COMMONWEALTH OF VIRGINIA

Voting Systems Management Standard

VOTING SYSTEMS SECURITY STANDARDS

State Board of Elections

Preface

Publication Designation

COV VSM Standard SEC2005-01.1

Subject

Voting Systems Security

Effective Date

January 17, 2005

Supersedes

Does not supersede any existing standard.

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 to 24.2-642
(Voting Equipment and Systems)

COV ITRM Policy 90-1
(Information Technology Security Policy)

COV ITRM Standard SEC2001-01.1
(Information Technology Security Standard)

COV ITRM Standard SEC2003-02.1
(Information Technology Security Standard)

Scope

This standard 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, maintaining and operating voting systems.

Purpose

1. To define the minimum requirements for the administration of an electoral board's Voting Systems Security Program.

2. To promote the appropriate protection of voting systems within the Commonwealth.

3. To facilitate the adoption of information security principles in the protection of voting systems.

Objectives

1. Define and promulgate the minimum-security standards for the protection of the voting systems.

2. Provide for the compilation of planning material and documentation to support the development and implementation of local Voting Systems Security Programs.

3. Clarify the security safeguards to be addressed as part of a local jurisdiction's security program.

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."

Secretary of the State Board of Elections
In accordance with the *Code of Virginia*, *§ 24.2-102*, the Secretary of the State Board of Elections "…may employ the personnel required to carry out the duties imposed by this title."

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 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."

County and City General, Assistant, and Special Assistant Registrars

In accordance with the *Code of Virginia*, *§ 24.2-114*, the general, assistant, and special assistant registrars shall "Carry out such other duties as prescribed by the electoral board."

County and City Officers of Election
In accordance with the *Code of Virginia*, *§ 24.2-611*, 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 VSM Policies, Standards, and Guidelines

COV VSM Policy SEC2005-01, Voting Systems Security Policy; 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

Introduction

The continuing support and involvement of County and City electoral boards is a prerequisite for an effective Commonwealth-wide Voting Systems Security Program. Electoral Board responsibilities shall include the following:

- Establishing local Voting Systems Security Programs that meet or exceed the requirements established in this standard.
- Administering local Voting Systems Security Programs.

The electoral boards shall formalize their local Voting Systems Security Programs in writing. This documentation will be used to communicate the specific local procedures needed to implement the security program. The documentation shall contain information on all aspects of the program, inclusive of the following twelve mandatory security safeguard components:

1. Security Risk Assessment
2. Security Awareness and Training
3. Security Incident Handling
4. Security Monitoring and Review Control
5. Security Contingency Planning
6. Access Management
7. Physical Access Controls
8. Environmental Controls
9. Access Control
10. Configuration Management
11. Testing
12. Network Security

The electoral boards shall provide the State Board of Elections copies of all the Voting Systems Security Program-related documentation they develop and document in conjunction with satisfying the requirements of this standard.

This standard supports the Statement of Policy for Voting Systems Security (COV VSM Policy SEC2005-01) endorsed by the State Board of Elections. Additionally, those security best practices that are recommended as associative guidelines, but which are not mandatory, are stated in COV VSM Guideline SEC2005-01.1, *Voting Systems Security Guideline*.

Background

This standard is applicable to all County and City electoral boards that, purchase, lease, test, manage, and operate voting systems in the Commonwealth.

Responsibility for the development and implementation of the Local Jurisdiction's Voting Systems Security Program begins at the electoral board level and flows down through the general registrar and employees to the officers of election.

- The electoral board is responsible for the security of the voting systems within its local jurisdiction.
- The electoral board is responsible for implementing and maintaining an adequate Voting Systems Security Program.
- The electoral board is responsible for determining adequate and appropriate levels of protection for the voting systems under their control to prevent unauthorized access to or alteration of equipment and systems and to ensure effective and accurate functioning and continuity of the elections process.
- The electoral board is responsible for ensuring the adequate and appropriate levels of protection for the voting systems under their supervision to prevent unauthorized access or disclosure, and to ensure effective and accurate functioning and continuity of election operations.
- Each election official, including electoral board members, general registrars, assistant registrars, special assistant registrars, officers of election, voting machine custodians, and electoral board staff members is responsible for the adequate protection of voting systems within their control or possession.

Approach

The State Board of Elections' Voting Systems Security Program is based upon the following voting systems security principles.

1. Voting systems are critical and vital assets to the Commonwealth.
2. These assets require a degree of protection commensurate with their value (material and non-material) to the Commonwealth.
3. Measures should be taken to protect these assets against accidental or unauthorized disclosure, alteration or destruction, as well as to assure their security, reliability, integrity and availability.
4. The protection of assets is a management responsibility.
5. Access to voting systems must be strictly controlled.
6. Information that is sensitive or confidential must be protected from unauthorized access or alteration.

