

COMMONWEALTH OF VIRGINIA



Voting Systems Management Self-Assessment Guide

VOTING SYSTEMS SECURITY SELF-ASSESSMENT GUIDE

State Board of Elections

Preface

Publication Designation

COV VSM Self-Assessment Guide
SEC2005-01.1

(Information Technology Security
Standard)

Subject

Voting Systems Security

Scope

This self-assessment guide 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.

Effective Date

January 17, 2005

Supersedes

Does not supersede any guideline.

Purpose

This self-assessment guide is published as a complementary document to the Voting Systems Security Policy (i.e., COV VSM Policy SEC2005-01) and the Voting Systems Security Standard (i.e., COV VSM Standard SEC2005-01.1). As such, it provides a mechanism for assessing a local jurisdiction's compliance with the requirements of the Commonwealth's voting systems security policy and standard. Accordingly, this security self-assessment guide should be considered:

Scheduled Review

One (1) year from effective date

1. To further assist and strengthen an electoral board's implementation of its Voting Systems Security Program.
2. To further facilitate an electoral board or third-party review of voting systems security safeguards.
3. To further facilitate an electoral board or third-party review of the local jurisdiction's compliance with Commonwealth voting systems security policy and standard.

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 Guideline SEC2001-01.1
(Information Technology Security
Guideline)

COV ITRM Standard SEC2003-02.1

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 Standard SEC2005-01.1, Voting Systems Security Standards; Dated January 17, 2005

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

Table of Contents

Preface.....	ii
Definitions	iii
Related COV VSM Policies, Standards, and Guidelines.....	iii
Introduction.....	5
Questionnaire Structure	6
Questionnaire Control	6
Background Information	7
Date of Current Security Assessment and of the Most Recent Security Assessment	7
Electoral Board Chairman and Members Names, Addresses, and Telephone Numbers	7
General Registrar Name, Address, and Telephone Number	7
Assessors Names, Titles, Addresses, Telephone Numbers, and Organization.....	7
Purpose and Objectives of Assessment	7
Makes, Models, Numbers of Voting Systems In Use.....	7
Vendor Information	8
Voting Systems Storage Locations.....	8
Voting Systems Precinct Locations.....	8
Questions	8
Applicability of Questions	10
Using the Completed Questionnaire	10
Questionnaire Analysis	10
Action Plans	10
Reviews.....	11
Glossary	12

Introduction

Adequate security of voting systems is a fundamental management of each County and City electoral board. Electoral board members must understand the current status of their Voting Systems Security Program and security safeguards in order to make informed judgments and investments that appropriately mitigate risks to the security of voting systems to a reasonable and appropriate acceptable level.

Self-assessments provide a method for electoral boards to determine the current status of their Voting Systems Security Programs and, where necessary, identify targets for improvement. This self-assessment guide makes use of a comprehensive questionnaire containing specific questions that, along with their responses, can be used to determine a local jurisdiction's compliance with COV VSM Policy SEC2005-01, *Voting Systems Security Policy* and COV VSM Standard SEC2005-01.1, *Voting Systems Security Standard*. The guide does not establish any new security requirements. The questions are abstracted directly from the Commonwealth voting systems security policy and standard.

This document builds on the Voting Systems Security Framework defined in COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards*. The Voting Systems Security Framework established the foundation for standardizing on three types of security safeguards that electoral boards could use to protect the voting systems for which they are accountable. This document provides guidance on assessing the local jurisdiction's compliance with the requirements of the 12 security components spanning the three security safeguard types.

The self-assessment questionnaire (Attachment A) can be used for the following purposes:

- Electoral boards that know their jurisdiction's voting systems and security safeguards can quickly gain a general understanding of any security improvements needed to achieve compliance with COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards*.
- The compliance with COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards* can be thoroughly evaluated using the self-assessment questionnaire as a guide. The results of such a thorough review produce a reliable measure of the effectiveness of the security safeguards put in place by the electoral board and may be used to: fulfill reporting requirements, identify resources needed to improve the local jurisdiction's level of security standards compliance, and to prepare for internal and external reviews.

It is important to note that the questionnaire is not intended to be an all-inclusive list of security safeguards and related techniques. It is intended only to assess an electoral board's compliance with COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards*. Electoral boards should obtain information on such additional security safeguards from other sources, such as vendors, and use that information to supplement this guide.

