol, that clearly identifies the number as the required serial number.
[Nonretroactive as of January 1, 1986]

(2) Abbreviations for the word "Serial" shall, as a minimum, begin with the letter "S," and abbreviations for the word "Number" shall, as a minimum, begin with the letter "N" (e.g., S/N, SN, Ser. No., and S. No.).
[Nonretroactive as of January 1, 2001]

(*d*) the current software version or revision identifier for not-built-for-purpose software-based devices; **manufactured as of January 1, 2004, and all software-based devices or equipment manufactured as of January 1, 2022;**
[Nonretroactive as of January 1, 2004]
(Added 2003) **(Amended 2016)**

(1) The version or revision identifier shall be:

    i. prefaced by words, an abbreviation, or a symbol, that clearly identifies the number as the required version or revision;
    [Nonretroactive as of January 1, 2007]
    (Added 2006)

    Note: If the equipment is capable of displaying the version or revision identifier but is unable to meet the formatting requirement, through the NTEP type evaluation process, other options may be deemed acceptable and described in the CC.
    (Added 2016)

    ii. continuously displayed or be accessible via the display. Instructions for displaying the version or revision identifier shall be described in the CC. As an alternative, permanently marking the version or revision identifier shall be acceptable providing the device does not always have an integral interface to communicate the version or revision identifier.
    [Nonretroactive as of January 1, 2022]
    (Added 2016)

*(2) Abbreviations for the word "Version" shall, as a minimum, begin with the letter "V" and may be followed by the word "Number." Abbreviations for the word "Revision" shall, as a minimum, begin with the letter "R" and may be followed by the word "Number." The abbreviation for the word "Number" shall, as a minimum, begin with the letter "N" (e.g., No or No.). **Prefix lettering may be initial capitals, all capitals, or all lowercase.***
[Nonretroactive as of January 1, 2007]
(Added 2006) (Amended 2016)

(*e*) *an* National Type Evaluation Program (NTEP) Certificate of Conformance (CC) *number or a corresponding CC Addendum Number for devices that have a CC.*

> *(1)* *The CC Number or a corresponding CC Addendum Number shall be prefaced by the terms "NTEP CC," "CC," or "Approval." These terms may be followed by the word "Number" or an abbreviation of that word. The abbreviation for the word "Number" shall, as a minimum, begin with the letter "N" (e.g., No or No.)*
> *[Nonretroactive as of January 1, 2003]*
>
> The required information shall be so located that it is readily observable without the necessity of the disassembly of a part requiring the use of any means separate from the device. (Amended 1985, 1991, 1999, 2000, 2001, 2003, ~~and,~~ 2006, **and 2016**)

Concerns were raised regarding situations where a particular device can be ordered with or without a display. In those situations, the manufacturers would prefer to hard-mark the software version/revision in all cases, keeping the manufacturing process simple. In this case, the wording "as an exception" is problematic since it is only allowed as an exception if the device has no capability of displaying it. Mr. Marc Buttler and Mr. Michael Keilty suggested that "exception" be replaced by "alternative," and "always" be added after "not" to address this concern, that is:

> ii. *continuously displayed or be accessible via the display. Instructions for displaying the version or revision identifier shall be described in the CC. As an ~~exception~~ alternative, permanently marking the version or revision identifier shall be acceptable providing the device does not always have an integral interface to communicate the version or revision identifier.*
> *[Nonretroactive as of January 1, 2022]*
>
> **(Added 20XX)**

The Software Sector Chair asked the members of the Measuring and Software Sector in attendance whether everyone agreed to this modification of the proposal. Since no one objected, this change was included in the recommendation to the S&T Committee (and is included in the version shown above).

We debated whether to leave the non-retroactive date as 2020. It is possible to use 20XX and explain the intent in the proposal, but it might be better to leave it as a hard target. Since time has passed since we selected 2020, we backed it off until 2022, anticipating adoption by 2017 which would provide the intended period of five years after adoption.

In last year's proposal, there was an additional sub-clause included (in the 2014 Software Sector Summary version, this clause was in G-S.1.d(1).ii, and read *directly linked to the software itself*). That line has been removed in this year's submission after further discussion during the 2015 joint meeting. Objections were raised that the clause did not actually represent a marking requirement. One suggestion was it could be removed from Identification and moved to Sealing Requirements. Ms. Tina Butcher suggested instead that it be removed and a definition be added for Software Version or Revision Identifier. Unfortunately, if a definition is used instead, the non-retroactive date would be lost. Another alternative suggested was to add a brand-new section specifically for this; however, there's a general reluctance to add new sections to NIST Handbook 44 that would have to be overcome.

It was realized that the word "permanently" in the very first paragraph of G-S.1. was sufficient language to require the software version or revision identifier to be linked to the software, so we ultimately decided to remove it from the proposed change. Since we already have a proposal on the agenda for the S&T Committee's meeting, we will be submitting an amendment to reflect the new version of this proposal, rather than using Form 15 as for a new proposal.

The new version of the proposal was sent to the regions and other sectors for comment.

The amended proposal was accepted as a Voting item at the 2016 Interim Meeting and passed at the 2016 Annual Meeting.

Discussion:
Mr. Darrell Flocken reported that the Weighing Sector asked what alternatives were permissible (per the Note to G-S.1.(d)i. above). Mr. Jim Pettinato described potential situations, such as a seven-segment display, where such a problem might exist.

Conclusion:
G-S.1.1. Location of Marking Information for Not-Built-For-Purpose, Software-Based Devices pertains to the location of marks. It currently maintains the distinction between built-for-purpose and not-built-for-purpose. The Software Sector would like to see that distinction eventually be eliminated, but the current thinking is that until the non-retroactive date of 2022 is reached, the differentiation cannot be eliminated. Due to that complication, Mr. Flocken recommended we table the issue until then. Mr. Jim Truex pointed out that we should begin working on it in 2021 so it could be considered in 2022. The Software Sector agreed to remove this item from the agenda until then. To prevent the intent to revisit this section of the general code being lost or forgotten, the item will remain on the agenda as a carry-over item, which has been tabled until 2021.

2. Identification of Certified Software

Source:
NTEP Software Sector

Background:
See the 2015 Software Sector Meeting Summary for more background on this item.

This item originated as an attempt to answer the question, "How does the field inspector know that the software running in the device is the same software evaluated and approved by the lab?"