7. Voting systems components that are essential to the proper functioning of voting systems must be protected from theft, vandalism, tampering, alteration, loss or destruction.

8. Risks to voting systems must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected.

9. The integrity of voting systems software must be assured. Changes to software must be made only in authorized and acceptable ways.

10. Security needs must be considered and addressed in all phases of elections operations.

11. Security awareness and training of elections personnel is one of the most effective means of reducing vulnerability to security risks and must be continually emphasized and reinforced. All elections personnel must be accountable for their actions relating to voting systems.

12. Voting Systems Security Programs must be responsive and adaptable to changing operational and environmental vulnerabilities and technologies.

The State Board of Elections' Voting Systems Security Program addresses the security of voting systems across three types of security safeguards:

- Administrative
- Physical
- Technical

Each of these safeguard areas is further divided into security components that serve as the basis for the standards set forth in this Voting Systems Security Standard. These security safeguard areas and components comprise a Voting Systems Security Framework. The security safeguard areas and their associated components contained in the framework are shown in the table below.

Security Safeguard Type	Security Component
Administrative	Security risk assessment Security awareness and training Security incident handling Security monitoring and review control Security contingency planning Access management
Physical	Physical access controls Environmental controls
Technical	Technical access control Configuration management Testing Network security

Voting Systems Security Framework

All voting systems security standards shall be implemented in accordance with COV ITRM Policy 90-1, *Information Technology Security Policy* and COV ITRM Standard 2001-01.1, *Information Technology Security Standard*.

Reviews

A full, annual review of COV VSM Standard SEC2005-01.1 is anticipated.

Statement of Standards for the Voting Systems Security Framework

This section groups the specifications of the Voting Systems Security Standard by the security safeguard types that comprise the Voting Systems Security Framework.

A. Administrative Security Safeguards

Administrative security safeguards refer to those standards, procedures, and actions taken to manage the selection, development, implementation, and maintenance of security measures to protect voting systems and to manage the conduct of elections personnel in relation to the protection of voting systems.

A.1. Security Risk Assessment

The purpose of a security risk assessment is to identify and evaluate the risks to which a local jurisdiction's voting systems are subject. For example, the existence of a potential risk, the probability of a risk occurring and the resultant impact of its occurrence would be assessed during such an assessment. Examples of potential risks to voting systems that would adversely impact a local jurisdiction include loss, theft, vandalism, tampering, or alteration. Examples of potential impacts that would adversely affect a local jurisdiction include financial loss, public embarrassment, loss of public confidence, noncompliance with Commonwealth or Federal statutes, and degraded capability to conduct elections.

Based upon the risk assessment, the electoral board determines what types of safeguards are appropriate to address the identified risks. In this manner, the administrative, physical, and technical safeguards put in place reflect those security safeguards that are reasonable and appropriate for a local jurisdiction's technical and operational environments. Security safeguards should be referable back to the risk assessment.

A.1.a. Standards

A.1.a.i. In accordance with COV VSM Policy SEC2005-01, each electoral board must develop, document, implement and maintain a Voting Systems Security Program appropriate to its technical and operational environments.

A.1.a.ii. Voting Systems Security Program documentation must specify how exceptions to any mandatory security standard are to be determined, approved, and documented.

A.1.a.iii. Each electoral board must conduct a security risk assessment to identify the potential security risks to those voting systems for which they

are accountable and to determine the appropriate security safeguards to be implemented to protect these voting systems.

A.1.a.iv. The security risk assessment should be reviewed and updated as necessary (e.g., after a change in equipment or systems, after a change in facilities, after a change in operational procedures), but at a minimum it must be formally reviewed and updated annually (no later than 90 days before each November general election).

A.1.a.v. All Voting Security Programs must include protective measures and procedures to ensure that the appropriate levels of confidentiality, integrity and availability of voting systems are maintained.

A.1.a.vi. Changes in the local jurisdiction's technical and operational environments must be reviewed for security implications by the electoral board; risks must be reviewed and assessed and appropriate safeguards must be put in place. Such reviews must be documented.

A.1.a.vii. Each electoral board must document a Voting Systems Security Policy Statement that describes in broad terms the electoral board's Voting Systems Security Program and the security safeguards and procedures taken to protect the local jurisdiction's voting systems and that can be made available to the media and public.