Consistent with COV VSM Policy SEC2005-01, *Voting Systems Security Policy*, each electoral board must implement and maintain a Voting Systems Security Program to adequately secure its voting system assets. An electoral board's Voting Systems Security Program must assure that its voting systems operate effectively and provide appropriate confidentiality, integrity, and availability; and that they are protected commensurate with the level of risk and magnitude of harm resulting from their loss, misuse, unauthorized access, or modification. Performing a self-assessment and mitigating any of the weaknesses found in the assessment is one way to determine if their voting systems are adequately protected.

Questionnaire Structure

The Voting Systems Security Self-Assessment Questionnaire (Attachment A) contains three sections: cover sheet, questions, and notes. The questionnaire begins with a cover sheet requiring descriptive information about the local jurisdiction, the electoral board, the general registrar, the assessors, the purpose and objectives of the assessment, the types of voting systems in use, vendor information, and the locations where the voting systems are stored and used.

The questionnaire may be customized. An electoral board can add questions or require more descriptive information. The questionnaire must not have questions removed or questions modified.

After each question, there is a "Yes" field, a "No" field, an evidence field, a comment field, and an initial field. The "Yes" field is used to indicate a positive response to the content of the question. The "No" field is used to indicate a negative response to the content of the question. The evidence field is used to note the reference to supporting documentation that can be attached to the questionnaire or is obtainable. The evidence field is also used to describe the types of the security safeguards implemented by the electoral board. The evidence field is used primarily to support a "check" in the "Yes" field. The comment field is used to note any observations concerning the effectiveness of the implemented security safeguards, as well as, any observations concerning deficiencies in voting systems security and recommended mitigation. The comment field is used to support "checks" in either the "Yes" field or the "No" field. The initial field is used to identify the assessor developing the response to the question. At the end of each set of questions, there is an area provided for notes. This area should be used for identifying where in the electoral board's Voting Systems Security Program changes should be made. It should also be used to document the justification as to why a particular security standard is not being implemented fully or why it is being implemented more rigorously. The notes section should be used to provide a summary of findings for that particular section of the questionnaire.

Questionnaire Control

All completed self-assessment questionnaires should be marked, handled, and controlled at the level of sensitivity determined by the Secretary of the State Board of Elections. It should be noted that the information contained in a completed self-assessment questionnaire could easily depict where the local jurisdiction's voting systems are most vulnerable.

Background Information

Date of Current Security Assessment and of the Most Recent Security Assessment

The background information pages of the self-assessment questionnaire begin with the start date of this security assessment and the completion date of the most recent security assessment using the COV VSM Self Assessment Guide SEC2005-01.1, *Self-Assessment Questionnaire*. The length of time required to complete an assessment will vary. The time and resources needed to complete an assessment will vary depending on the size and complexity of the local jurisdiction and the accessibility of personnel and information.

Electoral Board Chairman and Members Names, Addresses, and Telephone Numbers

The next entries in the background information section of the questionnaire identify the names, addresses, and telephone numbers of the electoral board chairman and members. The documentation of this information is so that electoral board members may be contacted should there be any questions during the completion of the questionnaire or during a subsequent review of the completed questionnaire.

General Registrar Name, Address, and Telephone Number

The next entry in the background information section of the questionnaire identifies the name, address, and telephone number of the general registrar. The documentation of this information is so that the general registrar may be contacted should there be any questions during the completion of the questionnaire or during a subsequent review of the completed questionnaire.

Assessors Names, Titles, Addresses, Telephone Numbers, and Organization

The next entries in the background information section of the questionnaire identify the names, titles, addresses, telephone numbers, and organizations of the members of the assessment team. The documentation of this information is so that assessment team members can be contacted should there be any questions during the completion of the questionnaire or during a subsequent review of the completed questionnaire.

Purpose and Objectives of Assessment

The purpose and objectives of the security risk assessment should be identified. For example, the assessment is intended to be a thorough and reliable evaluation of voting systems security safeguards for purposes of developing a Voting Systems Security Program.

Makes, Models, Numbers of Voting Systems In Use

The makes, models, and numbers of voting systems in use by the local jurisdiction should be listed in the background information section of the questionnaire. This information will help

orient both the assessors in their completion of the questionnaire and any subsequent reviewer of the completed questionnaire.

Vendor Information

The name, address, and telephone number of the voting system vendor's local representative, as well as, the vendor's company name, address, and telephone number should be provided as part of the background information contained in the questionnaire. The documentation of this information is so that the vendor's local representative or the vendor's corporate headquarters can be contacted should there be any questions during the completion of the questionnaire or during a subsequent review of the completed questionnaire.