In 2010, the Sector recommended the following change to NIST Handbook 44, General Code: G-S.1.(d) to add a new subsection (3):

> (d) *the current software version or revision identifier for* ~~*not-built-for-purpose*~~ ***software-based electronic devices;***
> *[Nonretroactive as of January 1, 2004]*
>
> (Added 2003) **(Amended 20XX)**
>
> *(1) The version or revision identifier shall be prefaced by words, an abbreviation, or a symbol, that clearly identifies the number as the required version or revision.*
> *[Nonretroactive as of January 1, 2007]*
>
> *(Added 2006)*
>
> *(2) Abbreviations for the word "Version" shall, as a minimum, begin with the letter "V" and may be followed by the word "Number." Abbreviations for the word "Revision" shall, as a minimum, begin with the letter "R" and may be followed by the word "Number." The abbreviation for the word "Number" shall, as a minimum, begin with the letter "N" (e.g., No or No.).*
> *[Nonretroactive as of January 1, 2007]*
>
> (Added 2006)
>
> **(3) The version or revision identifier shall be directly and inseparably linked to the software itself. The version or revision identifier may consist of more than one part, but at least one part shall be dedicated to the metrologically significant software.**
> ***[Nonretroactive as of January 1, 201X]***
>
> **(Added 20XX)**

Also, the Sector recommended the following information be added to NCWM Publication 14 as explanation/examples:

- Unique identifier must be displayable/printable on command or during operation, etc.

- At a minimum, a version/revision indication (1.02.09, rev 3.0 a, etc.). Could also consist of/contain checksum, etc. (crc32, for example).

This item was eventually Withdrawn. Mr. Darrell Flocken shared his recollection of why the S&T Committee objected to this wording back in 2010. Basically, it went too deep for Handbook 44 and would be better placed in NCWM Publication 14.

In addition, the Sector considered the following information to be added to NCWM Publication 14 as explanation/examples:

- The current software identifier must be displayable/printable on command during operation (or made evident by other means deemed acceptable by G-S.1.)

- At a minimum, the software identifier must include a version/revision indication (1.02.09, rev 3.0 a, etc.). It could also consist of/contain checksum, etc. (crc32, for example).

- The version or revision identifier may consist of more than one part, but at least one part shall be dedicated to the metrologically significant software.

Other questions previously brought up that have not really been satisfied to date are:

- If we allow hard-marking of the software identifier (the sector has wavered on this in the past), does the above wording then imply that some mechanical means is required (i.e. physical seal) to "inseparably link" the identifier to the software?

- If a device is capable of doing so, does it still have to be able to display, print or communicate the identifier somehow, even if it is hard-marked?

The possibility of creating a separate NCWM Publication 14 section specific to software was debated. There are pros and cons in terms of the chances of adoption with that approach. It might be beneficial to manufacturers, due to keeping the requirements in one place. This becomes a philosophical question – is the content of NIST Handbook 44 intended to be a guide to manufacturers, or is it intended as direction to field inspectors? This discussion was tabled for present.

Historically, CC's have been written in terms of "version X and higher." It is not our intention to change that "policy," but it is not documented anywhere. Perhaps that should be addressed by the Software Sector. Mr. Truex reviewed the administrative policy text, which includes the requirement to report changes to NTEP, based on whether they are metrologically significant.

California indicated their NTEP lab only puts the software version on the certificate if it is not-built-for-purpose, but it seems that the other labs do so for all software-based devices.

If pushed, the Sectors agreed that a simple defining statement to qualify the class of devices to be included would be forwarded to the interested parties:

Software Based Device – Any device with metrologically significant software.

The Software Sector decided to leave the previously withdrawn recommendation as-is, in the hopes that the other changes to G-S.1. will be adopted, and then this can be revisited. Several Measuring Sector members and all the labs indicated their support for the language as written.

Regarding field inspection and locating the required information, the lists of acceptable menu text and symbols in Appendix A are intended to assist the labs in finding the certification number. The Sector noticed no action by the Sectors had been taken when this list was circulated for comment. We would like to remind them that the Sector would like to have it reviewed. We feel that this belongs in, for example, the Weighing Device NCWM Publication 14, page DES-22, Section 3; the Belt – Conveyor Scales, page BCS-10, Section 8.7; the Measuring Devices, page LMD-21, Section 1.6; the Grain Moisture Meter, page GMM-14, Section 1 (G.S.1); and Near Infrared Grain Analyzers, page NIR-8, Section 1 (G.S.1).

Ms. Tina Butcher mentioned that the Weighing Sector has a Weighing Checklist that has a similar set of approved symbols, so the examples shown in Appendix A would be in line with their current practice.

Discussion:
Since the G-S.1. change from Item 1 was voted on and adopted in 2016, we can now move forward on this item and consider adding to NCWM Publication 14 the specifics that the Sector has been discussing related to presenting the software identification.

Mr. Flocken asked whether it's a specification or information. This would determine whether it should belong in NIST Handbook 44 or only in NCWM Publication 14. One possibility is follows:

(3) **The version or revision identifier shall be directly and inseparably linked to the software itself.**

> **Note: The version or revision identifier may consist of more than one part, but at least one part shall be dedicated to the metrologically significant software.**
> *[Nonretroactive as of January 1, 201X]*
> **(Added 20XX)**

Concern was expressed that this could cause confusion with field inspectors. Software separation isn't something that's intended to be useful in the field, it is intended to ease type approval and software maintenance release processing. This would lend weight to the argument of keeping it in NCWM Publication 14.

If the Sector desires to include this in NCWM Publication 14, we would need to identify all the sections where this concept would need to be added. The Software Sector doesn't have the authority to add it to the other sectors' NCWM Publication 14s. Mr. Flocken reported that a note regarding the concept of software separation has already been added to several of the various NCWM Publication 14 sections.

It was also noted that the checklist being developed for the labs currently includes (1.4.3) the requirement that the software version or revision be linked to the software itself.

Ms. Diane Lee relayed Ms. Cathy Brenner's comment that she believes most grain analyzers are currently using a checksum, which would meet the requirement for the version/revision be linked to the software. The general consensus seemed to be that this type of requirement would not be an imposition for grain analyzer manufacturers as it is already current practice to include a checksum.

As a side note, it was noted there is precedence in the load cell code in NIST Handbook 44 of including requirements pertinent only at type evaluation. Mr. Flocken does not like this practice, but it is a possibility (for the requirement to make the software revision/version linked to the software itself).

Mr. Flocken found the wording added to NCWM Publication 14 pertaining to the software version/revision marking requirement. The following wording has been added to the Weighing, Measuring, and Automatic Bulk Weighing Sections of Marking Requirements (Section 3), but not the Grain Analyzer Sector's section because they hadn't had a meeting in 2015 (or the Near Infrared).