A.2. Security Awareness and Training

The purpose of security awareness and training is to promote elections personnel awareness, training and responsibility with respect to security risks, policy, standards, guidelines, and procedures related to the protection of voting systems. Elections personnel refer to ALL personnel employed or appointed/designated to support the testing, preparation, operation, movement, or storage of voting systems.

All elections personnel, within a local jurisdiction, need to understand the sensitivity of the jurisdiction's voting systems and their responsibilities in protecting these systems. For example, elections personnel need to be aware of the risks and the associated impacts of compromises to the confidentiality, integrity, or availability of voting systems.

The responsibility to adhere to the *Code of Virginia*, State Board of Elections policy and standards, and local electoral board procedures is accepted when the Oath of Office is taken and signed by electoral board members, general registrars, and officers of election upon their assumption of duties. Security awareness and training programs also provide a proactive mechanism of fostering further comprehension of each individual's responsibilities in sustaining the security of voting systems. They also delineate the security responsibilities of elections personnel based on their specific positions or functional roles; motivate elections personnel towards security-conscious behavior while

performing their duties; and reinforce their understanding of the consequences of security failures upon the elections process.

Security awareness and training programs are most effective when they are composed of a combination of initial and periodic, refresher security training sessions along with on-going security awareness reminders. The amount, depth, and timing of security awareness and training that should be conducted, is a risk-based decision. Additionally, only in extreme circumstances, should personnel begin to perform their duties until they have received their initial security training. Finally, as the local jurisdiction's technical and operational environments change, the local jurisdiction's security awareness and training materials should be updated accordingly.

A.2.a. Standards

A.2.a.i. Each electoral board must develop, document and maintain a Voting Systems Security Awareness and Training Program to ensure that ALL elections personnel are aware of their security responsibilities and know how they are expected to fulfill them.

A.2.a.ii. All elections personnel must receive or have easy access to all security policy, standards, and procedures and security awareness and training instructional materials.

A.2.a.iii. The local jurisdiction's Voting Systems Security Awareness and Training Program must:

- Be approved by the electoral board.
- Define specific timeframes for receiving initial and periodic refresher security training.
- Provide both general and position specific security training content.
- Define a security awareness/reminder program.
- Be documented.
- Be reviewed and revised as required, but at a minimum it must be reviewed and updated annually (no later than 60 days before each November general election).

A.2.a.iv. All new elections personnel must receive formal security training prior to assuming their duties.

A.2.a.v. The date and time of security training must be documented and each individual receiving training must provide written acknowledgement that they have received and understand the training. This written acknowledgement must be maintained as part of the Voting Systems Security Awareness and Training Program documentation.

A.2.a.vi. Periodic, refresher security training must be provided to ALL elections personnel on an annual basis (no less than three nor more than 30 days before each November general election).

A.3. Security Incident Handling

The purpose of security incident handling is to respond to a suspected or known instance where voting systems security policy, standards, and procedures have been violated and/or a security safeguard has been breached. Once a suspected security incident has been identified, it is imperative that it be contained as soon as possible, and then terminated so as to minimize any further damage and/or risk exposure to a local jurisdiction's voting systems and elections process.

The handling of security incidents can be politically, managerially, and technically complex and require information and assistance from sources outside the local jurisdiction (e.g., technical specialists, vendor representatives, law enforcement personnel, public affairs personnel, political party representatives, and State Board of Elections representatives). Each local jurisdiction shall adopt both proactive and reactive means to handle security incidents and limit the negative impacts of such incidents. An example of proactive activity includes, the development and use of a security incident reporting mechanism, such as, a standardized security incident reporting form. An example of reactive activity includes, changing a lock to a facility where voting equipment is stored following the loss of a key.

A.3.a. Standards

A.3.a.i. Each electoral board must develop a Security Incident Response and Reporting Procedure, which identifies the responsibilities and actions to be taken in response to security incidents involving the voting systems.

A.3.a.ii. The local jurisdiction's Security Incident Response and Reporting Procedure must:

- Be approved by the electoral board.
- Identify the general types of incidents that must be reported.
- Identify who is responsible for reporting security incidents.
- Prescribe the mechanisms for reporting security incidents.
- Identify those officials who must receive notification of security incidents.
- Require the documentation of actions taken.
- Require the production of an after action report focused on preventing a recurrence of the incident.
- Be documented.
- Be reviewed and revised as required, but at a minimum it must be reviewed and updated annually (no later than 60 days before each November general election).

A.4. Security Monitoring and Review Control

The purpose of security monitoring and review control is to ensure that the implementation and maintenance of security safeguards are adequately documented and managed and that accountability can be established.

