★ VIRGINIA ★
STATE BOARD of ELECTIONS

BOARD MEETING

Wednesday, November 16, 2022
Video and Teleconference

Videoconference:

https://covaconf.webex.com/covaconf/j.php?MTID=m5f80bae3cb6fa102e0813b7c370e8fbe

Meeting password: 6mUreiWF5M2

Teleconference:

1-517-466-2023 US Toll

1-866-692-4530 US Toll-Free

Access Code: 2436 693 3333

3:00 P.M.

SBE Board Working Papers

STATE BOARD OF ELECTIONS
AGENDA

***DATE*: Wednesday, November 16, 2022**
TELECONFERENCE:
+1-517-466-2023 US Toll
+1-866-692-4530 US Toll Free
Access code: 2436 693 3333
VIDEO CONFERENCE:
https://covaconf.webex.com/covaconf/j.php?MTID=m5f80bae3cb6fa102e0813b7c370e8fbe
Password: 6mUreiWF5M2
***TIME*: 3:00 P.M.**

I. CALL TO ORDER — *Robert Brink, Chairman*

II. APPROVAL OF MINUTES — *Georgia Alvis-Long, Secretary*
- **A. September 27, 2022**
- **B. November 8, 2022**

III. COMMISSIONER'S REPORT — *Susan Beals, Commissioner*

IV. RISK LIMITING AUDIT
- **A. Selecting Races for Risk-Limiting Audits for the November 2022 General Election** — *Karen Hoyt-Stewart, Locality Security (Voting Tech) Program Manager; Rachel Lawless, Confidential Policy Advisor*
- **B. Setting the Risk Limit, Generating the Random Seed Number for Risk Limiting Audits, and Setting the Dates for the RLA** — *Karen Hoyt-Stewart, Locality Security (Voting Tech) Program Manager; Claire Scott, ELECT Policy Analyst*

V. VRSS RECOMMENDATIONS REGARDING 2023 LOCALITY ELECTION SECURITY STANDARDS

Virginia Voter Registration System Security Advisory Group (VRSS)
Arielle Schneider
ELECT Privacy Officer

VI. PUBLIC COMMENT

VII. CLOSED SESSION

- **A. LESS 2023**
- **B. Legal Updates**

VIII. ADJOURNMENT

NOTE: https://townhall.virginia.gov/L/ViewMeeting.cfm?MeetingID=34702

Re. Entrance to the Washington Building
All members of the public will be required to show his/her driver's license, passport or other government issued ID to enter the Washington Building.

All State employees must have on his/her state ID badge on at all times while in the building.

Re. Face Mask
A face mask is required to enter the building if you have NOT been fully vaccinated. A face mask is NOT required if you are fully vaccinated.

Re. public comment
Public comment will first be heard from those persons participating in person as per the sign-up list. Next, we will hear from the persons who requested to speak via chat on the WebEx. Last, we will hear from persons who provided their name and phone number to FOIA@elections.virginia.gov.

Re. limitation on individual participation in public comment
Due to the large number of persons who may wish to speak, we encourage you to be as brief as possible, with a maximum of **THREE** minutes per person. We also ask that you be prepared to approach the podium or unmute yourself if you hear your name announced as the next participant.

Re. individual requests for additional information
Citizens seeking additional information related to matters on this agenda may submit questions to info@elections.virginia.gov

Re. How to Participate in Public Comment
If you are a member of the public and wish to participate, you must sign up in order to be recognized to speak. Please note the following:
If you are attending in person, please ensure your name is on the sign-up list at the front door.
If you are participating virtually using WebEx, sign up using the chat feature, located on the bottom right part of the WebEx application, to add your participant name.
If you are participating virtually using a phone and cannot access WebEx's chat feature, please send an email with your name and your phone number to FOIA@elections.virginia.gov. You will need to provide your first and last name and the phone number you've used to call in.

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Approval of Minutes

BOARD WORKING PAPERS

State Board of Elections
Tuesday, September 27, 2022
FINAL Meeting Minutes

The State Board of Elections ("the Board") meeting was held on Tuesday, September27, 2022, in Senate Room A of the Pocahontas Building in Richmond, Virginia. The meeting also offered public participation through electronic communication so the public could view and hear the meeting at remote locations. In attendance: Robert Brink, Chairman; John O'Bannon, Vice Chairman; Georgia Alvis-Long, Secretary, Angela Chiang, and Delegate Donald Merricks, members; represented the State Board of Elections ("the Board"). Susan J. Beals, Commissioner, represented the Department of Elections ("ELECT"), and Joshua Lief and Travis Andrews represented the Office of the Attorney General ("OAG"). Chairman Brink called the meeting to order at 1:01 P.M.

The first item of business was the approval of the minutes, presented by Secretary Alvis-Long. Delegate Merricks moved *that the Board approve the minutes from the August 16, 2022 Board Meeting.* Vice Chair O'Bannon seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The second item of business was the Commissioner's Report, presented by Commissioner Beals. Commissioner Beals informed the Board that ELECT was out of compliance on its use of the SAVE Program as a part of its list maintenance activities. The

Commissioner stated that ELECT has conducted research on the uses of the SAVE program and staff has completed the necessary training. Commissioner Beals also informed the Board that ELECT has finished redistricting and is in the process of sending out voter notices.

The Commissioner stated that Election Day is November 8, 2022 and early voting began September 23, 2022. Commissioner Beals advised the Board that after two days of early voting 16,726 have voted early in person, and out of 296,339 absentee ballots mailed 4,696 absentee ballots have been returned. The Commissioner stated that the last day to registrar to vote is October 17, 2022 and Same-Day Registration begins the following day. Commissioner Beals stated that this will allow voters to registrar to vote after October 17 and vote a provisional ballot for the November election. The provisional ballot and the voter registration form will then go to the registrar's office to be researched for eligibility. The registrar will make a recommendation to the local Electoral Board and determine whether or not to count the ballot.

The Commissioner expressed her deepest sympathy on the unexpected passing of Warren Younce, ELECT IT System Support Analyst. Commissioner Beals introduced new ELECT employees Claire Scott, ELECT Policy Analyst and Brian Tynes, Media Relations Specialist. Mr. Lief introduced Travis Andrews, Assistant Attorney General to the Board.

The third item of business was the Finalization of Stand By Your Ad Decisions from August 16th Meeting, presented by Tammy Alexander, Campaign Finance Compliance Training Specialist. *This memo is in the Working Papers for the September 27, 2022 Meeting.* Ms. Chiang moved *that the Board finalize the decisions made on the two Stand By Your Ad (SBYA) violations assessed at the August 16, 2022 State Board of Elections (SBE).* Secretary Alvis-Long seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The fourth item of business was the Electronic Meeting Policy, presented by Ashley Coles, ELECT Policy Analyst. *This memo is in the Working Papers for the September 27, 2022 Meeting.* Delegate Merricks moved *that the Board adopt the proposed policy to conduct meetings through electronic communication means in compliance with §2.2-3708.3(D) of the Code of Virginia.* Ms. Chiang seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The fifth item of business was the State Board of Elections Report pursuant to § 103(J) of the Code, presented by Ashley Coles, ELECT Policy Analyst. *This report is in the Working Papers for the September 27, 2022 Meeting.* Chairman Brink opened the floor to public

comment. James Manship addressed the Board. As this was an information item, no motion was required.

