COMMONWEALTH OF VIRGINIA

Voting Systems Management Policy

VOTING SYSTEMS SECURITY POLICY

State Board of Elections

Preface

Version	Date	Purpose of Revision
Original	Jul 2004	Base Document: COV VSM Policy *SEC2004-01*
Revision 2	Jul 2008	Updates in accordance with changes to the *Code of Virginia* as well as other minor content adjustments.

Publication Designation

COV VSM Policy SEC2008-01

Subject

Voting System Security

Effective Date

March 20, 2009

Supersedes

Supersedes any existing policy.

Scheduled SBE Review

One (1) year from the effective date, and annually thereafter.

Authority

Code of Virginia, § 24.2-103
(Powers and duties in general of the State Board of Elections)

Code of Virginia, §§ 24.2-625 - 642
(Voting Equipment and Systems)

COV ITRM Policy SEC500-02
(Information Technology Security Policy)

COV ITRM Standard SEC501-01
(Information Technology Security Standard)

Scope

This policy is applicable to all county and city electoral boards, general registrars and officers of election that are engaged in such functions as purchasing, testing, managing, and operating voting equipment and systems.

Purpose

To define the State Board of Elections' Voting System Security Program and the recommended minimum security requirements for a county or city electoral board's and registrar's security program. This policy recognizes that overall security of voting systems within the Commonwealth is achieved through the collective operation of the various county and city programs.

Objectives

The objective of this policy is to establish and promulgate guidance for the protection of county and city voting systems and the elections data they collect, store, and transmit.

General Responsibilities

State Board of Elections
In accordance with the *Code of Virginia, § 24.2-103*, the State Board of Elections is assigned the

following duties: "…supervise and coordinate the work of the county and city electoral boards and of the registrars to obtain uniformity in their practices and proceedings and legality and purity in all elections." The State Board of Elections "shall make rules and regulations and issue instructions and provide information to the electoral boards and registrars to promote the proper administration of election laws."

In accordance with the *COVA ITRM Policy SEC500-02*, the State Board of Elections is "Responsible for complying with COV ITRM policies and standards and considering COV ITRM guidelines issued by the Secretary of Technology."

Secretary of the State Board of Elections

In accordance with the *Code of Virginia, § 24.2-102*, "The Governor shall designate one member of the Board as the Secretary…." The Secretary of the State Board of Elections "…may employ the personnel required to carry out the duties imposed by this title" (i.e., *Code of Virginia, Title 24.2*).

County and City Electoral Boards

In accordance with the *Code of Virginia, § 24.2-109*, the electoral board "…shall perform the duties assigned by this title (i.e., *Code of Virginia, Title 24.2*) including, but not limited to, the preparation of ballots, the administration of absentee ballot provisions, the conduct of the election, and the ascertaining of the results of the election."

In accordance with the *Code of Virginia, § 24.2-625.1, paragraph D*, "The electoral board of each county and city that utilizes electronic voting systems shall develop and annually update written plans and procedures to ensure the security and integrity of its electronic voting systems."

County and City Officers of Election

In accordance with the *Code of Virginia, § 24.2-109*, officers of election are sworn to "…perform the duties of this election according to the law and the best of my ability..." and "…studiously endeavor to prevent fraud, deceit, and abuse in conducting this election."

Definitions

See Glossary

Related COV ITRM and VSM Policies, Standards, and Guidelines

COV ITRM Standard SEC501-01, Information Technology Security Standard; Dated July 24, 2008

COV VSM Standard SEC2005-01.1,

Voting Systems Security Standards; Dated January 17, 2005

COV VSM Guideline SEC2005-01.1, Voting System Security Guidelines; Dated January 17, 2005

COV VSM Self-Assessment Guide SEC2005-01.1, Voting System Security Self-Assessment Guide; Dated January 17, 2005

Table of Contents

Statement of Policy for Voting Systems Security

The use of direct recording electronic (DRE) voting, optical scan electronic counting, and electronic ballot marking systems within the Commonwealth has grown over the last several years. The migration to these systems, in large part, was in response to the Help America Vote Act of 2002 (HAVA). Three HAVA provisions provided impetus for this shift. First, HAVA authorized funding for the replacement of punch card and lever voting equipment. Second, in 2006, HAVA began requiring that voting systems notify voters of over-votes and permit them to review their ballots and correct errors before casting their ballots. Third, also beginning in 2006, HAVA required that each polling place used in a federal election have at least one voting machine that is fully accessible for persons with disabilities. DRE voting systems and optical scan counting systems [in concert with accessible ballot marking devices] fulfill the accessibility requirement of HAVA. These electronic systems also satisfy the error prevention and correction requirements of HAVA.

With the pervasive use of electronic voting systems across the Commonwealth, the State Board of Elections recognizes these systems are computer-based and, as such, are subject to the same security concerns and necessary safeguards as other Information Technology systems. Consequently, in accordance with COV ITRM Policy SEC500-02, *Information Technology Security Policy*, the State Board of Elections published this *Voting Systems Security Policy* which establishes a formal Voting Systems Security Program.

It is the policy of the State Board of Elections that each electoral board is responsible for the security of ALL voting systems under their control and that they shall take appropriate steps to provide for the security of these systems through the implementation of a local Voting Systems Security Program (VSSP). The State program requires each locality to develop a written security plan and update it annually; this requirement was codified by the General Assembly in 2007 (*§ 24.2-625.1(D)).*

While some details of each local jurisdiction's security program may vary depending on the number and type of voting systems in use and the jurisdiction's elections environment, the core considerations should be similar for all localities. Each Electoral Board shall establish and maintain an effective Voting Systems Security Program and document that program in a security plan. Each plan must be submitted to SBE for review. SBE will formally endorse each plan that meets all of the requirements of the *Voting Systems Security Standards*, COV VSM Standard SEC2005-01.1.

Glossary

Authorized Personnel – Those individuals granted access to voting system components by an electoral board.

Critical – The term "critical" refers to those voting system components whose unavailability or improper use has the potential to adversely affect the ability of the Commonwealth or the local jurisdiction to conduct an election and/or to maintain the legality and purity of the elections process.

Confidential Information – The term "confidential information" refers to information prohibited from public disclosure that may cause harm to the state or local jurisdiction, its citizens or other individuals or organizations.

Elections Information – The term "elections information" means any communication or representation of ballot, vote or voter information in any medium or form, including textual, numerical, graphic, narrative or audiovisual forms.

Elections Personnel – The term "elections personnel" refers to ALL personnel employed or appointed /designated to support the testing, preparation, operation, movement, or storage of voting systems, including officers of election and/or contractors and their employees.

Sensitive Elections Information – The term "sensitive elections information" refers to any confidential or elections information for which the loss, misuse, or unauthorized access to or modification of or improper disclosure of could adversely affect the creditability of the elections process or the privacy of individual voters.

Voting Systems - The term "voting system" refers to the total combination of mechanical, electro-mechanical, and electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to: define ballots; cast and count votes; report or display election results; and to maintain and produce any review trail information. Voting Systems also include the procedures, practices, and associated documentation used to: identify voting system components and versions of such components; test the system during its development and maintenance; maintain records of system errors and defects; determine specific system changes to be made a system after the initial qualification of the system; ensure optimal security of the voting device; and make available any materials to the voter (such as notices, instructions, forms, or paper ballots).