Security monitoring and review control activities should be those parts of an electoral board's overall management responsibilities. They provide a means to assess compliance with security policy, standards, and procedures, verify consistent application of sound operational practices, maintain individual accountability, and support security incident analysis.

Security monitoring and review control activities can be self-administered (by the electoral board) or independently administered (by third-parties). Personnel involved in these activities must have appropriate expertise or training in security management and in review practices, and must be capable of conducting the security monitoring and review control activities in an objective manner.

Security safeguards tend to degrade as personnel discover new ways to intentionally or unintentionally bypass security safeguards or simply become lax in their compliance with security procedures. Each electoral board must therefore make risk-based decisions regarding the timing and the scope of follow up, evaluation, walk-through or formal review of security monitoring and review control activities.

A.4.a. Standards

A.4.a.i. Each electoral board must monitor and review all activities associated with the purchase, testing, configuration, storage, transport, preparation, maintenance and operation of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures.

A.4.a.ii. A formal electoral board or third-party (e.g., County/City internal reviewer, contract reviewer) review must be conducted on an annual basis (no later than 90 days before each November general election), using COV VSM Self-Assessment Guide SEC2005-01.1, *Voting Systems Security Self-Assessment Guide*.

A.4.a.iii. All formal electoral board and third-party audits must be fully documented.

A.5. Security Contingency Planning

The purpose of security contingency planning is to provide for the continued security of voting systems in the event of a disruption in the normal operational environment caused

by a voting systems security policy, standard, or procedure having been violated and/or a security safeguard having been breached. A secondary purpose of security contingency planning is to minimize the effect of such disruptions. Many of the potential effects of security contingencies can be averted, or their impact mitigated, if appropriate steps are taken as soon as possible to control the event that caused the disruption.

A.5.a. Standards

A.5.a.i. Each electoral board shall develop and maintain a Security Contingency Plan (SCP) for the voting systems for which they are accountable.

A.5.a.ii. Each electoral board shall develop, document, maintain and annually test a Security Contingency Plan that will provide a reasonable assurance that the overall security and integrity of the voting system components will be preserved should the local jurisdiction's normal technical and/or operational environment be disrupted.

A.5.a.iii. Each local jurisdiction's Security Contingency Plan must include emergency response procedures appropriate to any incident or activity that may threaten the security or integrity of voting equipment or system components.

A.5.a.iv. Each local jurisdiction's Security Contingency Plan must include:

- A general description of the chain-of command and the decision-making process that will be followed when executing the contingency plan.
- Arrangements, procedures, and responsibilities that ensure that the security and integrity of the voting systems can be maintained if normal technical and/or operational conditions are interrupted for any reason for an unacceptable length of time.
- Procedures and responsibilities to facilitate the rapid restoration of normal security conditions at the primary location (i.e., storage location or precinct location on election day), or if necessary, at an alternate location, following the destruction, major damage or other interruption at the primary location.
- A minimally acceptable, prioritized level of security safeguards for voting systems to guide the relocation of equipment and systems to an alternate location.
- Arrangements and procedures for the implementation of an alternative voting system if the security or integrity of the voting systems cannot be restored.

A.5.a.v. Security Contingency Plans must be fully documented.

A.5.a.vi. All Security Contingency Plans must be operationally tested at a frequency commensurate with the risk and the magnitude of loss or harm that could result from a disruption in the security safeguards of voting systems.

A.5.a.vii. Training and instructional materials prepared for poll workers shall include a description of their responsibilities and authorities relative to the execution of the Security Contingency Plan.

A.6. Access Management

The purpose of access management is to ensure that access to voting systems is consistent with the applicable requirements of Federal and Commonwealth statutes, State Board of Elections policy and standards, and local electoral board procedures.

A.6.a. Standards

A.6.a.i. Only the electoral board may grant/approve access to voting systems.

A.6.a.ii. Only personnel granted access to voting systems by the electoral board may have access to voting systems.

A.6.a.iii. Access may be granted on an identity (by name), role (by job description), location (by local jurisdiction) or some combination thereof basis, and may be defined in terms of the level of access, duration and type (i.e., unaccompanied/accompanied) of the individual's access.

A.6.a.iv. The granting of access must be documented in writing and reflect the following:

- Name, title, organization, work address, office telephone number, of the person being granted access/control.
- The reason for granting access/control.
- Level of access.
- The date access/control is to be granted.
- The date access/control is to end.
- Name, title, organization, address, and telephone number of person granting access/control.

A.6.a.v. Each person to be granted access to voting systems that is to be of appreciable duration or of a recurring nature must receive formal security training prior to gaining access appropriate to level, type and duration of access.

