December 2003

Inspecting Equipment with Audit Trails

By Juana Williams

Did you ever encounter a device equipped with audit trail security? Audit trails are an acceptable form of electronic security for protecting a device's metrological features. Audit trails are recognized in NIST Handbook 44 General Code paragraph G-S.8. *Provision for Sealing Electronic Adjustable Components* and in the provisions for sealing sections within many device codes. The device-specific code requirements for audit trails specify a category number, based on the means to access metrological features, and a required method of sealing a particular category of device. When device codes do not include specific provisions for audit trail security, General Code paragraphs G-S.8. or G-A.3. *Special and Unclassified Equipment* may apply.

Both physical seals and/or electronic security are recognized by Handbook 44 to prevent unauthorized or accidental access to device features that affect (1) the accuracy and validity of measurements or transactions, (2) compliance with weights and measures requirements, or (3) the suitability for use of a device in a particular application. These same features that require sealing or security are also known as configuration parameters or calibration parameters.

The manufacturer selects the method of sealing or securing a device's metrological features and must ensure that method complies with Handbook 44 requirements. Typically, no individual manufacturer or single device type uses the exact same set up for electronic audit trail security. Part of the duties for weights and measures officials and service industry representatives is to verify that a device's audit trail security meets minimum requirements for (1) the amount of stored information, (2) proper operation, and (3) access to that stored information.

Audit trails provide many benefits to the manufacturer, operator, and consumer. For the manufacturer, audit trails provide an alternative means for securing electronic features. Unlike physical seals, an audit trail record includes information about changes to features and alerts officials that further investigation is necessary. The audit trail provides evidence to both the device owner and official that tampering may have taken place. Because audit trails are an automatic electronic record of changes to features they provide a deterrent to fraud. More in-depth computer-based training is nearing completion for those interested in the fundamentals and requirements for audit trail security. The Audit Trail Device Security CD-ROM will be available in early 2004.

NIST Handbook 44 code references: *G.S8 and G-UR.4.5*

Verification of device security is a routine part of the inspection process. The procedures for accessing and using audit trail information are as follows:

1. Review the NTEP Certificate of Conformance Sealing section; if there is none, refer to alternate sources of sealing and security information (manuals, manufacturer, etc);
2. Follow the steps for accessing the information;
3. Record and/or print audit trail information;
4. Exit the audit trail view mode;
5. Compare current audit trail values to previous values;
6. Refer to the General Code or other device-specific codes when no code requirements exist in Handbook 44; and
7. Determine the appropriate course of action based on test data, audit trail information, business history, complaints, jurisdiction policy, and other pertinent information.