A. Additional Marking Requirements- Not Built-for-Purpose Software-Based Devices

Identification of Certified Software:

Note: Manufacturers may choose to separate metrologically significant software from non-metrologically significant software. Separation would allow the revision of the non-metrological portion without the need for further evaluation. In addition, non-metrologically significant software may be updated on devices without breaking a seal, if so designed. Separation of software requires that all software modules (programs, subroutines, objects, etc.) that perform metrologically significant functions or that contain metrologically significant data domains form the metrologically significant software part of a measuring instrument (device

or sub-assembly). If the separation of the software is not possible or needed, then the software is metrologically significant as a whole.

The manufacturer must describe and possibly demonstrate how the version or revision identifier is directly and inseparably linked to the metrologically significant software. Where the version revision identifier is comprised of more than one part, the manufacturer shall describe which portion represents the metrological significant software and which does not.

For the Weighing Sector, there is a holding spot in the checklist for this, due to the delay for implementation until 2022 for built-for-purpose. For now, it only pertains to not-built-for-purpose.

Mr. Flocken suggested that the text be rearranged a bit:

B. Additional Marking Requirements - Not Built-for-Purpose Software-Based Devices

Identification of Certified Software:

3.1. The manufacturer must describe and possibly demonstrate how the version or revision identifier is directly and inseparably linked to the metrologically significant software. Where the version revision identifier is comprised of more than one part, the manufacturer shall describe which portion represents the metrological significant software and which does not. Yes __ No ___ N/A ___

Note: Manufacturers may choose to separate metrologically significant software from non-metrologically significant software. Separation would allow the revision of the non-metrological portion without the need for further evaluation. In addition, non-metrologically significant software may be updated on devices without breaking a seal, if so designed. Separation of software requires that all software modules (programs, subroutines, objects, etc.) that perform metrologically significant functions or that contain metrologically significant data domains form the metrologically significant software part of a measuring instrument (device or sub-assembly). If the separation of the software is not possible or needed, then the software is metrologically significant as a whole.

Conclusion:
Mr. Jim Truex thinks that putting the requirement in the checklist in NCWM Publication 14 could be linked to the marking requirement just adopted in 2016. Mr. Doug Bliss pointed out how permanence of markings is tested (via NCWM Publication 14), but it isn't specifically spelled out in NIST Handbook 44.

Given that no grain analyzers are currently implemented as not-built-for-purpose devices, the requirement wouldn't affect them until 2022. Mr. Flocken will forward the proposed text to the other sectors (the Measuring Sector meets next week, but they have a full agenda already). Ms. Diane Lee will include this as part of the summary for Grain Analyzer's meeting and ask for feedback and guidance as to where to put it. That means it won't be adopted this year for the Grain Analyzer's Section of NCWM Publication 14.

The Chair proposed we table agenda Item 2 until 2021, we continue to pursue implementing the checklist in NCWM Publication 14. Mr. Darrell Flocken suggested that the Software Sector recommend that the various Sectors adopt this for their NCWM Publication 14s. It would take a year or so, to make it through all the various sectors. A note could be added saying that a device can't be rejected if it doesn't meet this requirement in the checklist until 2022. It was agreed that we would table this item until the 2021 meeting, at which time we will propose the following (updated) wording for the 2022 NCWM Publication 14:

C. Additional Marking Requirements- Software

Identification of Certified Software:

The manufacturer must describe and possibly demonstrate how the version or revision identifier is directly and inseparably linked to the metrologically significant software. Where the version revision identifier is

comprised of more than one part, the manufacturer shall describe which portion represents the metrological significant software and which does not.

Note: Manufacturers may choose to separate metrologically significant software from non-metrologically significant software. Separation would allow the revision of the non-metrological portion without the need for further evaluation. In addition, non-metrologically significant software may be updated on devices without breaking a seal, if so designed. Separation of software requires that all software modules (programs, subroutines, objects, etc.) that perform metrologically significant functions or that contain metrologically significant data domains form the metrologically significant software part of a measuring instrument (device or sub-assembly). If the separation of the software is not possible or needed, then the software is metrologically significant as a whole.

3. Software Protection/Security

Source:
NTEP Software Sector

Background:
See the 2014 Software Sector Summary for additional background on this item.

The Sector continued to develop a proposed checklist for NCWM Publication 14. The numbering will still need to be added. This is based roughly on R 76-2 checklist and discussions beginning as early as the October 2007 NTEP Software Sector Meeting. The information requested by this checklist is currently voluntary, however, it is recommended that applicants comply with these requests or provide specific information as to why they may not be able to comply. Based on this information, the checklist may be amended to better fit with NTEP's need for information and the applicant's ability to comply.

The California, Maryland, and Ohio laboratories agreed to use this check list on one of the next devices they have in the lab and report back to the Sector on what the problems may be. In February 2011, the North Carolina laboratory was also given a copy of the check list to try.

The labs using this checklist on a trial basis indicated there was some confusion as to versions/wording. There may be more than one version in circulation. The version shown in this Summary shall be used henceforth.

During the discussion, Mr. Ed Payne (NTEP lab, Maryland) said his impression is that this is at least making some of the manufacturers think about security, which they hadn't necessarily done in the past.

It was indicated that some more or better examples may be helpful to manufacturers, and more guidance is needed. Clearer instructions could be part of the checklist, or it could be a separate document. The Sector would like additional feedback specifically regarding what portions of it are causing confusion.

Due to proprietary issues, the labs cannot simply give us direct feedback from the companies they interact with. Mr. Darrell Flocken volunteered to obtain information from the labs, aggregate it, and remove any potential proprietary information issues.

The checklist as updated during the 2014 meeting:

1. Devices with Software

1.1. Declaration of the manufacturer that the software is used in a fixed hardware and software environment. **The manufacturer should indicate whether it's solely software or includes hardware in the system. Can the software be changed after the system has been shipped without breaking a seal? AND** ☐ Yes ☐ No ☐ N/A

1.2. Cannot be modified or uploaded by any means after securing/verification. ☐ Yes ☐ No ☐ N/A
With the seal intact, can you change the software?

Note: It is acceptable to break the "seal" and load new software, audit trail is also a sufficient seal.