A.6.a.vi. The electoral board must establish an authentication mechanism (e.g., identification badge, authorization letter) that can be used to verify the identity of those accessing voting systems.

A.6.a.vii. The electoral board must review and update the list of individuals granted access to voting systems on an as required basis, but at a minimum it must be reviewed and updated annually (no later than 60 days before each November general election).

A.6.a.viii. The list of personnel granted access to voting systems must be documented.

B. Physical Security Safeguards

Physical security safeguards refer to those standards, procedures, and actions taken to protect voting systems and related facilities and equipment, from natural and environmental hazards, as well as, tampering, vandalism, and theft.

Accordingly, physical security safeguards need to be considered for voting systems in storage (e.g., in warehouses), in transit (e.g., being transported between a warehouse and a polling place), in the polling place (e.g., before and after election-day), and in use (e.g., during election day). Appropriate physical security safeguards need to be established based on the hazards/risks related to the physical location of the voting systems. Lastly, physical security safeguards need to assure that the required levels of infrastructure support such as electric power, heating, and air-conditioning are sustainable.

For example, facility access controls may be used to restrict and monitor the entry and exit of personnel to and from a facility where voting systems are stored. Such facility access controls may range from traditional keyed locks and magnetic keycards/badges to retina scanning personal identification equipment to physical recognition and sign-in by uniformed security personnel. Physical security safeguards need to be considered for all voting systems at all times.

Physical security safeguards provide the primary means of protection for voting systems from natural and environmental hazards, as well as, tampering, vandalism, and theft.

B.1. Physical Access Controls

The purpose of physical access controls is to define the procedures and physical safeguards to control physical access to voting systems and the facility or facilities in which they are housed, whether in storage between elections, in transit to and from a polling location, or in a polling location, while ensuring that personnel granted access by the electoral board are allowed access.

B.1.a. Standards

B.1.a.i. The facility or facilities where voting systems are stored must be secured and access restricted to authorized personnel only.

B.1.a.ii. A method of monitoring and reviewing physical access to voting systems storage locations must be implemented (e.g. identification badges, keycards, access logs, Etc.).

B.1.a.iii. The electoral board must regularly review the list of persons gaining access to voting systems.

B.1.a.iv. While being moved or relocated, voting systems must remain in the physical custody (i.e., in plain view) of authorized personnel at all times.

B.1.a.v. All visitors, vendors, maintenance, Etc. personnel gaining physical access to voting systems must be authenticated through the use of appointments and identification checks and be authorized access to voting systems by the electoral board.

B.1.a.vi. A method of monitoring and reviewing physical custody of voting systems during transport must be implemented (e.g. chain-of-custody log, hand receipts, truck seals).

B.1.a.vii. In the event of an emergency or crisis, the physical security of voting systems must be ensured.

B.1.a.viii. In the event of an emergency or crisis that threatens the physical security of voting systems, the general registrar, the members of the electoral board and the Secretary of the State Board of Elections are to be notified immediately.

B.1.a.ix. The physical security procedures and safeguards controlling physical access to voting systems and the facility or facilities in which they are housed must be documented.

B.1.a.x. All repairs and modifications to the physical components of a facility, where voting systems are stored, that are security related (e.g., walls, doors, locks, cameras, alarm systems, Etc.) must be documented.

B.1.a.xi. Only those functions that are directly elections related are to be performed with voting systems.

B.1.a.xii. The physical security safeguards proscribed by this standard are to be applied to all voting systems.

B.2. Environmental Controls

The purpose of environmental controls is to define the procedures and physical safeguards to secure the physical environment in which voting systems must operate and are stored.

B.2.a. Standards

B.2.a.i. The electoral board must ensure the appropriate fire alarm, and/or fire suppression and prevention systems are installed.

B.2.a.ii. The electoral board must periodically inspect the facility or facilities in which voting systems are housed for potential fire ignition sources, such as improperly stored materials in close proximity to voting systems.

B.2.a.iii. The electoral board must ensure that environmental controls (e.g., heating, cooling, humidity) are adequate to prevent damage to voting systems.

B.2.a.iv. The electoral board must review the risks of damage to voting systems from a failure in electrical power distribution, environmental control, plumbing, or other utilities within the facility or facilities in which voting systems are housed.

B.2.a.v. The electoral board must review the risks to voting systems due to natural disasters, such as tornadoes and flooding and develop, document, and implement appropriate risk mitigation strategies.

C. Technical Security Safeguards

Technical security safeguards refer to the technology and the standards and procedures for its use that protect the integrity and security of voting systems and control access to them.

C.1. Technical Access Control

The purpose of technical access control is to implement technology and procedures that control access to voting systems only to those persons and software authorized by the electoral board.