Voting Systems Storage Locations

The addresses, points of contact, and telephone numbers of each point of contact should be provided as part of the background information contained in the questionnaire. The documentation of this information is so that the assessors can plan any visits to these locations and so that the point of contact can be contacted should there be any questions during the completion of the questionnaire or during a subsequent review of the completed questionnaire.

Voting Systems Precinct Locations

The addresses, points of contact, and telephone numbers of each precinct location where voting systems are used should be provided as part of the background information contained in the questionnaire. The documentation of this information is so that the assessors can plan any visits to these locations and so that the point of contact can be contacted should there be any questions during the completion of the questionnaire or during a subsequent review of the completed questionnaire.

Questions

The questions contained in the self-assessment questionnaire are separated into three sections: administrative security safeguards, physical security safeguards, and technical security safeguards. The division of the questionnaire in this manner reflects the categorization of voting systems security safeguards contained in COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards*. This reference should be used to obtain additional detail for any of the questions listed in the questionnaire.

The questions portion of this document easily map to the COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards* since the sections in both documents are organized according to the same security safeguard types, i.e., administrative, physical, and technical.

Within each of the three security safeguard types, there are a number of security components; for example, security risk assessment, security awareness and training, and security monitoring and review control are security components found under the administrative security safeguard type. There are a total of twelve security components contained in the questionnaire; each security component is integral to an effective Voting Systems Security Program.

The three security safeguard types and twelve security components comprise the Voting Systems Security Framework, endorsed by the State Board of Elections.

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

The method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the security safeguards. The review, for example, should consist of testing the physical access control methods in place by attempting to gain access during non-work hours. Supporting documentation describing what has been tested and the results of the tests add value to the assessment and will make the next assessment of the voting systems security easier.

Once the questionnaire, including all references, is completed for the first time, future assessments will require considerably less effort. The completed questionnaire will establish a baseline. If this year's assessment indicates that most of the security standards are being met, then that would be the starting point for the next assessment. More time can be spent identifying ways to improve the level of overall compliance instead of having to gather all the initial information again. Use the evidence section to list whether there is supporting documentation and the notes section for any lengthy explanations.

The assessment techniques to test the implementation or effectiveness of each security component are beyond the scope of this document.

When answering the questions about whether the requirements of a specific standard have been met, consider both the operational and technical environments of the local jurisdiction. There

may be certain situations where an electoral board will chose not to comply with a particular requirement because compensating security safeguards exists or because the benefits of operating without the safeguard (at least temporarily) outweigh the risk of waiting for full compliance. Alternatively, there may be times when an electoral board decides to implement more stringent safeguards than generally applied elsewhere. When, either of the above circumstances exist, note the reason in the comment field of the questionnaire. Additionally, the electoral board's Voting Systems Security Program documentation should contain supporting documentation as to why the particular security standard has or has not been implemented.

Applicability of Questions

If a question does not reasonably apply in the local jurisdiction's operational or technical environments, then a "non-applicable" or "N/A" should be entered in the comment field next to the question.

Using the Completed Questionnaire

The completed self-assessment questionnaire can be used for two purposes. First it can be used by an electoral board that know their jurisdiction's voting systems and security safeguards to quickly gain a general understanding of any security improvements needed to achieve compliance with COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards*. Second, it can be used as a guide for thoroughly evaluating the local jurisdiction's compliance with COV VSM Standard SEC2005-01.1, *Voting Systems Security Standards*. The results of such thorough reviews provide a much more reliable measure of the effectiveness of the security safeguards put in place by the electoral board and may be used to: fulfill reporting requirements; identify resources needed to improve the local jurisdiction's level of security standards compliance, and to prepare for internal and external reviews.

Questionnaire Analysis

Because this is a self-assessment, ideally the individuals assessing the electoral board's Voting Systems Security Program are responsible for administering the program. The same individuals who completed the assessment can conduct the analysis of the completed questionnaire. By being familiar with the electoral board's Voting Systems Security Program, the supporting documentation, and the results of the assessment, the next step that the assessor takes is an analysis, which summarizes the findings. A centralized group, such as local jurisdiction's Internal Auditor, can also conduct the analysis as long as the supporting documentation is sufficient. The results of the analysis should be placed in an action plan, and the electoral board's Voting Systems Security Program should be created or updated to reflect each security safeguard implementation/improvement decision.

Action Plans

How the security safeguards are to be implemented/improved, i.e., specific procedures written, equipment installed and tested, and personnel trained, should be documented in an action plan. The

action plan must contain projected dates, an allocation of resources, and follow-up reviews to ensure that remedial actions have been effective. Routine reports should be submitted to senior management on weaknesses identified, the status of the action plans, and the resources needed.

