Draft Recommendations for Setup Validation: Supplement to the 2002 Voting Systems Standard

Draft Version March 2, 2005

National Institute of Standards and Technology (NIST)

Provided for consideration by the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission under the requirements of the Help America Vote Act (HAVA) of 2002.

Acknowledgements

The National Institute of Standards and Technology (NIST) would like to acknowledge the individuals and groups who helped contribute to the preparation of this document. Members of Technical Guidelines Development Committee (TGDC) and the NIST voting team that provided substantial assistance. NIST would also like to acknowledge the IEEE organization for permission to use excerpts from the IEEE P1583 Draft Standard for the Evaluation of Voting Equipment.

Authority

This document has been provided for consideration by the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission under the requirements of the Help America Vote Act (HAVA) of 2002.

Disclaimer

This document is a work in progress, provided solely as draft input to the TGDC. Portions of this document may change substantially. This document references some material from an unapproved draft of a proposed IEEE Standard, P1583. As such, the material is subject to change in the final standard. Because this material is from an unapproved draft, the IEEE recommends that it not be utilized for any conformance/compliance purposes. It is used at your own risk.

1. Introduction

The Technical Guidelines Development Committee (TGDC) of the Election Assistance Commission (EAC) has tasked the National Institute of Standards and Technology (NIST) via TGDC resolution 16-05 "Setup Validation" to research and develop standards specifying characteristics of acceptable setup validation methods. This document represents NIST's response to the tasking called for in TGDC resolution 16-05 "Setup Validation."

1.1 Scope

This section analyzes TGDC resolution 16-05 "Setup Validation" and scopes the issues raised in the resolution to provide a framework by which the issues can be addressed systematically. The complete text of TGDC resolution 16-05 "Setup Validation" has been included in Appendix A as a reference.

The scope of the TGDC resolution 16-05 "Setup Validation" is unclear because the first two sentences of the resolution seem to have different views of the scope of the resolution. In the general, a voting system is a large system composed of several other systems including but not limited to polling place systems, central counting/aggregation systems, and election management systems. These systems reside on several different computer based platforms and at different locations. The first sentence of the resolution uses the term "electronic voting machine" which seems to limit the scope of the resolution to the part(s) of a voting system deployed to polling places used to collect cast ballots; not the "machines" or systems used to centrally count/aggregate cast ballots or for election management. However, the second sentence of the resolution use the general term of "a voting system" which seems to widen the scope of the resolution to all parts of a voting system; not just those deployed at polling places used to collect cast ballots. This document will consider the scope of the resolution cover setup validation methods for all parts of a voting system.

The text of the resolution provides some insight into what is considered covered by an acceptable setup validation method. The second sentence of the resolution clearly states a setup validation method determines that only authorized software is present on a voting system and unauthorized software is absent. The resolution does not contain text addressing how authorized software is installed or unauthorized software is prevented from being installed on the voting system, so this will not be discussed in the document.

The second sentence of resolution also says a setup validation method determines the voting system is in the "proper initial state." However, the resolution does not contain text about how a voting system reaches this "proper initial state." Although process used to put a voting system into the "proper initial state" affects the assurance of the voting system, this seems to be beyond the scope of the resolution and will not be discussed in this document. In addition, the text of the resolution does not provide guidance on what software and/or hardware needs to be inspected to determine the voting system is in a "proper initial state." Since the resolution specifically refers to software that should and should not be on the voting system, this document will focus on ensuring that the software that should be on the voting system is in the "proper initial state" such as registers and variables containing an appropriate value. As a result issues related to the setup validation of the voting system's hardware such as being connected to a proper backup power supply will be considered beyond the scope of this document. This document will provide a list of software related items that needs to be inspected, and when appropriate possible techniques to perform the inspection, to determine the voting system is in a "proper initial state."

The techniques and tools used to inspect the items may be very implementation specific, however the resolution is clear that the techniques and tools used to inspect items should not change the state of the voting system or execute software installed on the voting system. However, it is unclear if the computing capability of the voting system can be used to perform the setup validation. If possible, this document will provide requirements so that the computing capability of the voting system can be used to perform the setup validation.

The following is a summary of the assumptions and interpretations upon which the recommended requirements for setup validation methods will be created:

- the scope of the resolution to include all parts of the voting system – polling place systems, central counting/aggregation systems, and election management systems.
- process used to install authorized software or prevent unauthorized software from being installed on the voting system will not be discussed in the document;
- process used to put a voting system into the "proper initial state" will not be discussed in this document;
- if possible, this document will provide requirements so that the computing capability of the voting system can be used to perform the setup validation; and
- a list of items that needs to be inspected, and when appropriate possible techniques to perform the inspection, to determine the voting machine is in a "proper initial state" will be provided by this document.

2. Proposed Recommendations

The following are NIST recommendations to the TGDC be considered for inclusion in voting system standards related to the setup validation methods for voting systems.

2. 1 General Requirements

1) The vendors shall identify and document all voting system software required to be installed on voting system for proper operation including the software jurisdictions are required to modify to conduct a specific election.

2) The vendors shall identify and document all static and dynamic registers and variables used by the voting system software including the values jurisdictions are required to modify to conduct a specific election.

3) The vendors shall document the values for all the static registers and variables; and initial starting values of all dynamic registers and variables listed for voting system software except for the values set by jurisdictions.

4) Jurisdictions shall verify that only the software listed by the vendors is installed on the voting system.

5) Jurisdictions shall verify that software not listed by the vendors is absent from the voting system.

6) Jurisdictions shall obtain reference information (See TGDC resolution 15-05: Software Distribution) for the software listed by the vendors from an authoritative source.

7) Jurisdictions shall identify and document the list of all voting system software that it customizes for an election.

8) Jurisdictions shall document the values for all the static registers and variables; and initial starting values of all dynamic registers and variables listed for voting system software it customizes for an election.

9) Jurisdictions shall generate reference information (See TGDC resolution 15-05: Software Distribution) for all that the software it customizes for an election.

10) Jurisdictions shall verify that all software on the voting system has not been modified using the reference information

11) Jurisdictions shall verify that all the static registers and variables; and initial starting values of all dynamic registers and variables are consistent with the documented values provided by the vendors and jurisdictions.

12) Jurisdictions shall document the results of the verification performed on the voting system. The document shall include the date, time, results, location of verification, time, the list of software verified, name of the people that preformed the verification, verification technique used, authoritative source of reference information, identifying information of media with reference information (if appropriate), and unique identifiers of the voting systems inspected.

13) The techniques used by jurisdictions to inspect software, register values, and variable values of a voting system shall only execute software not installed on the voting system being inspected.

14) The techniques used by jurisdictions to inspect software, register values, and variable values of a voting system shall not modify of the software, register values, variable values on the voting system being inspected.

15) Vendors of voting systems shall provide a means to access the installed software on a voting system so that it may be inspected and verified.

A.1 Appendix A: Text of TGDC Resolution 16-05: Setup Validation

The TGDC has considered the issue of electronic voting machine setup validation, and has concluded that current standards and practice need substantial improvement in this regard. A setup validation method ensures that a voting system contains the authorized software, contains no unauthorized software, and is in the proper initial state. The TGDC requests NIST to do research and develop standards:

1. That specify the characteristics of acceptable setup validation methods (such as, for example, that the setup validation method may not modify the state of the system nor require the execution of any software currently on the system), and
2. That require each voting system submission to specify an acceptable setup validation method.