The sixth item of business was the Risk Limiting Audit Manual, presented by Karen Hoyt-Stewart, Locality Security Program Manager and Rachel Lawless, Confidential Policy Advisor. *This report is in the Working Papers for the September 27, 2022 Meeting.* Chairman Brink opened the floor to public comment. Ned Jones, James Manship, and Darrell Bow addressed the Board. Vice Chair O'Bannon moved *that the Board approve the proposed Risk Limiting Audit Manual pursuant to §24.2-671.2(B).* Secretary Alvis-Long seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The seventh item of business was Ballot on Demand Systems Certifications, presented by Karen Hoyt-Stewart, Locality Security Program Manager. *This report is in the Working Papers for the September 27, 2022 Meeting.* Chairman Brink opened the floor to public comment. Ned Jones addressed the Board. Delegate Merricks moved *that the Board approve the Ballot on Demand Systems certifications listed effective on the dates on the Testing Certifications.* Vice Chair O'Bannon seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The eighth item of business was the Locality Extensions, presented by Karen Hoyt-Stewart, Locality Security Program Manager. *This memo is in the Working Papers for the September 27, 2022 Meeting.* Chairman Brink opened the floor to public comment. Darrell Bow addressed the Board. Ms. Chiang moved *that the Board approve extensions to the following localities to use the current electronic pollbooks for voter check in on Election Day for the November 2022 General Election.* A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

Chairman Brink opened the floor to public comment. Darrell Bow, Paul Theil, James Manship, Jeffery Shapiro, Ned Jones, Ann Grigorian and Clara Belle Wheeler addressed the Board.

At 2:11 P.M., Delegate Merricks moved pursuant to Virginia Code Section 2.2-3711(A)(7), *that the Board go into closed session for the purpose of discussing pending and threatened litigation. In accordance with Section 2.2-3712(F), Susan Beals, Commissioner of Elections, Joshua Lief and Travis Andrews of the Office of the Attorney General, and Lyn McDermid, Secretary of Administration will attend the closed session because their presence will reasonably aid the Board in its consideration of the subject of the meeting.* Vice Chair O'Bannon seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

At 2:52 P.M., Vice Chair O' Bannon moved *to reconvene the meeting in open session, and take a roll call vote certifying that to the best of each member's knowledge (i) only such public business matters lawfully exempted from open meeting requirements under this chapter and (ii) only such public business matters as were identified in the motion by which the closed meeting was convened were heard or discussed by the State Board of Elections.* Ms. Chiang seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

Delegate Merricks moved *to adjourn the meeting.* Secretary Alvis-Long seconded the motion and the motion passed unanimously. The meeting adjourned at 2:53 P.M.

_____

Chairman

_____

Vice-Chairman

_____

Secretary

_____

Board Member

_____

Board Member

The State Board of Elections ("the Board") meeting was held by electronic communication Tuesday, November 8, 2022. In attendance: Robert Brink, Chairman; John O'Bannon, Vice Chairman; Georgia Alvis-Long, Secretary, Angela Chiang and Delegate Donald Merricks members; represented the State Board of Elections ("the Board"). Susan J. Beals, Commissioner, represented the Department of Elections ("ELECT"), and Joshua Lief and Travis Andrews represented the Office of the Attorney General ("OAG"). Chairman Brink called the meeting to order at 10:00 A.M.

Chairman Brink informed the Board that the only item on the agenda was oversight of the General Election and that there would be no opportunity for public comment. At 10:02 A.M., the Board went into recess.

Chairman Brink opened the meeting from recess at 3:40 P.M.

At 3:41 P.M., Vice Chair O'Bannon moved pursuant to Virginia Code Section 2.2-3711(A)(7), *that the Board go into closed session for the purpose of discussing pending and threatened litigation. In accordance with Section 2.2-3712(F), Susan Beals, Commissioner of Elections, Ashley Coles, ELECT Policy Analyst, Joshua Lief and Travis Andrews of the Office of the Attorney General, will attend the closed session because their presence will reasonably aid the Board in its consideration of the subject of the meeting.* Delegate Merricks seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

At 4:26 P.M., Vice Chair O'Bannon moved *to reconvene the meeting in open session, and take a roll call vote certifying that to the best of each member's knowledge (i) only such public business matters lawfully exempted from open meeting requirements under this chapter and (ii) only such public business matters as were identified in the motion by which the closed meeting was convened were heard or discussed by the State Board of Elections.* Ms. Chiang seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

Vice Chair O'Bannon moved *to authorize the Attorney General to take action to challenge the Circuit Court Order regarding extended hours for the Blackstone Primary School Precinct in Nottoway County.* Secretary Alvis-Long seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary Alvis-Long – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

At 4:27 P.M., the Board went into recess.

Chairman Brink opened the meeting from recess at 7:05 P.M. No further business was conducted during this meeting. Delegate Merricks moved to adjourn the meeting. Ms. Chiang seconded the motion and the motion passed unanimously. The meeting adjourned at 7:06 P.M.

_____
Chairman

_____
Vice Chairman

_____
Secretary

_____
Board Member

_____
Board Member

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Commissioner's Report

BOARD WORKING PAPERS
Susan Beals
Commissioner

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Risk Limiting Audit Drawing

BOARD WORKING PAPERS
Karen Hoyt-Stewart
Locality Security Program Manager

Rachel Lawless
Confidential Policy Advisor

Claire Scott
ELECT Policy Analyst

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Memorandum

To: Chairman Brink, Vice-Chair O'Bannon, Secretary Alvis-Long, Delegate Merricks, and Ms. Chiang

From: Rachel Lawless, Confidential Policy Analyst,
Karen Hoyt-Stewart, Locality Security (Voting Tech) Program Manager

Date: November 16, 2022

Re: Selecting Races for Risk-Limiting Audits for the November 2022 General Election

---

Suggested Motions:

"I move that the Board randomly draw a U.S House of Representative contest to determine the participants of the risk-limiting audit required by the Code of Virginia § 24.2-671.2(C)(1)."