    1.3. The software documentation contains:

        1.3.1. Description of all functions, designating those that are considered metrologically significant. ☐ Yes ☐ No ☐ N/A

        1.3.2. Description of the securing means (evidence of an intervention). ☐ Yes ☐ No ☐ N/A

        1.3.3. Software Identification, including version/revision. **It may also include things like name, part number, CRC, etc.** ☐ Yes ☐ No ☐ N/A

        1.3.4. Description how to check the actual software identification. ☐ Yes ☐ No ☐ N/A

    1.4. The software identification is:

        1.4.1. Clearly assigned to the metrologically significant software and functions. ☐ Yes ☐ No ☐ N/A

        1.4.2. Provided by the device as documented. ☐ Yes ☐ No ☐ N/A

        1.4.3. Directly linked to the software itself. **This means that you can't easily change the software without changing the software identifier. For example, the version identifier can't be in a text file that's easily editable, or in a variable that the user can edit.** ☐ Yes ☐ No ☐ N/A

2. Programmable or Loadable Metrologically Significant Software

    2.1. The metrologically significant software is:

        2.1.1. Documented with all relevant (see below for list of documents) information. *The list of docs referred to exists in agenda item 5.* ☐ Yes ☐ No ☐ N/A

        2.1.2. Protected against accidental or intentional changes. ☐ Yes ☐ No ☐ N/A

    2.2. Evidence of intervention (such as, changes, uploads, circumvention) is available until the next verification/inspection (e.g., physical seal, Checksum, Cyclical Redundancy Check (CRC), audit trail, etc. means of security). ☐ Yes ☐ No ☐ N/A

3. Software with no access to the operating system and/or programs possible for the user. This section and section 4 are intended to be mutually exclusive. Complete this section only if you replied Yes to 1.1.

    3.3. Check whether there is a complete set of commands (e.g., function keys or commands via external interfaces) supplied and accompanied by short descriptions. ☐ Yes ☐ No ☐ N/A

    3.4. Check whether the manufacturer has submitted a written declaration of the completeness of the set of commands. ☐ Yes ☐ No ☐ N/A

4. Operating System and / or Program(s) Accessible for the User. Complete this section only if you replied No to 1.1.

    4.5. Check whether a checksum or equivalent signature is generated over the machine code of the metrologically significant software (program module(s) subject to legal control Weights and Measures jurisdiction and type-specific parameters). **This is a declaration or explanation by the manufacturer.** ☐ Yes ☐ No ☐ N/A

4.6.   Check whether the metrologically significant software will detect and act upon any unauthorized alteration of the metrologically significant software using simple software tools (e.g., text editor). **This is a declaration or explanation by the manufacturer.** ☐ Yes ☐ No ☐ N/A

5.   Software Interface(s)

5.7.   Verify the manufacturer has documented:

5.7.1.   **If software separation is employed, t**he program modules of the metrologically significant software are defined and separated. ☐ Yes ☐ No ☐ N/A

5.7.2.   **For software that can access the operating system or if the program is accessible to the user, t**he protective software interface itself is part of the metrologically significant software. ☐ Yes ☐ No ☐ N/A

5.7.3.   The functions of the metrologically significant software that can be accessed ~~via the protective software interface~~. ☐ Yes ☐ No ☐ N/A

5.7.4.   The **metrologically significant** parameters that may be exchanged ~~via the protective software interface~~ are defined. ☐ Yes ☐ No ☐ N/A

5.7.5.   The description of the functions and parameters are conclusive and complete. ☐ Yes ☐ No ☐ N/A

5.7.6.   There are software interface instructions for the third party (external) application programmer. ☐ Yes ☐ No ☐ N/A

The Sector discussed examples, such as the upgrade of application programs and how these changes would affect audit trails and version numbers. It should be clear that if the upgraded software doesn't affect anything metrologically significant, then it's irrelevant for the purposes of this checklist. On the other hand, if it does affect metrologically significant functions or parameters, it should be tracked and/or identified somehow.

Some of the labs have used the checklists, but they don't have easy access for the data to share. Not all the labs have tried to use the checklist yet. In general, when the software programmers themselves are approached with the checklist, it's useful, but that's heavily dependent on who is interacting with the labs.

Mr. Jim Pettinato reiterated the Software Sector's request that the labs continue (or begin) to ask manufacturers whether they're willing to participate in the use of this checklist (on a voluntary basis), and to send their feedback to Mr. Darrell Flocken. Mr./Ms. Teri Gulke will clean up the checklist and put it in a separate document that can be posted on the NCWM website under the Software Sector's documents.

The contents of the checklist should tie back to requirements in NCWM Publication 14. We originally crafted our checklist from the contents of D-31, so we went back to it to see if we could use it as a starting point for writing our own requirements for NCWM Publication 14.

Though they need to be reworded, of course, the most useful portion of D-31 for our current purposes are probably sections 5.1.1., 5.1.3.2.a., 5.1.3.2.d., and 5.2.6.1. which state, respectively:

5.1.1.   Software identification
Legally relevant software of a measuring instrument/electronic device/sub-assembly shall be clearly identified with the software version or another token. The identification may consist of more than one part but at least one part shall be dedicated to the legal purpose. The identification shall be inextricably linked to the software itself and shall be presented or printed on command or displayed during operation or at start up for a measuring instrument that can be turned off and on again. If a sub-assembly/an electronic device has neither display nor printer, the identification shall be sent via a communication interface in order to be displayed/printed on another sub-assembly/electronic device.

5.1.3.2.a.   The legally relevant software shall be secured against unauthorized modification, loading, or changes by swapping the memory device. In addition to mechanical sealing, technical means may be necessary to secure measuring instruments having an operating system or an option to load software.

5.1.3.2.d.   Software protection comprises appropriate sealing by mechanical, electronic and/or cryptographic means, making an unauthorized intervention impossible or evident.

5.2.6..1   Only versions of legally relevant software that conform to the approved type are allowed for use (see 5.2.5.). Applicability of the following requirements depends on the kind of instrument and is to be worked out in the relevant OIML Recommendation. It may differ also depending on the kind of instrument under consideration.

The question was asked, do these new requirements need to go into a new appendix specific to software in NCWM Publication 14? Do we need to document new requirements at all if the checklist is put into NCWM Publication 14? It could be considered that the checklist itself constitutes the new requirements. Mr. Flocken and Mr. Truex supported that interpretation.

The Sector asked that the revised checklist continue to be used by the labs.

As we meet with each Sector jointly, we can get an updated report on the trial and decide if we're ready to recommend it for NCWM Publication 14. We can also look at the language from D-31 in more detail to craft guidance in line with NCWM/NTEP philosophy.

Discussion:
The Grain Analyzer Sector's labs have not had the opportunity to try using the checklist because they didn't meet in 2015. Mr. Tom Buck from Ohio reported that they've been giving the checklist to manufacturers but haven't been getting them back. Mr. Flocken has two examples, one for built-for-purpose and one for a built-for-purpose device.