Reviews

A full, annual review of COV VSM Self-Assessment Guide SEC2005-01.1 is anticipated.

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.

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 its 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 (NASSED) or the National Institute of Standards and Technology (NIST) to conduct qualification testing for voting systems."

Information 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 system 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 system 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.

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 encompasses 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. An Independent Testing Authority (ITA) normally conducts qualification testing.

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 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.

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 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. 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 audit 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.

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Table of Contents – Attachment A

Table of Contents – Attachment A.....	2
Background Information	3
A. Administrative Security Safeguards.....	5
A.1. Security Risk Assessment.....	5
A.2. Security Awareness and Training.....	9
A.3. Security Incident Handling.....	14
A.4. Security Monitoring and Review Control.....	18
A.5. Security Contingency Planning	22
A.6. Access Management	26
B. Physical Security Safeguards.....	30
B.1. Physical Access Controls.....	30
B.2. Environmental Controls	34
C. Technical Security Safeguards	37
C.1. Technical Access Controls.....	37
C.2. Configuration Management	40
C.3. Testing.....	49
C.4. Network Security	51

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Background Information

Date of Current Security Assessment: _____ **Date of Most Recent Security Assessment:** _____

Local Jurisdiction Name: _____

Electoral Board Chairman Name, Address, and Telephone Number: _____

Electoral Board Members Names, Addresses, and Telephone Numbers:

General Registrar Name, Address, and Telephone Number: _____

Assessors Names, Title, Addresses, Telephone Numbers, and Organizations: _____

Purpose and Objectives of Assessment:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Makes, Models, and Numbers of Voting Systems In Use: _____

Vendor Information (company name, address, telephone number; local representative's name, address, telephone number): _____

Voting Systems Storage Locations Addresses, Points of Contact, and Telephone Numbers: _____

Voting Systems Precinct Locations Addresses, Points of Contact, and Telephone Numbers: _____

A. Administrative Security Safeguards

Administrative security safeguards refer to those 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. 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.

Standard	Yes	No	Evidence	Comments	Initials
A. Administrative Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
A.1. Security Risk Assessment					
A.1.a.i. Has the electoral board developed, documented and implemented a Voting Systems Security Program?					
A.1.a.i. Does the electoral board maintain its Voting Systems Security Program?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.1.a.i. Is the Voting Systems Security Program appropriate to its technical and operational environment?					
A.1.a.ii. Does Voting System Security Program documentation specify how exceptions to mandatory security standards are to be determined, approved, and documented?					
A.1.a.iii. Has the electoral board conducted a security risk assessment in order to identify the potential security risks to the voting systems for which they are accountable?					
A.1.a.iii. Has the electoral board determined the appropriate security safeguards necessary to protect its voting systems?					
A.1.a.iii. Has the electoral board implemented the security safeguards necessary to protect its voting systems?					
A.1.a.iv. Has the electoral board reviewed and updated its security risk assessment on an as necessary basis?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.1.a.iv. Has the electoral board formally reviewed and updated its security risk assessment within the past two years?					
A.1.a.iv. Has the electoral board formally reviewed and updated its security risk assessment not later than 90 days prior to each general/federal election?					
A.1.a.v. Does the electoral board's Voting Systems Security Program 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. Does the electoral board review changes in the local jurisdiction's technical and operational environments for security implications?					
A.1.a.vi. Does the electoral board then review and assess any risks and implement appropriate security safeguards?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.1.a.vi. Has the electoral board documented its review and assessment of the changes in the local jurisdiction's technical and operational environments for security implications in a format that can be easily reviewed?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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. 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. 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. 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.