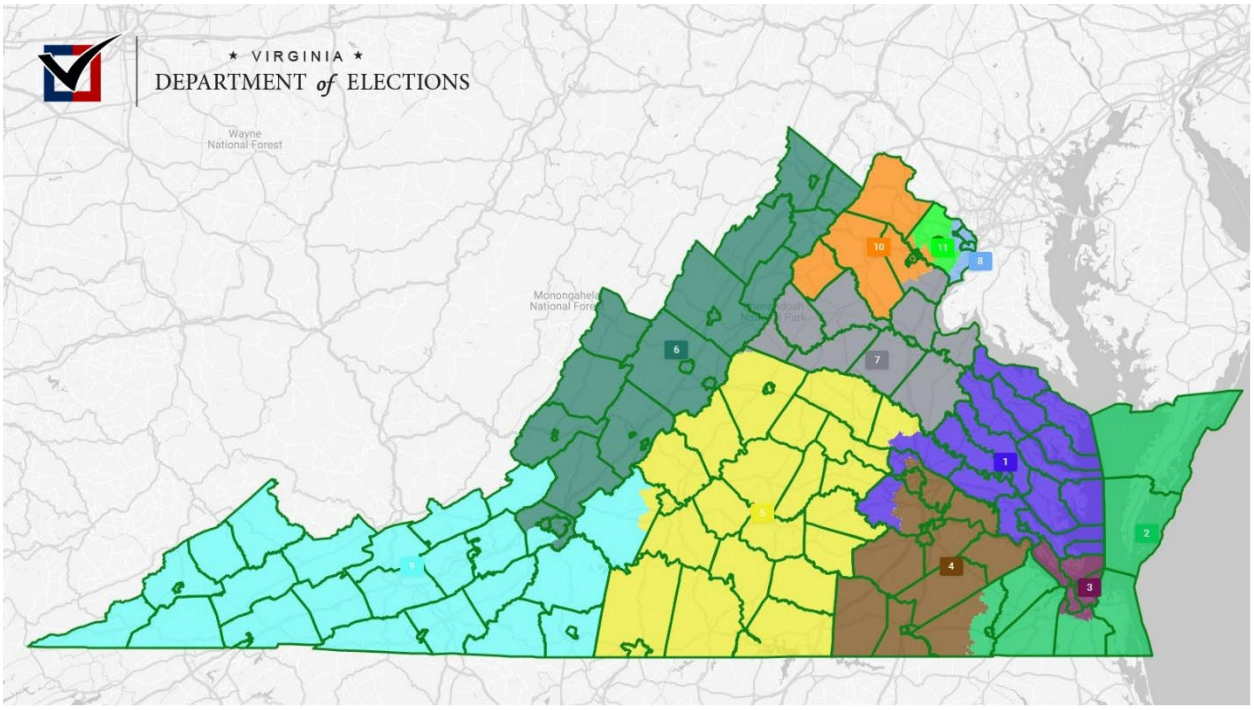
Applicable Code Sections:

§24.2-671.2(C)(1) & (D) Risk Limiting audits; 1VAC20-60-80 Request for a risk-limiting audit for a contested race within a jurisdiction

Overview

Pursuant to §24.2-671.2(F), the State Board of Elections (SBE), in accordance with Subsection C, will determine the contested races for the elections that will receive a risk-limiting audit (RLA). For the November 2022 General Election, at least one contested race for the U.S. House of Representatives will be randomly selected for an RLA. Additionally, this general election will be the first time where local electoral boards have the option, pursuant to §24.2-671.2(D), to apply to the SBE for an RLA to be performed for a contested race in their locality. Those applications submitted to the SBE must fulfill the requirements of the Administrative Code of Virginia 1VAC20-60-80 in order to be approved for to participate in an RLA.

Potential U.S House Races:



Congressional District 1	Congressional District 2	Congressional District 3	Congressional District 4	Congressional District 5	Congressional District 6
James City, York, Gloucester, New Kent, Westmoreland, King William, Northumberland, Lancaster, Middlesex, Essex, Richmond, Mathews, King & Queen Counties; Cities of Williamsburg and Poquoson *Partial: Henrico, Chesterfield, and Hanover Counties*	Accomack, Isle of Wight, Northampton Counties; City of Virginia Beach, Suffolk, and Franklin *Partial: Southampton County; City of Chesapeake*	Cities of Norfolk, Hampton, Newport News, Portsmouth *Partial: City of Chesapeake*	Prince George, Dinwiddie, Brunswick, Greensville, Sussex, Charles City, Surry Counties; Cities of Richmond, Petersburg, Hopewell, Colonial Heights, and Emporia *Partial: Chesterfield, Henrico, and Southampton Counties*	Pittsylvania, Campbell, Louisa, Halifax, Amherst, Mecklenburg, Powhatan, Fluvanna, Goochland, Prince Edward, Buckingham, Nottoway, Appomattox, Nelson, Amelia, Lunenburg, Charlotte, Cumberland Counties; Cities of Lynchburg, Charlottesville, and Danville *Partial: Albemarle, Bedford, and Hanover Counties*	Frederick, Rockingham, Augusta, Harrisonburg, Shenandoah, Warren, Botetourt, Page, Rockbridge, Alleghany, Clarke, Bath, Highland Counties; Cities of Roanoke, Harrisonburg, Winchester, Staunton, Salem, Waynesboro, Lexington, Buena Vista, and Covington *Partial: Roanoke County*

Congressional District 7	Congressional District 8	Congressional District 9	Congressional District 10	Congressional District 11
Stafford, Spotsylvania, Culpeper, Orange, Caroline, King George, Greene, Madison Counties; City of Fredericksburg *Partial: Prince William and Albemarle Counties*	Arlington County; Cities of Alexandria and Falls Church *Partial: Fairfax County*	Montgomery, Franklin, Washington, Henry, Tazewell, Wise, Pulaski, Smyth, Carroll, Wythe, Russell, Lee, Scott, Buchanan, Patrick, Giles, Floyd, Dickenson, Bland, Craig Counties; Cities of Norton, Galax, Martinsville, Bristol, and Radford *Partial: Bedford and Roanoke Counties*	Loudon, Fauquier, Rappahannock Counties; Cities of Manassas and Manassas Park *Partial: Prince William and Fairfax Counties*	City of Fairfax *Partial: Fairfax County*

Selecting a Random U.S. House of Representatives Race

The Chairman of the SBE or their designated representative, SBE or ELECT staff, will randomly select a U.S. House of Representative Race for an RLA. The selection process for the U.S. House of Representatives Race will proceed with the random selection of a film canister from a bowl. Each canister will have one district inside, and the chosen district will be required to perform an RLA.

Selecting Local Races Applied for by Local Electoral Boards

Pursuant to §24.2-671.2(D) and Administrative Code of Virginia 1VAC20-60-80, if a local electoral board votes to have request an RLA for a local contested race they must submit the SBE 24.-671.2(D) Form. The SBE will grant the request if all the requirements and conditions outlined in the regulation are met. Pursuant to 1VAC20-60-80, "Upon granting an electoral board's request for a risk-limiting audit, the SBE may grant an extension not to exceed two weeks of the local electoral board's certification deadline pursuant to § 24.2-671 of the Code of Virginia if necessary for the conduct of the audit."

At this time, no localities have requested races that are within their jurisdiction.

Recommend Actions:

- ELECT staff recommends that Chairman Brink and Commissioner Beals randomly choose a U.S. House of Representatives district via the process described above.

1100 Bank Street
Washington Building – First Floor
Richmond, VA 23219-3947
www.sbe.virginia.gov
info@sbe.virginia.gov

Telephone: (804) 864-8901
Toll Free: (800) 552-9745
TDD: (800) 260-3466
Fax: (804) 371-0194

★ VIRGINIA ★
DEPARTMENT of ELECTIONS

Memorandum

To: Chairman Brink, Vice-Chair O'Bannon, Secretary Alvis-Long, Delegate Merricks, and Ms. Chiang

From: Claire Scott, Policy Analyst, Karen Hoyt-Stewart, Locality Security (Voting Tech) Program Manager

Date: November 16, 2022

Re: Setting the Risk Limit, Generating the Random Seed Number for Risk Limiting Audits, and Setting the Dates for the RLA

Suggested Motion

"I move the Board set the risk limit to 10% for all RLAs performed in the Commonwealth of Virginia for the November 2022 general election."

"I move that the Board generate a random seed number for selecting ballots to be used in the risk-limiting audit, pursuant to §24.2-671.2.