C.1.a. Standards

C.1.a.i. Voting systems must ABSOLUTELY NOT be remotely accessed.

C.1.a.ii. For those voting system components that are capable of being password protected, the electoral board must establish criteria for password composition, length and aging.

C.1.a.iii. All elections personnel having access to voting system components that are password protected, must create and use passwords in accordance with the criteria established by the electoral board.

C.1.a.iv. For all password protected voting system components that are capable, an automatic logoff feature must be implemented and a record of all logon attempts must be maintained.

C.1.a.v. Password access to voting systems must be terminated when an individual's employment or contract is terminated, or when an individual no longer requires access or when an individual's access is changed.

C.1.a.vi. The electoral board must develop, document and implement voting systems access procedures for use during emergencies (e.g., fires, natural disasters, bomb threat, civil disturbances).

C.2. Configuration Management

The purpose of configuration management is to implement technology and procedures that control the hardware, firmware, software, and documentation configurations of voting systems so that only those hardware, firmware, and software components that have been qualified by Independent Testing Agencies and certified by the Commonwealth become part of a local jurisdiction's voting systems configurations. Central to the implementation of configuration management is establishment of a Configuration Management Database that contains details (e.g., information that relates to the maintenance, movement, and problems experienced) on each of the hardware, firmware, software, and documentation components of a local jurisdiction's voting systems. Configuration Management essentially consists of four tasks:

- **Identification:** this is the specification, identification of all voting systems components and their inclusion in the Configuration Management Database.
- **Control:** this is the management of each voting systems component, specifying who is authorized to "change" (e.g., modify, move) it and whose approval is required for the "change".
- **Status:** this task is the recording of the status (e.g., modifications, problems, movements, Etc.) of all voting systems components in the Configuration Management Database, and the maintenance of this information.
- **Verification:** this task involves local reviews and third-party reviews (if conducted) to ensure that the information contained in the Configuration Management Database is accurate.

C.2.a. Standards

C.2.a.i. Each electoral board must establish a voting systems Configuration Management Database.

C.2.a.ii. All voting systems components (i.e., hardware, firmware, software, and documentation) that are uniquely identifiable and for which the local jurisdiction is accountable must be entered into the Configuration Management Database.

C.2.a.iii. All modifications (e.g., firmware or software updates or "patches", hardware changes) must be recorded in the Configuration Management Database along with, the identities of the person making the modification and the person approving the modification.

C.2.a.iv. Only the electoral board may approve the modification of a voting equipment or system component.

C.2.a.v. NO modification (e.g., firmware or software updates or "patches", hardware changes) is to be made to any voting equipment or systems component that has NOT been certified or approved by the State Board of Elections.

C.2.a.vi. NO modification (e.g., firmware or software updates or "patches", hardware changes) is to be made to any voting equipment or systems component subsequent to the equipment or systems being tested and certified for in an Election, on Election Day or from Election Day until the fifteenth (15^{th}) day after certification of election results.

C.2.a.vii. All movements of voting systems components outside the local jurisdiction (e.g., to a vendor for setup, modification or repair; to another jurisdiction as a "loaner") must be recorded in the Configuration Management Database along with, the identities of the person receiving the component and the person approving the movement. Likewise, return of the voting systems components must be recorded in the Configuration Management Database.

C.2.a.viii. Only the electoral board may approve the movement of a voting system component outside the local jurisdiction.

C.2.a.ix. Before a voting system or any of its components are transferred to another local jurisdiction within the Commonwealth, traded-in with a voting systems vendor, have a hard drive replaced, or replace memory media, all sensitive information present on any storage device (e.g., "ballot station" hard drive, floppy disk, AVC Edge solid state memory) or memory media (e.g., iVotronic PEB cartridge, AVC Edge Smart Card) must be completely erased or otherwise made unreadable unless there is

specific intent on the part of the electoral board to transfer the particular information to the recipient of the voting system or system component.

C.2.a.x. Before a voting system is declared surplus or are disposed of, all components of the system must be rendered unusable.

C.2.a.xi. Whenever licensed software is resident on any voting system storage device or memory media being declared surplus, transferred to another local jurisdiction within the Commonwealth, traded- in with a voting systems vendor, disposed of, the hard drive is replaced, or memory media is replaced, the terms of the license agreement must be followed.

C.2.a.xii. After the removal of sensitive data from the storage or memory media is complete, the electoral board must document that all sensitive data has been removed from the voting system and/or its components.