Standard	Yes	No	Evidence	Comments	Initials
A. Administrative Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
A.2. Security Awareness and Training					
A.2.a.i. Has the electoral board developed, documented a Voting Systems Security Awareness and Training Program?					
A.2.a.i. Does the electoral board maintain the currency of its Voting Systems Security Awareness and Training Program?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.2.a.i. Does the electoral board's Voting Systems Security Awareness and Training Program inform elections personnel of their security responsibilities and know how they are expected to fulfill them?					
A.2.a.i. Is voting systems security awareness training provided to ALL elections personnel?					
A.2.a.ii. Do ALL elections personnel have easy access to all relevant security policy, standards, and procedures and security awareness and training instructional materials?					
A.2.a.iii. Has the local jurisdiction's Voting Systems Security Awareness and Training Program been approved by the electoral board?					
A.2.a.iii. Has the electoral board specified the timeframes for receiving initial and periodic, refresher security training? What are they?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.2.a.iii. Does the local jurisdiction's Voting Systems Security Awareness and Training Program provide both general and position specific security training content?					
A.2.a.iii. Does the local jurisdiction's Voting Systems Security Awareness and Training Program define a security awareness/reminder program?					
A.2.a.iii. Is the local jurisdiction's Voting Systems Security Awareness and Training Program documented in a format that can be easily reviewed?					
A.2.a.iii. Has the electoral board formally reviewed and updated its Voting Systems Security Awareness and Training Program within the past two years?					
A.2.a.iii. Has the electoral board formally reviewed and updated its Voting Systems Security Awareness and Training Program not later than 60 days prior to each general/federal election?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.2.a.iv. Do ALL new elections personnel receive formal security training prior to assuming their duties?					
A.2.a.v. Does the local jurisdiction document the date and time each individual receives security training?					
A.2.a.v. Does each individual provide written acknowledgement that they have received and understand the security training?					
A.2.a.v. Is this written acknowledgement maintained as part of the local jurisdiction's Voting Systems Security Awareness and Training Program documentation?					
A.2.a.vi. Does the local jurisdiction provide periodic, refresher security training to ALL elections personnel on at least an annual basis?					
A.2.a.vi. Does the local jurisdiction provide periodic, refresher security training to ALL elections personnel not later than 30 days prior to each general/federal election?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.2.a.vii. Are security awareness reminders provided to ALL elections personnel not later than 30 days prior to each election?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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. 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).

Standard	Yes	No	Evidence	Comments	Initials
A. Administrative Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
A.3. Security Incident Handling					
A.3.a.i. Has the electoral board developed a Security Incident Response and Reporting Procedure for security incidents involving voting systems?					
A.3.a.i. Does the Security Incident Response and Reporting Procedure identify the responsibilities and actions to be taken in response to security incidents involving voting systems?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.3.a.ii. Has the local jurisdiction's Security Incident Response and Reporting Procedure been approved by the electoral board?					
A.3.a.ii. Does the local jurisdiction's Security Incident Response and Reporting Procedure identify the general types of incidents that must be reported?					
A.3.a.ii. Does the local jurisdiction's Security Incident Response and Reporting Procedure identify who is responsible for reporting security incidents?					
A.3.a.ii. Does the local jurisdiction's Security Incident Response and Reporting Procedure prescribe the mechanisms for reporting security incidents?					
A.3.a.ii. Does the local jurisdiction's Security Incident Response and Reporting Procedure identify those officials who must receive notification of security incidents?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.3.a.ii. Does the local jurisdiction's Security Incident Response and Reporting Procedure require the documentation of actions taken in response to security incidents?					
A.3.a.ii. Does the local jurisdiction's Security Incident Response and Reporting Procedure require the production of an after action report focused on preventing a recurrence of the security incident?					
A.3.a.ii. Is the local jurisdiction's Security Incident Response and Reporting Procedure documented in a format that can be easily reviewed?					
A.3.a.ii. Has the electoral board formally reviewed and revised its Security Incident Response and Reporting Procedure within the past two years?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.3.a.ii. Has the electoral board formally reviewed and revised its Security Incident Response and Reporting Procedure not less than 60 days prior to a general/federal election?					

NOTES:

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. 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 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.

Standard	Yes	No	Evidence	Comments	Initials
A. Administrative Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
A.4. Security Monitoring and Review Control					
A.4.a.i. (1). Does the electoral board monitor and audit all activities associated with the purchase of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.4.a.i. (2). Does the electoral board monitor and audit all activities associated with the testing of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					
A.4.a.i. (3). Does the electoral board monitor and audit all activities associated with the configuration of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					
A.4.a.i. (4). Does the electoral board monitor and audit all activities associated with the storage of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.4.a.i. (5). Does the electoral board monitor and audit all activities associated with the transport of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					
A.4.a.i. (6). Does the electoral board monitor and audit all activities associated with the preparation of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					
A.4.a.i. (7). Does the electoral board monitor and audit all activities associated with the maintenance of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.4.a.i. (8). Does the electoral board monitor and audit all activities associated with the operation of voting systems, to ensure compliance and accountability with the applicable security statutes, policies, standards, and procedures?					
A.4.a.ii. During general/federal election years, is a formal electoral board or third-party security review conducted at least 90 days prior to the general/federal election?					
A.4.a.ii. During non-general/federal election years, is a formal electoral board or third-party security review conducted at least annually?					
A.4.a.iii. Are all formal electoral board and third-party security reviews fully documented in a format that is easily reviewed?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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.