Applicable Code Section:

§24.2-671.2 Risking Limiting audits.

Overview

A risk limit is the maximum chance that the RLA will fail to correct an incorrectly reported outcome. For example, a 10% risk-limit means that there is as a 90% chance that the RLA will correct an incorrect outcome. Every RLA that has been held in the Commonwealth of Virginia has used a 10% risk-limit.

The RLA software uses a 20-digit random seed number to select ballots to be retrieved. A random seed number specifies the starting point of a computer-generated random sequence of numbers. The 20-digit number generated by this activity will be inputted into the RLA software by the RLA Administrator and used for the U.S. House of Representative Race previously selected. Once this number is inputted, the auditing software will randomly select and generate a list of ballots to be retrieved based on the sample size.

Setting the Risk Limit for the RLA

The SBE will set the risk limit of the RLA following industry best practices and announce the risk limit of each RLA at the virtual SBE meeting held to discuss RLAs.

Generating a Random Seed Number for the Selection of Ballots to be Audited in an RLA

To create this random number, the chairman of the SBE or their designated representative(s) will roll a ten-sided die twenty times or 20 ten-sided dice once each and record each number.

Setting the Dates of the Risk-Limiting Audit

ELECT will announce the dates of the risk-limiting audit and will post those dates on ELECT's website along with the races selected by the board.

Recommended Action

- ELECT staff recommends setting the risk limit to 10%.
- ELECT staff recommends generating the random seed number via the process stated above. ELECT also recommends that the Chairman verbally select designees to roll the dice on his behalf.
- ELECT staff recommends the dates of the risk-limiting audit be for the week after Thanksgiving, between November 28 and December 2.

★ VIRGINIA ★
STATE BOARD of ELECTIONS

VRSS Recommendations Regarding 2023 Locality Election Security Standards

BOARD WORKING PAPERS

Arielle Schneider
ELECT Privacy Officer
Virginia Voter Registration System Security Advisory Group
(VRSS)

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Memorandum

To: Chairman Brink, Vice Chair O'Bannon, Secretary Alvis-Long, Angela Chiang, and Delegate Merricks

From: Virginia Voter Registration System Security Advisory Workgroup (VRSS)

Date: November 16, 2022

Re: 2023 Locality Election Security Standards (LESS)

Executive Summary

In alignment with the Code of Virginia §24.2-410.2 Security of the Virginia Voter Registration System, the State Board of Elections is required to update the Locality Election Security Standards by November 30 annually, after consultation with the Voter Registration System Security (VRSS) Advisory Group ("representatives of local government information technology professionals and general registrars"). The VRSS has reviewed the 2022 Locality Election Security Standards (LESS) and made a concerted effort to streamline and clarify the election security standards for all localities regardless of size.

Proposed Motion

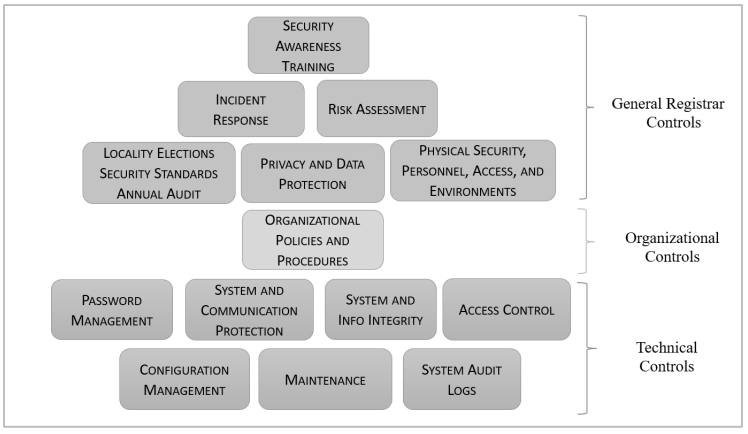
I move to adopt the revised 2023 Locality Election Security Standards effective December 1, 2022.

Background

The purpose of the Locality Election Security Standards (LESS) is to ensure that each county and city meet election security standards designed to maintain the security and integrity of the Virginia voter registration system and supporting technologies through appropriate security controls, policies, practices and procedures. To help all localities work toward improving their cybersecurity stance, the Virginia Voter Registration System Security Advisory Group (VRSS) met over a dozen times between June and October 2022 to write a revised, simplified, and re-structured set of standards and controls.

The Proposed 2023 LESS transforms 22 standards and 441 controls into a streamlined set of 14 standards and 165 controls to allow meaningful reporting and maturity improvements throughout the Commonwealth. The VRSS also restructured the standards into groups depending on implementation (General Registrar, Organizational, and Technical) as well as each control grouped into three maturity paths localities can adopt depending on their size, needs and resources.

To assist localities in organizing the resources needed to implement these controls, we organized the 14 control families into three types of security controls: physical and administrative, technical, and organizational. Within the Locality Election Security Standards, they are designated as GR 1-6, ORG 7, and TECH 8-14.



To assist localities in identifying the top priorities for their security posture, we organized the 165 controls into three maturity paths, identifying the most critical and urgent security controls as the Baseline path all localities are expected to meet. Localities within the Commonwealth must comply with the controls identified as Baseline, the lowest maturity path, and may choose to implement additional

controls as their locality election security posture strengthens. VRSS has also provided localities with a maturity matrix to assess their organizational standing. The maturity matrix has three categories:

BASELINE	Localities meet the minimum LESS controls
PREFERRED	Localities meet the minimum LESS controls and have taken additional steps to tighten their security posture and procedures
PLATINUM	Localities meet all the LESS controls

By law, each locality is required to submit an accurate report of its compliance with LESS by March 1 of each year. Additionally, by April 1, each locality must submit a formal remediation plan for any Baseline controls that it cannot meet.

In conclusion, the updated 2023 Locality Election Security Standards represents a collaborative effort that included input from members of the electoral board, general registrars, city and county information technology leadership, and ELECT staff who have a wide range of expertise in election management, information technology, and cybersecurity.

Attachments

2023 Locality Election Security Standards – Draft

PUBLIC

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

2023 LOCALITY ELECTION SECURITY STANDARDS (LESS)

Voter Registration System Security (VRSS) Advisory Group

Virginia Department of Elections

Virginia State Board of Elections

Presented to the State Board of Elections November 16, 2022

Approved by the State Board of Elections

Version Number: 4

2023 TABLE OF CONTENTS

QUICK START GUIDE

BACKGROUND

The Code of Virginia § 24.2-410.2(A) instructs the State Board of Elections to "promulgate regulations and standards necessary to ensure the security and integrity of the Virginia voter registration system and the supporting technologies utilized by the counties and cities to maintain and record registrant information. The State Board shall, in consultation with representatives of local government information technology professionals and general registrars, update the security standards at least annually. Such review shall be completed by November 30 each year."

The law (Code of Virginia § 24.2-410.2(B)) requires each locality electoral board to "develop and annually update written plans and procedures to ensure the security and integrity of those supporting technologies. All plans and procedures shall be in compliance with the security standards established by the State Board pursuant to subsection A. Each electoral board shall report annually by March 1 to the Department of Elections on its security plans and procedures."

