EAC Decision on Request for Interpretation 2012-04 (Software Setup Validation)

2005 VVSG Volume I, Section 7.4.6.e

Date:

August 23, 2012

Question:

Does the 2005 VVSG require a trusted external interface or can voting system software be validated by other means?

Section of Guidelines:

7.4.6.e Software Setup Validation

e. Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.

i. The external interface shall be protected using tamper evident techniques
ii. The external interface shall have a physical indicator showing when the interface is enabled and disabled
iii. The external interface shall be disabled during voting
iv. The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software

Discussion:

The requestor suggests the standard's intent should be to ensure the system's software can be verified through either a trusted external interface or by other secure and trusted means. The requestor states that the read-only external interface is one method which could be used to accomplish verification, but that an external interface that is not read-only could also be used for the verification process.

The requestor believes that if an alternative method (i.e., something other than an external interface) is used, then the requirements in Section 7.4.6.e.i-iv do not apply. Additionally, the requestor states that if an alternative method is used the manufacturer must provide procedures and describe functional safeguards so that the VSTL can evaluate the alternative method's compliance with the 2005 VVSG. Finally, the requestor notes that the VSTL will review the proposed alternative method to several requirements in the 2005 VVSG.

Conclusion:

Although there is potential to read the language of 7.4.6e in two different ways, the EAC finds that it shall be read in the following manner. *Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface (such as a read-only external interface, or by other means.)* This interpretation ensures consistency with the intent of the standard. Also, any other interpretation of the sentence would make a trusted external interface optional and would thus obviate, or at least make conditional, the requirements i-iv. Since the requirements were included as mandatory "shall" requirements any other interpretation would be inconsistent with the plain language of the standard.

The EAC disagrees with the requestor's interpretation of the requirements. The implementation of the software setup validation provided by the requestor does not meet the requirements of Section 7.4.6.e.

The intent of this standard is to require manufacturers to provide a method to validate that only authorized software is present on the voting system and any modification to the software shall be tracked. Section 7.4.6.e states:

> "*Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.*"

The EAC finds that 7.4.6.e. requires an external interface but that a read-only interface is one alternative way of meeting the requirement. Thus, the sentence in question shall be interpreted such that any trusted external interface implemented must be as secure as a read-only interface.

An external interface is a feature to enable commands, status or data to transcend the physical boundary of a device. The boundary for voting equipment is the physical enclosure of the voting machine and is defined as a secure boundary that prevents unauthorized access without detection (e.g., seals, locks, software write-blockers). The interface can be implemented in various ways including: human, mechanical and electrical interactions. Examples of human interfaces include displays, buttons and keyboards. Mechanical interfaces are less common in today's equipment, but may be implemented to mechanically move ballot sorters, deflectors, etc. The primary interface for this RFI is an electrical interface placed at the physical boundary of the equipment that communicates commands, status, and/or data to and from the system that is contained inside the enclosure to an outside interface or entity (e.g., another computer).

The EAC considers 7.4.6.e.i-iii as requirements systems shall meet without exception, as there is not a conditional clause allowing 7.4.6.e.i-iii to go unmet. Requirement 7.4.6.e.iv is strongly recommended, but allows for implementation of an external interface that does not provide read-only access. This interpretation is in line with proposed future iterations of the VVSG. Practical applications of this RFI require all systems to have an external interface. This interface does not need to be dedicated to the single task of software validation.

Effective Date:

Effective for all systems without an approved application for testing.