Conclusion:
Mr. Jason Jordan from GIPSA said they'd try it out. Mr. Doug Bliss and Mr. Jim Pettinato have volunteered to answer any questions that might arise as the labs attempt to use the checklist.

4.   Software Maintenance and Reconfiguration

Source:
NTEP Software Sector

Background:
See the 2015 Software Sector Meeting Summary and the 2015 Interim Meeting S&T Agenda Item 310-1 for more background on this item.

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, that is, it originates from the owner of the type approval certificate. This can be accomplished, for example, 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, that is, it has not been inadmissibly changed before loading. This can be accomplished, for example, 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 U.S. weights and measures requirements.

The Sector **agreed** 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).

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.

Dr. Ambler Thompson raised a concern about the fact, 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. Mr. Jim Truex thinks this will eventually need to be addressed, but not right now.

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.

We debated once again whether this would be redundant. It can certainly be argued that G-S.8. already covers this requirement. If G-S.9. isn't added, is there support for changing NCWM Publication 14 to add the software to the existing list of sealable parameters?

Philosophy of Sealing, Appendix A, in NCWM Publication 14 doesn't specifically say anything about software. It discusses calibration and configuration parameters. There is a list of features and parameters that are typically sealed and another list of features and parameters that are not sealed. A note below states that these lists aren't fully inclusive, but anything that's metrologically significant does need to be sealed. We've discussed before the fact that the terminology in Philosophy of Sealing repeatedly uses the term "parameter," which could cause confusion due to people interpreting this to only require sealing of parameters. G-N.8. Checklist 2.18. for LND's in the Measuring Sector's NCWM Publication 14 might be another place to add the word "software." This checklist is specific to the Measuring Sector's NCWM Pub. 14, so there wouldn't necessarily be something analogous in the other sectors' versions of Publication 14. G-S.8 refers to changing adjustable components, which could be interpreted as not having anything to do with software. At one point, the Software Sector had considered amending G-S.8., but that proved to be overly complicated.

The Software and Measuring Sector attendees, as well as the lab representatives agreed to forward the above proposed addition of G-S.9 to the S&T Committee and recommends it be considered as a Voting item in 2016. This item (See 2016 NCWM Publication 15, S&T Agenda Item 310-2.) was voted upon and adopted at the 2016 Annual Meeting.

Discussion:
The Sector will decide if any further action on this item is required.

All currently approved grain analyzers provide Category 3 audit trails, and the Grain Analyzer Sector is planning to change NIST Handbook 44 to make it a requirement that all grain analyzers must be Category 3.

The Weighing Sector (which is the only Sector that's met since the adoption of G-S.9.) has added language to NCWM Publication 14's Provision for Sealing, making software changes a sealable event.

Conclusion:
At this point, because the G-S.9. proposal has been voted upon and passed, the Software Sector can remove this item from its agenda. The only thing left to do is for the various Sectors to meet and adopt language similar to the Weighing Sector for their respective sections in NCWM Publication 14.

5. NTEP Application for Software and Software-based Devices

Source:
NTEP Software Sector

Background:
The purpose of initiating this item was to identify issues, requirements, and processes for type approving Type U device applications. It was suggested that it may be useful to the labs to devise a separate submission form for software for Type U devices. What gets submitted? What requirements and mechanisms for submission should be available? Validation in the laboratories – all required subsystems shall be included to be able to simulate the system as installed.

Mr. Roach, California Division of Measurement Standards, stated that if the software package being evaluated supports platforms/subsystems from multiple manufacturers, testing should be done using at least two platforms/subsystems. Scale laboratories and scale manufacturers indicated this is not usually done for scale evaluations.

Since the NTEP Committee passed the related item at NCWM Annual Meeting, we will continue to work on this. Mr. Truex, NTEP Administrator, indicated that we can move in this direction, but felt it was somewhat premature to develop this thoroughly now. At the point where the Sector has developed checklist requirements, then we could move to perhaps add a subsection to current NTEP applications for applicable software. Refer to D-31.6.1. It was also agreed that there seems to be no reason for limiting the scope of this item to software-only applications, and all software/software-based devices could benefit from an enhanced application process. Hence, the description of this agenda item was modified as shown in the marked-up heading.

Comments given at the meeting indicate the current practice does not require anything different for software/software based devices compared to any other type approval. It was also noted that for international applications, OIML D-31.6.5 states, "The approval applicant is responsible for the provision of all the required equipment and components." This would likely also be the policy of NTEP.

Since the checklist is still being tried out by some of the laboratories, the Sector is not quite ready to develop this fully. Some documentation that eventually might be required by applicants could include (from WELMEC doc. 7-2 Issue 4. This is the list of documents referred to in the checklist.

- A description of the software functions that are metrologically significant, meaning of the data, etc. (e.g., an architecture diagram or flowchart).

- The software identification (version, revision, etc.) and how to view it.

- An overview of the security aspects of the operating system (e.g., protection, user accounts, privileges, etc.).

Mr. Flocken and Mr. Truex reviewed existing documentation required for obtaining certification in NCWM Publication 14, Administrative Policy, and the application, to see what is already required. Administrative Policy 9.1.7 was where this was found:

- Engineering specification

- Operating descriptions that characterize the type

NTEP evaluators already have the authority to request whatever documentation they need. We can provide them with a list of documents we think would assist the evaluator in his job and give the manufacturer a good idea of what they should be capable of providing.

Darrell Flocken suggested that this list could be added to administrative policy 9.1.7 in NCWM Publication 14. Mr. Jim Truex suggested it could also be added to the application.

If we combine the two lists, it might appear as something like this:

- A description of the software functions that are metrologically significant, meaning of the data, etc. (e.g., an architecture diagram or flowchart).

- A description of the user interface, communication interface, menus, and dialogs.

- The software identification (version, revision, etc.) and how to view it.

- An overview of the system hardware (e.g., topology block diagram, type of computer(s), type of network, etc.) if not described in the operating manual.

- An overview of the security aspects of the operating system (e.g., protection, user accounts, privileges, etc.).

- The operating manual.

- Engineering specification.

- Operating descriptions that characterize the type.

A statement could be made along the lines of, "If not included in the operating manual, provide the following, as applicable."