To maintain access to the Virginia Voter Registration System, localities must follow the State Board of Elections' adopted Locality Election Security Standards. Prior to restricting access to the Virginia voter registration system, the Department of Elections must provide notice to the locality of the failure to comply with the required standards or the required reporting on compliance with those standards, and allow the locality seven days to correct deficiencies.

A locality has until March 1 annually to submit its report on compliance with the Locality Election Security Standards, and until April 1 to submit its full Remediation Plan in compliance with the Locality Election Security Standards GR 4 (Locality Election Security Standards Annual Audit).

UPDATES FOR THE 2023 LESS

The Voter Registration System Security (VRSS) Advisory Group annually reviews and recommends updates to the Locality Election Security Standards (LESS) in advance of the State Board's annual review in November. To prepare recommendations for the State Board of Elections, the Virginia Voter Registration System Security Advisory Group (VRSS) met over a dozen times between June and October 2022 to write a revised, simplified, and re-structured set of standards and controls. The VRSS reduced 22 standards and 441 controls to a streamlined, prioritized and mapped maturity path composed of 14 control families and 165 individual controls.

To assist localities in identifying the top priorities for their security posture, we have identified three maturity paths. Localities within the Commonwealth must comply with the controls identified as Baseline, the lowest maturity path, but may choose to implement additional controls as their locality election security posture strengthens. Each locality is required to submit an accurate report of its compliance with LESS by March 1 of each year. Additionally, by April 1, each locality must submit a formal remediation plan for any Baseline controls that it cannot meet.

To further assist you in organizing the resources needed to implement these controls, we organized the 14 control families into three types of security controls: physical and administrative, technical, and organizational. Within the Locality Election Security Standards, they are designated as GR 1-6, ORG 7, and TECH 8-14.

- **GR 1-6 are physical and administrative controls. Physical controls** address process-based security needs using physical hardware devices, such as a badge reader, architectural features of buildings and facilities, and specific security actions taken by people. **Administrative controls** (also known as managerial controls) are directives, guidelines or advisories aimed at the people within the organization. For the purpose of elections security, the local General Registrar typically controls the physical spaces in which elections systems, equipment and personnel operate, and the policies and procedures followed by elections staff-members. These are controls that mostly fall within the ability of the GR to implement. Some support from locality IT staff, and prioritization from local governing bodies and administrators will still be required.
- **ORG 7 is an organizational control (formerly LESS Organizational controls known as Contingency Planning, Security Planning, Program Management, Policy and Procedure, and Security and Acceptable Use).** Organizational controls in the elections context are security controls that require the involvement of locality leadership and technology personnel. These include organizational planning such as disaster recovery, organizational contingency plans, systems security plans, and locality-wide acceptable use policies, for example.
- **TECH 8-14 are technical controls. Technical controls** (also called logical controls) are security controls that computer systems and networks directly implement. A local General Registrar will likely need assistance from technology professionals in order to implement these controls. Examples include access control, system audit logs, and configuration management.

ROLES AND RESPONSIBILITIES

State Board of Elections, Department of Elections, and VRSS Advisory Group

- As per the Code of Virginia §24.2-410.2 the State Board shall, in consultation with representatives of local government information technology professionals and general registrars, update the security standards at least annually. Such review shall be completed by November 30 each year.

Locality Governing Body

- As per §24.2-111, "Each local governing body shall pay the reasonable costs of … conducting elections as required by this chapter", to include allocating the funds necessary to meet requirements in the Code of Virginia §24.2-410.2, regarding security standards approved by the State Board of Elections to ensure the security of the Virginia voter registration system and supporting technologies.

Electoral Board

- The local Electoral Board is accountable and responsible for adherence to and reporting on the Locality Election Security Standards.
- As per §24.2-410.2, the local Electoral Board is responsible for reporting annually to the Department of Elections regarding compliance with LESS. The local Electoral Board is also responsible for submitting exception requests to ELECT.
- The local Electoral Board is also responsible for liaising with the local governing body to ensure the funding of sufficient IT resources to comply with LESS, as well as to resolve any disputes that arise between the local Electoral Board and locality IT resources.

General Registrar

- The local General Registrar is responsible for being familiar with and supporting the local Electoral Board in the implementation of the Locality Election Security Standards.
- For localities with internal information technology (IT) resources, the GR, upon request by the local Electoral Board, may liaise with locality personnel on behalf of the Electoral Board. Issues related to compliance with the LESS should be raised to the attention of the local Electoral Board Chair and then addressed with the appropriate supervisor or manager responsible for locality IT. Issues that persist should be brought back to the local Electoral Board in a formal meeting and handled by the local Electoral Board.
- For localities without internal information technology resources, the GR, upon request by the local Electoral Board, may identify any existing contracts or arrangements the locality has made for the provision of IT resources. The GR should bring this information before the local Electoral Board in a formal meeting, so that the Board may take further action as necessary to secure locality funding and support.

REMEDIATION PLAN

If your locality does not meet all standards and controls designated as Baseline, the local Electoral Board must submit a Remediation Plan to the Virginia Department of Elections by April 1.

For each Baseline control that is not met, the Remediation Plan must include:

- The standard/control that is not met
- The locality's plan for remediation
- The person or people or organizational resources required to remediate
- Signature from local electoral board members (two of three are required)
- Signature of acknowledgement from city or county administrator

RELEASE OF INFORMATION

The Code of Virginia §24.2-410.2(D) mandates that information and records of the State Board or a local electoral board, that describe protocols for maintaining the security of the Virginia voter registration system and its supporting technologies be kept confidential *and excluded from inspection and copying under the Virginia Freedom of Information Act.*

GR 1 – SECURITY AWARENESS TRAINING

PURPOSE

82% of data breaches are tied to "human element" related security weaknesses. GR 1 outlines the requirements to develop and effectively implement Security Awareness Training programs, to lower the risk posed by system user personnel. All localities must meet the controls identified as Baseline in the Maturity Matrix below.

SCOPE

GR 1 applies to all elections staff, as well as personnel having access to elections equipment or responsibility for any information systems identified as sensitive to election-related activities or peripherals.

MATURITY MATRIX

GR 1 –Security Awareness Training	Baseline	Preferred	Platinum
1. Security Awareness Training	1.1	1.1-1.2	All
2. Role-Based Security Training	2.1	2.2	2.2
3. Training Records	3.1	3.1	All

1 Security Awareness Training

1.1 Your Security Awareness Training Program occurs at least annually to ensure each employee with access to elections equipment is aware of and understands the following concepts (and potential penalties for violations):

- 1.1.1 Concept of separation of duties, least privilege, and elevated privileges.
- 1.1.2 How to prevent, detect, and report information security incidents, including those caused by malicious code.
- 1.1.3 Proper use of encryption tools and disposal of data storage media.
- 1.1.4 Access controls, including creating and changing passwords, and the need to keep all authentication information confidential.
- 1.1.5 Special responsibility for the security and privacy of locality/ELECT data. Training specifically discusses personal and sensitive data; how to keep it secure, including redaction and clean desk expectations; and specific penalties for violations.

1.2 Additional security awareness training occurs to ensure each employee with access to elections equipment is aware of and understands the following concepts (and potential penalties for violations):

- 1.2.1 Locality's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data including Election information
- 1.2.2 Locality's acceptable use and Remote Access policies

1.3 Your training includes intellectual property rights, including software licensing and copyright issues and potential penalties for violations.

