EAC Decision on Request for Interpretation 2009-04
(Audit Log Events)

2002 VSS Volume I:
2.2.4.1, Common Standards, 2.2.5.1 System Audit
2005 VVSG Volume I:
2.1.4 Integrity, 2.1.5 System Audit, 2.1.5.1 Operational Requirements, 5.4.3 In-Process Audit Records

Date:

September 29, 2009

Question:

What items constitute an "event" as it relates to the requirements of a voting system's audit logging?

Section of Standards or Guidelines:

2002 VSS

2.2.4.1 Common Standards

To ensure system integrity, all systems shall:

- **a**. Protect, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place;
- **b**. Protect against the interruption of electronic power;
- **c.** Protect against generated or induced electromagnetic radiation;
- **d**. Protect against ambient temperature and humidity fluctuations;
- **e**. Protect against the failure of any data input or storage device;
- **f.** Protect against any attempt at improper data entry or retrieval;
- **g.** Record and report the date and time of normal and abnormal events;
- **h**. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.)
- **i.** Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator; and Include

built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.

2.2.5.1 System Audit Purpose and Context

Election audit trails provide the supporting documentation for verifying the correctness of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.

The following audit trail requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of error associated with manually generated audit records. Because most audit capability is automatic, the system operator has less information to track and record, and is less likely to make mistakes or omissions.

The sections that follow present operational requirements critical to acceptable performance and reconstruction of an election. Requirements for the content of audit records are described in Section 4 of the Standards.

The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail that ITAs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package (TDP). Documentation of items such as paper ballots delivered and collected, administrative procedures for system security, and maintenance performed on voting equipment are also part of the election audit trail, but are not covered in these technical standards. Future volumes of the Standards will address these and other system operations practices. In the interim, useful guidance is provided by the *Innovations in Election Administration #10, Ballot Security and Accountability,* available from the FEC's Office of Election Administration.

2005 VVSG

2.1.4 Integrity

- **g**. Record and report the date and time of **normal and abnormal events**
- **h**. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process)
- **i.** Detect and record **every event**, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator

2.1.5 System Audit

This subsection describes the context and purpose of voting system audits and sets forth specific functional requirements. Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.

These requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of error associated with manually generated audit records. Because most audit capability is automatic, the system operator has less information to track and record, and is less likely to make mistakes or omissions. The subsections that follow present operational requirements critical to acceptable performance and reconstruction of an election. Requirements for the content of audit records are described in Section 5.

The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail so that test labs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package.

2.1.5.1 Operational Requirements

Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records shall address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described below.

- **a.** The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below.
  - **i**. Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.
  - **ii**. All systems shall include a real-time clock as part of the system’s hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.
  - **iii**. All audit record entries shall include the time-and-date stamp.

5.4.3 In-process Audit Records

In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:

- **a.** Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
  - **i.** The source and disposition of system interrupts resulting in entry into exception handling routines

ii. All messages generated by exception handlers

iii. The identification code and number of occurrences for each hardware and software error or failure

iv. Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing

v. Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies

b. Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to:

i. Diagnostic and status messages upon startup

ii. The "zero totals" check conducted before opening the polling place or counting a precinct centrally

iii. For paper-based systems, the initiation or termination of card reader and communications equipment operation

iv. For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes

c. Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors

d. System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed

Discussion:

The purpose of the numerous audit log requirements in the VSS/VVSG is to enable the reconstruction of events related to a specific election. To determine each series of events occurring on the election system during a specific election – from ballot creation through the accumulation of the election's official results, it is necessary for the system(s) to record and retain a log of **all** significant events.

For the purposes of a voting systems audit log requirements, an "event" is defined as any occurrence that may have, alone or in combination with other occurrences, a significant impact upon election data, the management or integrity of the voting system, or configuration, setup, and delivery of the voting and tabulation functions of the system.

Examples of significant events include:

- Booting and shutting down of a system.
- Logging into and signing off of a system.
- Failed attempts at logging onto a system.
- Session connections by operators or sub-systems.
- Starting and stopping of a program (also when launched from a menu).

- Reading of precinct media into the central system.
- Data transfer from one machine or program to another machine or program by any means.
- Write operation to a data file or database.
- Creation or modification of a ballot definition.
- Transfer of the ballot definition.
- Generation of reports.
- Manual inserts or modifications to election results.
- Error messages.
- Recovery from a power or component failure.
- Password changes.
- Readiness testing.
- Opening and closing of polls.
- Adding or removing precinct machines to the election setup and/or operational status.

The list above is not intended to be a comprehensive list. It is a sampling of the types of messages that must be recorded in the logs. Additionally, it should be noted as per the VVSG, that all log entries must be time-stamped. Data transmissions from the precincts and uploads from media must also record the number of ballots transmitted or uploaded.

Conclusion:

This RFI is meant to ensure that all election systems record the necessary events in their audit logs as required by the VSS/VVSG sections noted in this document.

Applicability:

Immediate- for all voting system test plans submitted after the date of this document.