C.2.a.xiii. All problems associated with the storage (e.g., vandalism, tampering, left unsecured, experienced water damage, theft, Etc.), movement (e.g., left unattended, dropped, theft, Etc.), or operation (e.g., vandalism, tampering, failure to function as required, Etc.) must be recorded in the Configuration Management Database along with, the identity of the person recording the problem.

C.2.a.xiv. Each electoral board must review their voting systems Configuration Management Database before, no earlier than 3 days prior, and after, no later than 3 days following, each election for currency and accuracy.

C.2.a.xv. An electoral board or third-party review of each local jurisdiction's voting systems Configuration Management Database must be conducted no less frequently than once every two years.

C.3. Testing

The purpose of testing is to implement technology and procedures that demonstrate and confirm to the greatest extend possible that the voting systems in use within a local jurisdiction are identical to the voting systems certified by the State Board of Elections. Acceptance Testing is conducted when voting systems are initially received from a vendor or other outside source (e.g., another local jurisdiction). Logic and Accuracy Testing is conducted before each election.

C.3.a. Standards

C.3.a.i. Acceptance and Logic and Accuracy Tests must be structured and planned so that the complete functionality of all voting equipment and system components is tested.

C.3.a.ii. Before the electoral board can place a voting system into operation, it must successfully pass Acceptance Testing.

C.3.a.iii. Before and after each election, the complete functionality of all voting equipment and system components must be tested.

C.3.a.iv. Vendor personnel must NOT conduct Acceptance or Logic and Accuracy Testing. Vendor personnel may be present during testing to assist other elections personnel conduct testing.

C.4. Network Security

The purpose of network security is to implement technology and procedures that guard against unauthorized access to voting systems through an electronic communications network (e.g., dial-up, LAN, WAN, Internet, Etc.).

C.4.a. Standards

C.4.a.i. NO voting system component may be connected to an electronic communications network (e.g., dial-up, LAN, WAN, Internet, Etc.) without the explicit approval in writing from the Secretary of the State Board of Elections. Such a request should describe in detail the technical security mechanisms that the electoral board will put in place to ensure the confidentiality, integrity, and availability of the voting system components being connected to the network.

C.4.a.ii. For those voting systems with a wireless LAN capability, the wireless feature may be used to set up voting equipment for delivery to the precincts while in a “warehouse” setting. The wireless feature may also be used briefly to open and close the polls. The wireless feature must be turned off while the polls are open.

Glossary

Acceptance Testing - The purpose of acceptance testing is to demonstrate and confirm to the greatest extent possible that the voting systems purchased or leased by a local jurisdiction are identical to the voting systems certified by the State Board of Elections and that the voting systems equipment and software is fully functional and capable of satisfying the administrative and statutory requirements of the local jurisdiction. Acceptance testing is conducted when voting systems are initially received by the local electoral board from a vendor or other outside source (e.g., another local jurisdiction).

Access Control - The purpose of access control is to implement technology and procedures that control access to voting systems only to those persons and software authorized by the Chairman of the electoral board and/or the general registrar. The entire subject of voting systems security is based upon access control, without which voting systems security cannot, by definition, exist.

Access Management - The purpose of access management is to ensure that access to voting systems is consistent with the applicable requirements of Federal and to Commonwealth statutes, State Board of Elections policy and standards, and local electoral board procedures.

Administrative Safeguards - Those standards, procedures, and actions taken to manage the selection, development, implementation, and maintenance of security measures to protect voting systems and to manage the conduct of elections personnel in relation to the protection of voting systems.

Alteration - Any physical intrusion into voting system hardware or installation of non-certified software.

Reviewable – Voting Systems Security Program related documentation is easy to access, easy to understand, and easy to reference.

Authentication - Authentication refers to the verification of the authenticity of a person's identity. Authentication techniques usually form the basis for all forms of access control to voting systems.

Authorization - The process whereby the Chairman of the electoral board or general registrar approves a specific action or approves the granting of access to voting system components for a specific individual.

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

Availability - Ensuring that voting systems and the necessary supporting components are available for use when they are needed.

Best Practice - A management or technical policy, standard, guideline, procedure or practice that has consistently been shown to improve the

security of information technology resources.

Certification Testing - The purpose of certification testing is to verify that the design and performance of the voting system being tested comply with all of the requirements of the *Code of Virginia*. Certification testing is not intended to exhaustively test all of the voting system hardware and software attributes; these are evaluated during qualification testing. However, all voting system functions, that are essential to the conduct of an election, are evaluated.

Configuration Management - The purpose of configuration management is to implement technology and procedures that control the hardware, firmware, software, and documentation configurations of voting systems so that only those hardware, firmware, and software components that have been qualified by Independent Testing Agencies and certified by the Commonwealth become part of a local jurisdiction's voting systems configurations.