1.4 Your Security Awareness Training Program occurs quarterly or more regularly, including updates throughout the year and an annual refresher training. Additionally, methods of delivery include, but are not limited to, in-person, online, one-on-one instruction, videos, blogs, social media, posters, newsletters, contests and events consistent with best practices.

2 Role-Based Security Training

Note: This training must occur prior to being granted access or performing assigned duties and must be updated annually.

2.1 *If your locality does not require role-based training:* Within the last year, the GR provided written notice to locality management (CIO, CISO, or county/city administrator) of their responsibility as per the Locality Election Security Standards to ensure any information technology professional such as a system administrator, systems support professional, or help desk staff member who interacts with infrastructure and technology supporting the elections office completes appropriate role based security training annually.

2.2 The locality requires all employees (within the locality or third-party) with access to the locality systems and infrastructure including networks, servers, end-user stations, and elections mobile devices to take role-based security training commensurate with level of access.

3 Training Records

3.1 The General Registrar records required training for elections staff. At a minimum the records for the last two years capture the following: name of trainee, trainee role/access, date training completed, date training expires, and name of training to include the requirement it satisfies, if appropriate.

3.2 The Security Awareness Training Program is documented, monitored, tested, and reviewed for improvement annually.

GR 2 – INCIDENT RESPONSE

PURPOSE

Incident response is the effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents. The purpose of GR 2 is to ensure each elections employee knows signs of a potential cyberattack and how to report such incidents, and that the locality has a response plan outlining the steps to take in the event of a cyberattack.

SCOPE

GR 2 applies to all information systems identified as sensitive to election-related activities and individual components. Components include, but are not limited to: user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets.

MATURITY MATRIX

GR 2 – Incident Response	Baseline	Preferred	Platinum
1. Incident Reporting	All	All	All
2. Incident Response	2.1-2.2	2.1-2.3	All
3. Incident Reporting and Response Training	3.1	All	All

1 Incident Reporting

1.1 All elections employees are provided an internal (specific to your elections office or to your locality, if one is in place) incident reporting procedure to ensure potential cybersecurity incidents are reported to management and transferred to IT personnel for further investigation, as appropriate. This procedure or document defines reportable incidents and outlines how to report the incident internally to the official in Information Technology or your local county or city administrator for further action.

1.2 General registrar and locality officials have implemented and distributed a reporting procedure to comply with §2.2-5514(C) which requires reporting to the Virginia Fusion Center within 24 hours of discovering all (i) known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data protected by federal or state laws and (ii) other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies.

2 Incident Response

2.1 Your elections employees have a current and accurate reference guide for immediate mitigation procedures, including specific instructions based on information security incident type, particularly when and whether to shut down or disconnect affected IT systems.

2.2 Your incident plan identifies and provides contact information for incident response support resources such as your locality InfoSec, IT or systems support, or the Fusion Center for assistance and advice for reporting or handling security incidents.

2.3 Your plan outlines incident handling capability for real-time incident handling of security (and privacy) incidents including written documentation of preparation, detection and analysis, containment, eradication and recovery from incidents.

2.4 Your plan requires post-incident review to include incorporating lessons learned from the incident into training content, incident response procedures, and or employee documentation.

3 Incident Reporting and Response Training

3.1 All elections employees are provided training regarding how to detect potential cybersecurity incidents, including but not limited to red flags such as:

- 3.1.1 Usual files, applications, or services that cannot be accessed.
- 3.1.2 Accounts have been locked or the passwords have been changed without your knowledge
- 3.1.3 Files or software have been deleted or installed, or the contents have been changed without your involvement.
- 3.1.4 Suspicious pop-ups load when you access the internet, or unknown files or programs appear.
- 3.1.5 Slower than normal internet speeds due to a spike in network traffic (or computers "hang" or crash).
- 3.1.6 Files have been unexpectedly encrypted, blocking your access to them.
- 3.1.7 Programs running, turning off or reconfiguring themselves.
- 3.1.8 Emails sent automatically without the user's knowledge.
- 3.1.9 No control over functions of the computer (e.g. in instances whereby device can be controlled remotely, or computer gets locked and displays messages coaxing users into paying a ransom).
- 3.1.10 Requests for credentials

3.2 Incident response training occurs annually for locality personnel responsible for a role in incident response or incident management.

GR 3 – RISK ASSESSMENT

PURPOSE

GR 3 may require you to work with your locality IT and other locality administration officials as needed to identify potential hazards to elections processes and equipment, in order to analyze what could happen if a hazard occurs. The results of a risk assessment enable visibility into risks, potential issues, and existing vulnerabilities.

SCOPE

Risk assessments are conducted on information systems classified as sensitive to election-related activities, to include applications, servers, computers, and networks that process, store, and access or transmit voter registration system related information.

MATURITY MATRIX

GR 3 – Risk Assessment	Baseline	Preferred	Platinum
1. Security Inventory	All	All	All
2. Risk Assessment	2.1	2.1 2.2 2.4	All
3. Vulnerability Scanning	3.1	All	All

1 Security Inventory

1.1 The GR and locality IT support (as available) share an accurate and annually reviewed inventory of information systems and assets used for elections purposes as outlined in TECH 12 – Configuration Management controls 1.1 and 1.2.

1.2 The GR and locality IT support have met to identify the systems most critical to elections operations and which hold sensitive data. These systems are classified as "sensitive". The results of these ongoing discussions are documented in a System Security Plan for the information system.

2 Risk Assessment

2.1 A risk assessment has been conducted within the last two years for each IT system classified as sensitive, to identify threats and vulnerabilities to the confidentiality, integrity and availability of an IT system and the environment in which it operates, including risks posed to operations, assets, or individuals from individuals accessing locality's information systems.

2.2 Risk assessments take into account risk posed to operations, assets, or individuals from external parties, including service providers and contractors operating information systems on behalf of the organization.

2.3 Risk Assessments for each IT system classified as sensitive include an estimated loss impact if one or more vulnerabilities are exploited by a potential threat.

2.4 The GR has been provided within the last year a Risk Assessment Report, which includes at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary including major findings and risk mitigation recommendations. The executive summary in a Risk Assessment Report, including major findings and risk mitigation recommendations, are shared with the General Registrar and local Electoral Board in closed session.

2.5 You have a risk register that outlines each risk finding and provides a risk treatment plan for at least each critical or high risk assessment finding.

3 Vulnerability Scanning

3.1 Your information system and hosted applications are scanned for vulnerabilities regularly. The security classification of the system determines the frequency of scanning. Vulnerability scanning includes scanning for specific ports, protocols, and services that should not be accessible to users and for improper configurations.

3.2 Vulnerabilities identified in scans are classified according to criticality, and tracked via a Risk Register. Mitigation plans for specific vulnerabilities are documented via Plan of Actions and Milestones (POA&Ms). The Risk Register and POA&Ms regarding elections systems are reviewed quarterly at minimum.

GR 4 – LOCALITY ELECTION SECURITY STANDARDS ANNUAL AUDIT

PURPOSE

The Code of Virginia requires local electoral boards to report annually on locality compliance with the Locality Election Security Standards and turn the results into an actionable Remediation Plan. Each locality is required to comply with all standards identified as Baseline, and must submit a Remediation Plan to the Department of Elections by April 1 for each Baseline standard not met.