After the last sentence in 9.1.7, this could be added:

> **As part of the type evaluation submission, the following information should be provided for software-based devices:**
> - **A description of the software functions that are metrologically significant, meaning of the data, etc. (e.g., an architecture diagram or flowchart).**
>
> - **The software identification (version, revision, etc.), how to view it, and how it is tied to the software.**
>
> - **An overview of the security aspects of the operating system (e.g., protection, user accounts, privileges, etc.).**

These documentation requirements will be considered as input for requirements that will eventually appear in NCWM Publication 14 and the application paperwork. Further work by the Sector to develop the NCWM Publication 14 requirements is needed, after more input from the labs is gathered. The Sector recommends including the above bulleted list as an introduction to the checklist as part of our recommendation to include the checklist from agenda Item 3 in NCWM Publication 14. As a description of the accuracy of the measuring algorithms, simply declaring the type and class being aimed for may be sufficient. This list should reflect the needs of the labs for an evaluation. The bulleted list and the paragraph before it should be brought to the labs for an initial review and their input.

There may be concerns with disclosure of proprietary information. Mr. Jim Truex says that the labs already protect other proprietary information. If the information provided is sufficiently high level, even theft of the data shouldn't cause too much of a concern.

Mr. Michael Keilty didn't think it appropriate for the Measuring Sector, as a body, to make a recommendation regarding this proposal since it must do with administrative policy.

Per Mr. Jim Truex, the labs already have the authorization to require this information.

While working on writing requirements for NCWM Publication 14 from the checklist we've designed, we considered altering the second bullet point in our proposal for 9.17, so that it will require a description of how the software version or revision identifier is tied to the software itself.

Discussion:
The goal of this agenda item has somewhat shifted back to the original purpose, which is how do we communicate to applicants the expectations related to software based devices?

Ms. Diane Lee suggested we review the OIML requirements for documentation. The comment was made from the floor that OIML may go further than we are currently prepared to recommend.

Mr. Jason Jordan expressed his opinion that moving forward with this item will be helpful for the labs.

Mr. Darrell Flocken and Mr. Jim Truex think this should be added to the Application section. If limited to that section, it shouldn't require approval from any of the other Sectors.

Mr. Doug Bliss suggested it might be easier to provide examples that do not meet acceptable standards.

As we began discussing the training of field inspectors, Mr. Flocken asked that we also provide further training for lab inspectors. There's an annual lab meeting typically around April and in 2017, it will be in Annapolis, Maryland.

Conclusion:
The Software Sector's recommendation will be to add the requirements to the Application section.

The Software Sector agreed to provide support for any desired training of lab personnel at the April meeting.

6.   Training of Field Inspectors

Source:
NTEP Software Sector

Background:
During discussions at the 2009 NTEP Software Sector Meeting, the Sector concluded that a new agenda item should be initiated specific to the training of field inspectors in relation to evaluating/validating software-based devices.

California has an Examination Procedure Outline (EPO) that begins to address this. Use California Handbook 112 as a pattern template for how it could read.

Items to be addressed:

- Certificate of Conformance

- Terminology (as related to software) beyond what is in NIST Handbook 44.

- Reference materials/information sources

System Verification Tests
NOTE: Item numbers 1 through 5 apply to both weighing and measuring devices. Numbers 6 and 7 are specific to weighing devices; while numbers 9 and 10 apply to measuring devices.

1. Identification. The identification (ID) tag may be on the back-room computer server and could be viewed on an identification screen on the computer monitor. The ID information may be displayed on a menu or identification screen. Though currently discouraged, some systems may be designed so the system must be shut down and reset to view the ID information. G-S.1. [1.10]
   1.1. Manufacturer.
   1.2. Model designation.

2. Provisions for sealing. G-S.8. [1.10]; S.1.11. [2.20]; S.2.2. [3.30]
   2.1. Verify sealing category of device (refer to Certificate of Approval for that system).
   2.2. Verify compliance with certificate.

3. Units of measure.
   3.1. A computer and printer interfaced to a digital indicator shall print all metrological values, intended to be the same, identically. G-S.5.2.2.(a); G-S.5.1. [1.10]
   3.2. The unit of measure, such as lb, kg, oz, gal, qt, liters, or whatever is used, must agree.

4. Operational controls, indications, and features (buttons and switches). Verify that application criteria and performance criteria are met (refer to Certificate of Approval).
   4.1. Any indication, operation, function, or condition must not be represented in a manner that interferes with the interpretation of the indicated or printed values.

5. Indications and displays.
   5.1. Attempt to print a ticket. The recorded information must be accurate or the software must not process and print a ticket with erroneous data interpreted as a measured amount.

Weighing Devices

6. Motion detection.

    6.1. For railway track, livestock, and vehicle scales apply or remove a test load of at least 15d while simultaneously operating a print button, push-button tare or push-button zero. A good way to do this is to try to print a ticket while pulling the weight truck or another vehicle onto the scale. Recorded values shall not differ from the static display by more than 3d. Perform the test at 10 %, 50 % and 100 % of the maximum applied test load. S.2.5.1.(a) [2.20]; EPO NO. 2-3, 2.4

    6.2. For all other scales, apply or remove at least 5d. Printed weight values must agree with the static weight within 1d and must exactly agree with other indications. S.2.5.4.(b) [2.20]; EPO NO. 2-3, 2.4

7. Behind zero indication.

    7.1 Apply a load in excess of the automatic zero setting mechanism (AZSM) and zero the scale. S.2.1.3. [2.20]; EPO NO. 2-3, 2.4, 2.5.2

    Example: On a vehicle scale have someone stand on the scale, then zero them off (AZSM is 3d). Remove the weight (person) and note the behind zero display (usually a minus weight value) or error condition.

    7.2. Attempt to print a ticket. With a behind zero condition, (manually or mechanically operated) a negative number must not be printed as a positive value.

8. Over capacity.

    8.1. Manually enter a gross weight if permissible or apply a test load in excess of 105 % of the scale's capacity. S.1.7. [2.20]; S.1.12., UR.3.9. [2.20]

    8.2. Attempt to print a weight ticket. A system must not print a ticket if the manually entered weight or load exceeds 105 % of the scale capacity.

Measuring Devices

9. Motion detection.

    9.1. Initiate flow through the measuring element. Attempt to print a ticket while the product is flowing through the measuring chamber. The device must not print while the indication is not stable. S.2.4.1. [3.30]

10. Over capacity.

    10.1. Attempt to print a ticket in excess of the indicated capacity. A system must not print a ticket if the device is manually or mechanically operated in excess of the indicated value.

NOTE: Be aware of error codes on the indicator which may be interrupted as measured values.