Configuration Management Database - An electronic or non-electronic permanent record of all required configuration management data associated with all voting system components for which a local jurisdiction is accountable.

Confidentiality - Assurance that information is shared only among authorized persons or organizations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc. The classification of the information should determine is confidentiality and hence the appropriate safeguards.

Control (CM) - The management of each voting systems component, specifying who is authorized to "change" (e.g., modify, move) it and whose approval is required for the "change".

Elections Personnel - All personnel employed or appointed/designated to support the testing, preparation, operation, movement, or storage of voting systems.

Environmental Controls - The purpose of environmental controls is to define the procedures and physical safeguards to secure the physical environment in which voting systems must operate and are stored.

House - To place voting systems in a facility when in use.

Identification (CM) - The specification and identification of all voting system components and their inclusion in a Configuration Management Database.

Independent Testing Authority - Companies selected by the National Association of State Election Directors (NASED) or the National Institute of Standards and Technology (NIST) to conduct qualification testing of voting systems.

Integrity - Assurance that voting system components are authentic and complete.

LAN (Local Area Network) - A computer network that covers a relatively small area. Most LANs are kept to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

Logic and Accuracy Testing - The purpose of logic and accuracy testing is to demonstrate and confirm to the greatest extent possible that the voting systems in use within a local jurisdiction are identical to the voting systems certified by the State Board of Elections and accepted by the local electoral board. Logic and accuracy testing is conducted before and after each election.

Network Security - The purpose of network security is to implement technology and procedures that guard against unauthorized access to voting systems through an electronic communications network (e.g., dial-up, LAN, WAN, Internet, Etc.).

Physical Access Controls - The purpose of physical access controls is to define the procedures and physical safeguards to control physical access to voting systems and the facility or facilities in which they are housed, while ensuring that properly authorized personnel are allowed access.

Physical Safeguards - Those standards, procedures, and actions taken to protect voting systems and related facilities and equipment, from natural and environmental hazards, as well as, tampering, vandalism, and theft.

Qualification Testing - The purpose of qualification testing is to demonstrate that the voting system complies with the requirements of its own design specifications. This testing encompass selective in-depth examination of software; inspection and evaluation of voting system documentation; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; and tests to verify system performance and function under normal and abnormal operating conditions. Qualification testing is normally conducted by an Independent Testing Authority (ITA).

Security Awareness and Training - The purpose of security awareness and training is to promote Elections Personnel awareness, training and responsibility with respect to security risks, policy, standards, guidelines, and procedures related to the protection of voting systems.

Security Breach - Any event or action that compromises the security, confidentiality, integrity or availability of voting systems and the elections process they support.

Security Contingency Planning - The purpose of security contingency planning to provide for the continued security of voting systems in the event of a disruption in the normal operational environment caused by a voting systems security policy, standard, or procedure having been violated and/or a security safeguard having been breached. A secondary purpose of security contingency planning is to minimize the effect of such disruptions.

Security Incident - Any act or circumstance involving classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security Incident Handling - The purpose of security incident handling is to respond to a suspected or known instance where voting systems security policy, standards, and procedures have been violated and/or a security safeguard has been breached.

Security Monitoring and Review Control - The purpose of security monitoring and review control is to ensure that the implementation and maintenance of security safeguards are adequately documented and managed and that accountability can be established.

Security Risk Assessment - The purpose of security risk assessment is to identify and evaluate the risks to which a local jurisdiction's voting systems are exposed.

Status (CM) - The management of each voting systems component, specifying who is authorized to "change" (e.g., modify, move) it and whose approval is required for the "change".

Store – To place voting systems in a facility when not in use.

Technical Safeguards - The technology and the standards and procedures for its use that protect voting systems and control access to them.

Testing - The purpose of testing is to implement technology and procedures that demonstrate and confirm to the greatest extend possible that the voting systems in use within a local jurisdiction are identical to the voting systems certified by the State Board of Elections. Acceptance Testing is conducted when voting systems are initially received from a vendor or other outside source (e.g., another local jurisdiction). Logic and Accuracy Testing is conducted before and after each election.

Third-party - A party other than an electoral board member or another election official, such as a County or City auditor or a private contractor, providing independent assessment or review services.

Verification (CM) - The local review and/or third-party review to ensure that the information contained in a Configuration Management Database is accurate.

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; and the 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; to determine specific system changes to be made a system

after the initial qualification of the system; and make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

WAN (Wide Area Network) - A communications network that covers a wide geographic area, such as a city, county or state. It usually consists of several LANs.

Notes