SCOPE

GR 4 applies to the Virginia voter registration system and all supporting or connected technologies.

MATURITY MATRIX

GR 4 – LESS Security Audit	Baseline	Preferred	Platinum
1. Annual Assessment and Bi-Annual Penetration Test	All	All	All
2. Remediation Plan	All	All	All

1 Annual Assessment and Bi-Annual Penetration Test

1.1 Each locality must internally review LESS compliance annually. The audit will review the locality's overall organizational and information technology compliance to the LESS standards, showing particularly the Baseline controls for which a Remediation Plan will need to be submitted to the Department of Elections. Compliance checklists are submitted to ELECT as required by March 1.

1.2 An external penetration test is conducted at least once every two years.

- 1.2.1 Please provide the date of the penetration test.
- 1.2.2 Please provide the name of the person responsible for receiving the results of this penetration test.

1.3 The results of the external penetration test are provided to the local Electoral Board in a formal report no later than June 1 annually. All records regarding locality security compliance, penetration tests, and remediation must be designated "Restricted" (ineligible for release under the Freedom of Information Act) and sent encrypted if provided electronically.

2 Remediation Plan

2.1 For any controls that are not in compliance, a Remediation Plan is developed to address each non-compliance. A new Remediation Plan is created each year. Plans not closed out from the previous year are included in the new Remediation Plan which documents the following:

- 2.1.1 The control out of compliance
- 2.1.2 The plan to get to compliance
- 2.1.3 Estimated date to get to compliance
- 2.1.4 Person responsible for the plan
- 2.1.5 Progress
- 2.1.6 Progress Date
- 2.1.7 Status of the plan (Open/Closed)

2.2 A locality's Remediation Plan must be updated monthly with a progress report regarding completion efforts. This plan must be reviewed by and re-signed by the local electoral board quarterly at minimum Please provide the previous year's Remediation (or Corrective Action) Plan.

GR 5 – PRIVACY AND DATA PROTECTION

PURPOSE

GR 5 defines personal information, sensitive information and sensitive system, as well as outlines requirements for the protection of data to ensure its confidentiality, integrity and availability for legal purposes.

SCOPE

GR 5 applies to all data and information collected by or used for elections purposes, and to all users and locality assets and resources, including the following:

- Locality employees, contractors or third-parties with physical or logical access to data and information in all formats

For the purpose of this standard, the above individuals are collectively referred to as "users".

DEFINITIONS

Personal information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. This includes (i) identifiers such as internet protocol address, email address, home address, contact information, account name, social security number, driver's license number, passport number, or other similar identifiers; (ii) information contained in voter registration forms, applications for absentee ballots; and (iii) voter registration or participation history. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Sensitive information means all records, information and data in any format regarding (i) the security of elections offices, polling places, voting and counting equipment, ballots, the Virginia voter registration system and supporting technologies; (ii) personal information as defined in the Code of Virginia §24.2-101; (iii) sensitive personal information as defined in 1 VAC 20-20-20; (iv) personally identifiable information (PII) as defined in the Code of Virginia §18.2-186.6 and (v) information exempt or excluded from the Freedom of Information Act as described in the Code of Virginia 24.2, et seq. and 2.2-3700, et seq.

Sensitive system means a system is considered sensitive if it contains personally identifiable information about individuals, information about the security of elections (physical, cyber, etc.), information regarding the Virginia voter registration system, information designated as confidential or restricted, or information (or a system) designated as sensitive by the locality or Department of Elections.

MATURITY MATRIX

GR 5 – Privacy and Data Protection	Baseline	Preferred	Platinum
1. Personal and Sensitive Information	All	All	All
2. Data Release and Transport	2.1	All	All
3. Destruction	3.1	3.1	All

1 Personal and Sensitive Information

1.1 The General Registrar or designee conducts specific training for all elections employees and staff (full-time, part-time, and seasonal) to identify, mark (watermark, stamps, headers) and safeguard personal and sensitive information in elections records.

1.2 Anyone with access to elections records that include personal or sensitive information is trained to use a redaction tool.

1.3 Anyone with access to elections records that include personal or sensitive information has access to and is trained to use an email encryption tool.

2 Data Release and Transport

2.1 Prior to the locality releasing records and information, the General Registrar or trained designee confirms that records do not contain personal information, sensitive information, or information which is prohibited from release by the Code of Virginia.

2.2 The General Registrar documents the physical transport of elections information (data and records) outside of restricted areas (reference Physical: Access control 1) including

- 2.2.1 Description of information being transported.
- 2.2.2 Type of Information (e.g. Personally Identifiable Information) contained on the media.
- 2.2.3 Method(s) of transport.
- 2.2.4 Protection methods employed.
- 2.2.5 Name(s) of individual(s) transporting the information.
- 2.2.6 Authorized recipient(s) where practical/applicable.
- 2.2.7 Dates sent and received.

3 Destruction

3.1 The General Registrar works with locality IT or technology partner to ensure that sensitive data, information and records are sanitized prior to disposal. If no partner or support exists, the GR must provide written notice to locality management (CIO, CISO, or county/city administrator) of this responsibility as per the Locality Election Security Standards.

3.2 The locality has a documented process governing the destruction and sanitization of information technology resources. The process provides different methods of destroying and sanitizing media depending on the categorization or security classification of the information.

GR 6 – PHYSICAL SECURITY: PERSONNEL, ENVIRONMENT, & ACCESS

PURPOSE

GR 6 works to ensure that employees and business partners comply with the minimum-security prerequisites applicable to their function, and are informed of their responsibility to protect locality information; that physical access controls adequately protect equipment and information; and that environmental factors such as emergency are considered and implemented.

SCOPE

GR 6 applies to employees (classified or temporary), contractors and business partners who participate in election-related activities. This includes, but is not limited to: personnel with access (both general and privileged users) to information systems identified as sensitive to election-related activities; to include applications, servers, computers, devices and networks that process, store, access or transmit voter registration system related information. GR 6 also applies to all locality controlled facilities and those facilities or premises controlled by locality vendors or Third Party Associate organizations.

PHYSICAL SECURITY: PERSONNEL

MATURITY MATRIX

GR 6 – (Personnel)	Baseline	Preferred	Platinum
1 Personnel Screening	1.1-1.2	1.1-1.3	All
2 Personnel Termination and Transfer	All	All	All
3 Personnel, Vendor, and Third-Party Access Agreements	3.1	3.1-3.2	All

1 Personnel Screening

1.1 The GR will ensure any officers of election are registered voters by confirming their status in the Virginia voter registration system. The Code of Virginia 24.2-115 requires an officer of election to be a qualified voter of the Commonwealth.

1.2 The GR will conduct, or request the appropriate locality official to conduct, a background check on any full-time employee prior to the employee starting work.

1.3 Localities will conduct background checks on all (full, part-time, and seasonal) staff members involved in the election process.

1.4 Individuals granted access credentials to the Virginia voter registration system undergo a specific, documented screening process if their duties or tasks involve access to sensitive information and assets. Until the required controls are completed, individuals cannot be appointed to a position or have access to sensitive information and assets.

1.4.1 Please be ready to provide the document outlining your additional screening process for employees granted access credentials to the Virginia voter registration system.