Mr. Jordan, California Division of Measurement Standards, is already doing something similar, and he may be able to assist. Mr. Roach, California Division of Measurement Standards, will talk to him to see whether they're available. In addition, Mr. Parks, California Division of Measurement Standards, is based in Sacramento and a potential resource. If the meeting is held in Sacramento next year, they may be able to attend.

Mr. Truex, NTEP Administrator, pointed out that the PDC would also be a valuable resource on this subject. Mr. Pettinato, Co-Chair, will contact them.

NIST Handbook 112- Examination Procedure Outline for Commercial Weighing and Measuring Devices.

The PDC is focused on training sessions at the moment; so, it's unsure how much time they'd have to review this currently.

It was suggested by Mr. Truex and Mr. Flocken we make it part of our report as an attachment or an appendix of the meeting minutes. Then we can send out an e-mail notifying the Software Sector members as to where to find it.

Alternatively, we could forward the document to the PDC Committee, tell them it was our starting point, and ask them for their suggestions.

The Sector would like to continue exploring means by which it can be of assistance in training of field inspectors as software and electronic systems become more and more prevalent in their daily tasks.

It was also suggested we contact Mr. Ross Anderson, a paid consultant working with the PDC committee, to ask his opinion on how the Software Sector could best proceed to assist in the training of field inspectors. The Sector chair, Mr. Jim Pettinato, will act as primary point of contact for this communication.

Discussion:
Mr. Pettinato hasn't heard anything further from the PDC or Mr. Anderson, as they continue to be quite busy.

For the Grain Analyzer Sector, Ms. Diane Lee thought it would take some time to put together some training material, as they do not currently have anything in place for software requirements.

Examples from completed checklists would be very helpful when putting together field inspector training. A lot of training videos have been recently generated. Mr. Doug Musick suggested we recommend adding this to the agenda for the PDC Committee. Certification exams could be updated more easily, on a state-by-state level. It might be better to make software a separate exam.

Ms. Diane Lee suggested we look at developing a basic course for software, incorporating specific guidelines for specific device types.

Ms. Amanda Dubin was concerned about having the field inspectors know all the different existing software, which is a monumental task. Instead, the training should focus on how to find the pertinent CC and look up information from it on the website. Ideally, down the road there could be some sort of database or software tool disseminated to field inspectors to assist in the look up of certificate numbers and the approved version number(s) for the software for a particular device, and even instructions on how to view/print the audit trail.

Mr. Jim Truex holds a meeting once a year for the lab evaluators. Mr. Darrell Flocken suggested that we also focus on training them on software. Ms. Diane Lee mentioned that NIST has been having manufacturers coming in to provide training on, for example, how to access the audit trail.

Conclusion:
As mentioned in the previous agenda item, the lab meeting is expected to occur in the April timeframe next year and the Software Sector is willing to assist in providing such training.

Dr. Thompson will be reviewing the training courses to identify areas that will need to be updated to cover the new requirements that have been approved.

Mr. Jim Pettinato will contact Mr. Ross Anderson regarding the PDC Committee, offering the Software Sector's assistance in continuing to develop training pertaining to software.

7. Retrieval of Audit Log information

Source:
Adam Oldham, Gilbarco

Background/Discussion:
The current requirements for a Category III audit trail include printing of log on demand. However, many devices are approved standalone and can be connected to systems that are approved standalone. How could Category 3 audit trail mechanisms be approved in situations where multiple devices need to work together to attain it? How can a device maintain Category 2 and 3 approvals in this scenario? What alternatives to printing can be considered as potentially valid solutions (files, laptop, flash drive, etc.)?

This was discussed during the Measuring Sector's meeting on September 15. The wording suggested was not agreed upon. Mr. Adam Oldham would like to have the Software Sector's suggestions, so he can put together a proposal for next year.

The United States has rather unique requirements for printing the Category 3 audit trail, which are quite unwieldy – both in terms of the actual printing process (and results), as well as the needed approvals (the example provided by Mr. Adam Oldham required an approval for each and every Point-of-Sale [POS] system that might be connected to their system). The most similar is from Mexico, but they require an electronic copy.

Mr. Flocken reported there has been a little movement forward – alternative methods are now allowable, to some degree, but it's dependent on what the states are going to allow. It still requires the ability to print it. The change will be in LMD Code S.2.2., not in NIST Handbook 44, General Code 1.10., G-S.2.2.

We discussed the difficulty of requiring the electronic data be printable on-site, given that some sites don't have any printers, and other sites may have printers attached to computers that are restricted in what can be used to attach to them.

In Mexico, Gilbarco relies upon laptops being present, supplied by the auditing company.

LMD NCWM Publication 14 has a section in Appendix B, Requirements for Metrological Audit Trails, on the event logger, and this information doesn't seem to be in NIST Handbook 44. In fact, it may even contradict what is in the LMD NCWM Publication 14. In practice, what's in Publication 14 tends to be more influential with evaluators.

Mr. Adam Oldham will work on the wording for a proposal for next year, which the Software Sector will review during the 2016 meeting.

Discussion:
Mr. Oldham wasn't in attendance. Mr. Pettinato reported that North Carolina had recently run into an instance where the audit trail wasn't printable on-site.

The devices monitored by the Grain Analyzer Sector are all Category 3, and they are all capable of printing the audit trail.

Mr. Musick pointed out that if you keep the metrological information in the Category 3 audit trail, and separate it from the non-metrological information, there's less of a problem with the requirement to print the audit trail; however, such separation is not a requirement. Mr. Pettinato discussed various options for limiting what's printed, such as selecting a date range.

Mr. Pettinato reported that the S&T Committee reviewed this issue recently. Gilbarco's original proposal was shot down, but a revised proposal was made. Mr. Flocken reported in July a version with the caveat that the inspector has discretion was voted upon and accepted.

Mr. Bliss suggested we table this agenda item since we do not have a concrete proposal.

Conclusion:
Without a proposal and without Gilbarco being present, the Sector can take no action at this time. The Chair will attempt to ascertain whether the intent to move this item forward still exists prior to drafting next year's agenda.

NEW ITEMS

8. Transmission of Measurement Data

Source:
Software Sector

Background:
General discussion on various issues related to distributed systems seen in use today and how metrology might be affected or vulnerable to facilitation of fraud. Specifically, authenticating sources of transactional data; guaranteeing integrity and/or retaining privacy of data; local vs. remote application functionality, SaaS.

Discussion:
The discussion began with an example: the integration of 'smart' utility meters that send data directly to the utility company and is designed to (eventually) eliminate the need to do local meter reading. In this application, there may be need to associate data securely with the particular meter in question – be able to protect private information while guaranteeing the authenticity and integrity of the data being reported upstream.