Standard	Yes	No	Evidence	Comments	Initials
A. Administrative Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
A.5. Security Contingency Planning					
A.5.a.i. Has the electoral board developed a Security Contingency Plan (SCP) for the voting systems for which they are accountable?					
A.5.a.i. Does the electoral board maintain its Security Contingency Plan (SCP)?					
A.5.a.ii. Has the electoral board documented its Security Contingency Plan (SCP)?					
A.5.a.ii. Does the electoral board test its Security Contingency Plan (SCP) annually?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.5.a.iii. Does the Security Contingency Plan (SCP) contain emergency response procedures appropriate to any incident or activity that may threaten the security or integrity of the local jurisdiction's voting systems?					
A.5.a.iv. Does the local jurisdiction's Security Contingency Plan include a general description of the chain-of command and the decision-making process that will be followed when executing the contingency plan?					
A.5.a.iv. Does the local jurisdiction's Security Contingency Plan include 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?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.5.a.iv. Does the local jurisdiction's Security Contingency Plan include procedures and responsibilities to facilitate the rapid restoration of normal security conditions at the primary location, or if necessary, at an alternate location, following the destruction, major damage or other interruption at the primary location?					
A.5.a.iv. Does the local jurisdiction's Security Contingency Plan include a minimally acceptable, prioritized level of security safeguards for voting systems to guide the relocation of equipment and systems to an alternate location?					
A.5.a.iv. Does the local jurisdiction's Security Contingency Plan include 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. Is the local jurisdiction's Security Contingency Plan fully documented?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

<p>A.5.a.v. Is the local jurisdiction's Security Contingency Plan operationally tested at a frequency commensurate with the risk and the magnitude of loss or harm that could result from a disruption in the local jurisdiction's security safeguards for its voting systems?</p>					
<p>A.5.a.vi. Do poll worker training and instructional materials include a description of their responsibilities and authorities relative to the execution of the local jurisdiction's Security Contingency Plan?</p>					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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 to Commonwealth statutes, State Board of Elections policy and standards, and local electoral board procedures.

Standard	Yes	No	Evidence	Comments	Initials
A. Administrative Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
A.6. Access Management					
A.6.a.i. Is the electoral board the only entity that grants/approves access to voting systems?					
A.6.a.ii. Do personnel other than those granted access by the electoral board have access to voting systems?					
A.6.a.iii. Does the electoral board grant access based on identity (by name), based on role (by job description), based on location (by local jurisdiction) or some combination thereof?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.6.a.iii. Does the electoral board define the access granted in terms of the level of access, duration and type (i.e., unaccompanied or accompanied) of the individual's access?					
A.6.a.iv. Does the electoral board document the granting of access to voting systems in writing?					
A.6.a.iv. Does the electoral board's documentation of its granting of access to voting systems to an individual include the name, title, organization, work address, office telephone number, of the person being granted access/control?					
A.6.a.iv. Does the electoral board's documentation of its granting of access to voting systems to an individual include the reason for granting access/control?					
A.6.a.iv. Does the electoral board's documentation of its granting of access to voting systems to an individual include the level of access?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
A.6.a.iv. Does the electoral board's documentation of its granting of access to voting systems to an individual include the date access is to be granted?					
A.6.a.iv. Does the electoral board's documentation of its granting of access to voting systems to an individual include the date access is to end?					
A.6.a.iv. Does the electoral board's documentation of its granting of access to voting systems to an individual include the name, title, organization, address, and telephone number of the person granting access?					
A.6.a.v. Does each person granted access to voting systems for an appreciable length of time or of a recurring nature receive formal security training prior to gaining access?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

<p>A.6.a.vi. Has the electoral board established an authentication mechanism (e.g., identification badge, authorization letter) that can be used to verify the identity of those accessing voting systems?</p>					
<p>A.6.a.vii. Does the electoral board review and update the list of individuals granted access to voting systems on at least an annual basis?</p>					
<p>A.6.a.vii. Does the electoral board review and update the list of individuals granted access to voting systems at least 60 days, 30 days and 3 days prior to each general/federal election?</p>					
<p>A.6.a.viii. Is the electoral board's list of personnel granted access to voting systems documented in a format that can be easily reviewed?</p>					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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). 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, while ensuring that personnel granted access by the electoral board are allowed access.

