EAC Decision on Request for Interpretation 2008-12
(Ballot marking Device/ Scope of Testing)

2005 VVSG Volume1: 2.1.5. System Audit
2005 VVSG Volume1: 2.1.5.2 Shared Computing Platform

Date:
December 19, 2008

Question:

1. Does the ballot marking device use a shared computing platform as intended by Section 2.1.5.2 “Use of a shared computing platform”?

2. Does the ballot marking device “Host Election Software” that would require operating system audit enabled to ensure the accuracy and completeness of election data stored on the system as defined in section 2.1.5.2

Section of Standards or Guidelines:

VVSG 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.

Documentation of items such as paper ballots delivered, paper ballots 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. Useful guidance is provided by the Innovations in Election Administration #10; Ballot Security and Accountability, available on the EAC's website.

VVSG 2.1.5.2 Use of Shared Computing Platforms

Further requirements must be applied to Commercial-off-the-Shelf operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations, including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these systems is vulnerable to unintended effects from other user sessions, applications, and utilities executing on the same platform at the same time as the election software.

"Simultaneous processes" of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.

Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

Discussion:

The VVSG does not specifically address the terminology described in the RFI question "Ballot Marking Device". However it does talk to this type of capability in Appendix C as an informative section. One section of that appendix is listed below as demonstration of relevance but also describes other types of ballot marking devices and functions.

C.1.2.4 Direct IV Systems

Direct Independent Verification systems produce a record that the voter may verify directly with the voter's senses and which is then preserved for auditing or counting. Some optical scan voting systems fit this category, as well as DREs with VVPAT capability.

Conclusion:

It is not appropriate to issue a global clarification that exempts any existing or potential equipment that place a mark indicating a voting selection on a paper ballot, as always being exempt from the requirements of 2.1.5 and 2.1.5.2.

For a given system some requirements may appropriately be determined to be not applicable, which could include specific ballot marking devices. Those determinations will have to be decided on a case by case, model by model, revision by revision basis, primarily by the VSTL, and then presented to the EAC for approval.

Response to the specific questions posed in the RFI:

1. The ballot marking device may or may not use a shared computing platform depending on specifically how the design of a ballot marking device is implemented and what features are included.

2. The ballot marking device may or may not host election software depending on specifically how the design of a ballot marking device is implemented and what features are included.

Applicability:

Immediately for all voting system whose initial certification has not been issued as of the date of this document.