Dr. Ambler Thompson discussed his experience with "smart metering." They need some sort of positive ID, to associate the measurement with a time stamp, etc.

Mr. Bliss pointed out that the Europeans have requirements on this subject, but they're pulling back on them since there's little they can do in field verification, type evaluation, etc. to enforce them.

Mr. Pettinato asked the lab inspectors whether they regularly deal with systems that have portions remote from the originator of the data. Mr. Truex responded that they deal with that all the time. Mr. Musick says he's concerned particularly about retail-fuel dispensers.

In the Grain Analyzer Sector, their inspectors typically check for issues by tracking individual transactions all the way down the data chain.

In instances of fraud, particularly man-in-the-middle attacks, the generation of fraud tends to be by the simplest means possible. Fraudsters, at the current time, seem generally to be attacking hardware, not software, or communication interfaces. Also, it sounds like the various means of fraud are on a very case-by-case basis that would be impossible to apply across the board without major inconvenience to manufacturers.

Conclusion:
It sounds like it may be premature for the Software Sector to attempt to generate any recommendations or requirements on this subject. Mr. Pettinato suggested that, maybe at some point in time, we could consider issuing some sort of statement on the subject, but not now.

We will remove this from future agendas. Mr. Truex recommended we not put it back in unless we get more specific requests to deal with the issue from other Sectors.

9. Use of GPS Receivers and Mapping Software for Trade (e.g., fare determination)

Source:
Software Sector

Background:
Other Committees have initiated conversation on this topic primarily due to the surge in popularity of alternate taxi services (Uber and Lyft). Does the Software Sector see a need for technical guidance in this conversation? If so, what would be the scope of such guidance?

Discussion:
There were a few presentations at the Interim Meeting on this subject. The 2016 Annual Meeting archive (Denver, Colorado, 2016) has a presentation from Lyft that was given at that meeting.

Dr. Ambler Thompson has discussed this subject with the Europeans. One issue is traceability of the time stamp(s). You can also calculate velocity based upon the phase shift of the GPS signal, though it requires a high-end, survey-grade GPS receiver ($50k each). Car companies can use these devices to obtain a great deal of data.

Uber and Lyft claim that they are not billing upon GPS data, but rather a pre-negotiated contract based upon distance, time, and type of vehicle. Mr. Doug Bliss has been told the bill is based upon the starting GPS location from the driver's phone, the ending GPS location from the same phone, and a calculation of the shortest distance from Google Maps. If the driver's phone doesn't have a great GPS receiver, or if the reception is bad so it's relying upon cell towers, etc., that's a problem. We're also not sure of the accuracy of Google Map's route calculations. Also, Google Maps is a disinterested third party whose database is being used for a purpose that they didn't specifically authorize.

Mr. Musick reported that the Uber contract is based upon a unit price, though they do provide an estimate to the customer.

Mr. Truex pointed out the Taxi Meter Code in NIST Handbook 44 is obviously addressed to the old-style taxi. What's in NIST Handbook 44 isn't applicable to the new Uber and Lyft paradigm.

Mr. John Barton is leading a working group dealing with the Taxi Meter Code.

Mr. Andrei Brezoica from California, who is on the working group, reported there is a draft for new code to address this. Options exist for open-ended contracts for the customer. Google Maps is helping with the apps, pertaining to absolute distances, that Uber and Lyft are using. Mr. Pettinato asked that Mr. Brezoica send us a copy of the draft recommendation.

Ms. Lee pointed out there are several exemptions elsewhere in the code, which may be useful as examples when working on changes to the Taxi Meter Code.

Mr. Doug Musick suggested that there could be a requirement for the companies to post their unit price, per-mile, and per-time. Apparently, Uber does this, but Lyft does not.

Conclusion:
The Software Sector will offer assistance to the working group dealing with the Taxi Meter code. Dr. Thompson will talk to Mr. Barton.

10. Next Meeting

Background:
The Sector is on a yearly schedule for NTEP Software Sector Meetings. Now that we've adopted a joint meeting system, the next Sector joint meeting will coincide with one of the remaining Sector meetings.

Discussion:
The Belt-Conveyor Sector would be the next in the sequence, but they may not be a viable option. They may be meeting in November.

Mr. Pettinato suggested we instead schedule the Software Sector Meeting to convene with the Weighing Sector again. This would typically be in Annapolis, Maryland. The dates are still up in the air, but it would be close to Labor Day. The Grain Analyzer meeting is August 16 - 17. The Western Meeting also occurs in this timeframe.

The MDMD work group meeting might be another option, but it's in April, and they're not actually a Sector. They meet in Columbus, Ohio. This could help us get on the agenda for each of the other Sectors with any recommendations we might have for NCWM Publication 14.

Mr. Pettinato recommended we leave the decision up to Mr. Truex and Mr. Flocken depending on logistics and availability of open dates.

Conclusion:
After reviewing potential scheduling conflicts in the August/September timeframe, the group is leaning toward favoring the April option in conjunction with the MDMD meeting.   Mr. Flocken will contact Mr. Robert Kensington (Chair of the MDMD Work Group) to verify that the MDMD work group would be okay with combining the meetings.

Appendix A

Acceptable Menu Text/Icons for Weights and Measures information

Permitted Menu Text examples	*Permitted Icon shape examples*	*Essential characteristics*
Information Info		Top level menu text or icon • Icon text is a lower case "i" with block serifs • Text color may be light or dark but must contrast with the background color • Icon may have a circular border • Activation of this menu text/icon may invoke a second level menu text/icon that recalls metrology information.
Help ?		Top level menu text or icon • Icon text is a question mark • Text color may be light or dark but must contrast with the background color • Icon may have a circular border • Activation of this menu text/icon may invoke a second level menu text/icon that recalls metrology information.
Metrology Metrological Information		Top or second level menu text or icon • Icon text is an upper case "M" • Text color may be light or dark but must contrast with the background color • Icon may have a circular, rectangular, or rounded rectangle border. • If present, the activation of this menu text/icon must recall at a minimum the NTEP CC number.
NTEP Data N.T.E.P. Certificate		This one is debatable – what if the certificate is revoked? Does NTEP grant holders of CCs the right to display the logo on the device, or just in documentation?
Weights & Measures Info	W&M W/M	

Ms. Tina Butcher mentioned that the Weighing Sector has a Weighing Checklist that has a similar set of approved symbols, so the examples shown above would be in line with their current practice.

THIS PAGE INTENTIONALLY LEFT BLANK