Standard	Yes	No	Evidence	Comments	Initials
B. Physical Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
B.1. Physical Access Controls					
B.1.a.i. Is/are the facility or facilities where voting systems are stored secured?					
B.1.a.i. Is access to the facility or facilities where voting systems are stored restricted to authorized personnel only?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
B.1.a.ii. Has the electoral board implemented a method of monitoring and reviewing physical access to voting systems storage locations (e.g. identification badges, keycards, access logs, Etc.)?					
B.1.a.iii. Does the electoral board regularly review the list of persons gaining access to voting systems?					
B.1.a.iv. Do voting systems remain in the physical custody of authorized personnel at all times while being moved or relocated?					
B.1.a.v. Is the identity and access authorization of all visitors, vendors, maintenance personnel, etc. authenticated prior to gaining physical access to voting systems?					
B.1.a.v. Are access lists, preplanned appointments and identification checks used as part of the authentication process?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
B.1.a.vi. Has a method of monitoring and reviewing physical custody of voting systems during transport (e.g. chain-of-custody log, hand receipts, truck seals) been implemented?					
B.1.a.vii. Does the electoral board have plans in place to ensure the physical security of voting systems in the event of an emergency or crisis?					
B.1.a.viii. Does the electoral board have plans in place to immediately notify the general registrar, chairman of the electoral board and the Secretary of the State Board of Elections in the event of an emergency or crisis that threatens the physical security of voting systems?					
B.1.a.ix. Are the physical security procedures and safeguards controlling physical access to voting systems documented?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
B.1.a.ix. Are the physical security procedures and safeguards controlling physical access to the facility or facilities in which voting systems are housed documented?					
B.1.a.x. Are all security related (e.g., walls, doors, locks, cameras, alarm systems, etc.) repairs and modifications to the physical components of a facility, where voting systems are stored, that are security related documented?					
B.1.a.xi. Are any functions that are not directly elections related performed with voting systems?					
B.1.a.xii. Are mandatory physical security safeguards applied to all voting systems?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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.

Standard	Yes	No	Evidence	Comments	Initials
B. Physical Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
B.2. Environmental Controls					
B.2.a.i. Has the electoral board ensured that appropriate fire suppression and prevention equipment are installed and working in the facility or facilities in which voting systems are housed or stored?					
B.2.a.ii. Does the electoral board periodically inspect the facility or facilities in which voting systems are housed or stored for potential fire ignition sources, such as improperly stored materials in close proximity to voting systems?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
B.2.a.iii. Has the electoral board ensured that environmental controls (e.g., heating, cooling, humidity) in the facility or facilities in which voting systems are housed or stored are adequate to prevent damage to the voting systems?					
B.2.a.iv. Has the electoral board reviewed 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 or stored?					
B.2.a.v. Has the electoral board reviewed the risks to voting systems due to natural disasters, such as tornadoes and flooding?					
B.2.a.v. Has the electoral board developed appropriate risk mitigation strategies to address the risks to voting systems due to natural disasters, such as tornadoes and flooding?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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 Controls

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 electoral board.

Standard	Yes	No	Evidence	Comments	Initials
C. Technical Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
C.1. Technical Access Controls					
C.1.a.i. Are the local jurisdiction's voting systems configured so that they can be remotely accessed?					
C.1.a.ii. For those voting system components that are capable of being password protected, has the electoral board must established criteria for password composition, length and aging?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.1.a.iii. Do all elections personnel having access to voting system components that are password protected, 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, has an automatic logoff feature been implemented?					
C.1.a.iv. For all password protected voting system components that are capable, is a record of all logon attempts being maintained?					
C.1.a.v. Is an individual's password access to voting systems terminated when their employment or contract is terminated?					
C.1.a.v. Is an individual's password access to voting systems terminated when they no longer require access?					
C.1.a.v. Is an individual's password access to voting systems terminated when their access is changed?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.1.a.vi. Has the electoral board established voting systems access procedures for use during emergencies (e.g., fires, natural disasters, bomb threat, civil disturbances)?					

NOTES:

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. 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.

Standard	Yes	No	Evidence	Comments	Initials
C. Technical Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
C.2. Configuration Management					
C.2.a.i. Has the electoral board established a Voting Systems Configuration Management Database?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.ii. Are all voting systems components (i.e., hardware, firmware, software, and documentation) that are uniquely identifiable and entered into the Voting Systems Configuration Management Database?					
C.2.a.iii. Are all modifications (e.g., firmware or software updates or “patches”, hardware changes) to voting systems recorded in the Voting Systems Configuration Management Database?					
C.2.a.iii. Is the identity of the person making a modification to a voting system component recorded in the Voting Systems Configuration Management Database?					
C.2.a.iii. Is the identity of the person approving a modification to a voting system component recorded in the Voting Systems Configuration Management Database?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.iv. Has anyone other than an electoral board member approved the modification of a voting equipment or systems component?					
C.2.a.v. Have any modifications (e.g., firmware or software updates or “patches”, hardware changes) been 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. Have any modifications (e.g., firmware or software updates or “patches”, hardware changes) been made to any voting equipment or systems component on Election Day or from Election Day until the fifteenth (15 th) day after certification of election results?					
C.2.a.vii. Are 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”) recorded in the Voting Systems Configuration Management Database?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.vii. When voting system components are moved outside of the local jurisdiction, is the identity of the person receiving the components recorded in the Voting Systems Configuration Management Database?					
C.2.a.vii. When voting system components are moved outside of the local jurisdiction, is the identity of the person approving the movement of the components recorded in the Voting Systems Configuration Management Database?					
C.2.a.vii. When voting system components have been returned to the local jurisdiction, after having been moved outside of the local jurisdiction, is the fact that the components have been returned recorded in the Voting Systems Configuration Management Database?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.viii. Does anyone other than an electoral board member approve the movement of a system component outside the local jurisdiction?					
C.2.a.ix. Does the electoral board ensure that all sensitive information present on any voting system 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) is completely erased or otherwise made unreadable before a voting system or any of its components are transferred to another local jurisdiction within the Commonwealth?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.ix. Does the electoral board ensure that all sensitive information present on any voting system 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) is completely erased or otherwise made unreadable before a voting system or any of its components are traded-in with a vendor?					
C.2.a.ix. Does the electoral board ensure that all sensitive information present on any voting system component 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) is completely erased or otherwise made unreadable before it is replaced?					
C.2.a.x. Does the electoral board ensure that before a voting system is declared surplus or disposed of, all of its components are rendered unusable?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.xi. Does the electoral board ensure that 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 vendor, disposed of, the hard drive is replaced, or memory media is replaced, the terms of the license agreement are followed?					
C.2.a.xii. In all instances where the electoral board is expected to have ensured that sensitive information has been erased from or otherwise made unreadable on voting system storage devices or memory media, has the electoral board documented their actions?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.xiii. Are 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.) of voting system components recorded in the Configuration Management Database?					
C.2.a.xiii. When problems associated with the storage, movement, or operation of voting system components recorded in the Configuration Management Database, is the identity of the person reporting the problem also recorded?					
C.2.a.xiv. Does the electoral board review its Voting Systems Configuration Management Database for currency and accuracy before, but no earlier than 3 days prior to each election?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.2.a.xiv. Does the electoral board review its Voting Systems Configuration Management Database for currency and accuracy after, but no later than 3 days following each election?					
C.2.a.xv. Has a third-party review of the local jurisdiction's Voting Systems Configuration Management Database been conducted within the past two years?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

C.3. Testing

The purpose of testing is to implement technology and procedures that 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. 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.

Standard	Yes	No	Evidence	Comments	Initials
C. Technical Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
C.3. Testing					
C.3.a.i. Are Acceptance and Logic and Accuracy Tests structured and planned so that the complete functionality of all system components is tested?					
C.3.a.ii. Does the electoral board place voting systems into operation before they have successfully completed Acceptance Testing?					
C.3.a.iii. Does the electoral board test the complete functionality of all equipment and system components before each election?					

Attachment A
Voting Systems Security Self-Assessment Questionnaire

Standard	Yes	No	Evidence	Comments	Initials
C.3.a.iii. Does the electoral board test the complete functionality of all equipment and system components after each election?					
C.3.a.iv. Do vendor personnel conduct either Acceptance or Logic and Accuracy Testing of equipment or system components?					
C.3.a.iv. Do vendor personnel assist elections personnel in the conduct of Acceptance and Logic and Accuracy Testing? If so, how do they assist?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire

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.).

Standard	Yes	No	Evidence	Comments	Initials
C. Technical Security Safeguards <i>COV VSM Standard SEC2005-01.1</i>					
C.4. Network Security					
C.4.a.i. Are any voting system components connected to an electronic communications network (e.g., dial-up, LAN, WAN, Internet, etc.)?					
C.4.a.i. Has the State Board of Elections approved the connection of any voting system components to an electronic communications network?					

NOTES:

Attachment A
Voting Systems Security Self-Assessment Questionnaire