2 Personnel Termination and Transfer

2.1 The General Registrar or Secretary of the locality electoral board must notify ELECT (during working hours) of the termination or resignation of any user with a VERIS account. Notifications are made via email to electit@elections.virginia.gov. The notification must occur within 4 hours of the user's resignation if voluntary, and within 1 hour if the termination is involuntary.

2.2 The locality or GR's office has a documented off-boarding and transfer process which includes the requirements to terminate/revoke any authenticators/credentials associated with the individual or role and retrieve the appropriate assets (laptops, ID's, remote access tokens, removable media, etc.).

3 Personnel, Vendor, and Third-Party Access Agreements

3.1 Document (and include in Inventory discussed in Risk Assessment 1.1 and Access Control 1.6) any third-party access to organizational information and information systems, and ensure each has signed appropriate confidentiality agreements.

3.2 Develop and document access agreements including NonDisclosure Agreements (NDAs) for sensitive systems.

3.3 Responsible locality entity ensures the appropriate access agreement(s) has (have) been signed and are retained in a secure location, in accordance with locality record retention policies. The base agreements are reviewed annually and changed if needed, and include the below (not an inclusive list):

- 3.3.1 Contractor shall fully cooperate with Commonwealth incident response resources and all required law enforcement personnel for assistance in the handling and reporting of security incidents.
- 3.3.2 Contractor shall, at all times, remain compliant with the privacy and security requirements mandated by federal, state and local laws and regulations.
- 3.3.3 Contractor shall not use any software, hardware or services which have been prohibited pursuant to § 2.2-5514 of the Code of Virginia.
- 3.3.4 Contractor shall only store and process Elect data within the continental United States.

3.4 As part of contracts or service level agreements (SLAs), require third-party entities to perform the appropriate background checks of personnel, and to notify the localities when the entity's personnel are transferred or terminated.

Page Break

PHYSICAL SECURITY: ENVIRONMENT

MATURITY MATRIX

GR 6 – (Environment)	Baseline	Preferred	Platinum
4. Emergency Power	4.1	All	All
5. Location of Information System Components	5.1	5.1	5.1

4 Emergency Power

4.1 Short-term uninterruptible power supply (UPS) or a generator is installed to facilitate an orderly shutdown of elections desktops or servers in the event of a primary power source loss.

4.2 Any UPS supporting infrastructure is tested quarterly and generators are tested annually to ensure the devices are working properly. The results of these tests are documented. The following information is documented:

- 4.2.1 Date of test
- 4.2.2 Name of Person performing the test
- 4.2.3 Name of Device tested
- 4.2.4 Results of the test

5 Location of Information System Components

5.1 Elections equipment and documents are stored in a secure environment. This environment is only accessible to people noted on the physical access list.

Page Break

PHYSICAL SECURITY: ACCESS

MATURITY MATRIX

GR 6 – (Access)	Baseline	Preferred	Platinum
6. Restricted Access Area	All	All	All
7. Monitor Physical Access	7.1	All	All
8. Access Records for Secure Areas	All	All	All
9. Visitor Access	9.1	All	All

6 Restricted Access Area

6.1 Personnel with access to elections equipment or documents are listed in the Inventory (referenced in Risk Assessment 1.1). Access is physically restricted to authorized election personnel through keys, combination locks, badges, or smart cards.

6.2 Access list to physical spaces is reviewed quarterly to ensure that individuals still require access. Physical access devices are collected from those that no longer need access.

6.3 Keys, badges, smart cards, equipment, and documents are collected and deactivated within 24 hours of last active day of work. Combinations are changed within 24 hours of last active day of work in a voluntary termination or transfer. Keys, badges, smart cards, equipment, and documents are collected and deactivated immediately for involuntary terminations. Combinations are changed immediately for involuntary terminations.

6.4 Physical access devices are secured in a lock box or cabinet. Combinations are stored securely, such as a software key vault.

7 Monitor Physical Access

7.1 Excepting election-day chain of custody provisions, access to physical spaces where elections equipment and/or ballots are stored or kept are monitored with cameras or card readers.

7.2 Review access logs monthly for anomalies.

7.3 Violations are handled through the incident response process as discovered.

8 Access Records for Secure Areas

8.1 Individuals given access to elections equipment or documents is documented and updated quarterly. The document captures the following:

- 8.1.1 The individual provided physical access
- 8.1.2 Approval of access
- 8.1.3 Date access was provided
- 8.1.4 What physical access the individual has. (Rooms/Cabinets/Physical Documents)
- 8.1.5 Physical access devices (Keys, badges, smart cards) provided to the individual \
- 8.1.6 Date access was revoked

9 Visitor Access

9.1 Visitors such as guests or maintenance personnel that do not have access must register their visit with the locality before being given access. Documentation must capture the following:

- 9.1.1 Visitor name and business they represent
- 9.1.2 Purpose of visit
- 9.1.3 Date/time of arrival
- 9.1.4 Date/time of departure
- 9.1.5 Temporary badge id if applicable

9.2 All visitors to must be escorted by a locality representative at all times.

ORG 7 – ORGANIZATIONAL POLICIES AND PROCEDURES

PURPOSE

ORG 7 exists to assist locality leadership and management, as well as technology or security personnel to prioritize, fund and establish a locality Information Security Program that will support compliance with the Locality Election Security Standards.

SCOPE

Requirements for policies, plans and procedures apply to all organizations which support information systems identified as sensitive to election activities and individual components or software – or necessary to access said system(s). Components include, but are not limited to: user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets. Software includes, but is limited to operating systems, database software, applications, firmware, encryption software, security software, network/General Support System (GSS) support applications, and any other software resident on (or necessary to a component to access) the sensitive elections related system(s). *This standard also applies to all network- based and locally based authentication and stand-alone systems utilized to gain access to these sensitive election-related systems*.

ORG 7 – Organizational Policies and Procedures	Baseline	Preferred	Platinum
1. Organizational Security Planning	1.1 1.2 1.5	1.1 1.3 1.5 1.7	1.1 1.4 1.5-1.8
2. System Security Planning	2.1	All	All
3. Acceptable Use and Policies	All	All	All

1 Organizational Security Planning

1.1 Locality leadership (city/county administrator or technology leadership) has provided the General Registrar a Business Impact Assessment (BIA) within the last year, that specifically addresses the locality's elections-specific mission and goals and:
- 1.1.1 Lists all core functions, in order of priority with relation to organizational mission and goals.
- 1.1.2 Outlines impact of the loss or degradation of the functions with respect to the mission goals.

1.2 Within the last year, your locality has created and/or updated an elections-specific Contingency Plan (CP) that, among other goals, does the following:
- 1.2.1 Identify essential missions and business functions and associated contingency requirements.
- 1.2.2 Identify critical system assets supporting essential missions and business functions.
- 1.2.3 Provide recovery objectives, restoration priorities, and metrics.
- 1.2.4 Address contingency roles, responsibilities, assigned individuals with contact information.
- 1.2.5 Address maintaining essential missions and business functions despite a system disruption, compromise, or failure.
- 1.2.6 Address eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented.
- 1.2.7 Be reviewed and agreed to by the locality General Registrar and Electoral Board.

1.3 The Contingency Plan lists the people, tools, technologies, processes, and support functions that must be in place to resume normal or possibly degraded functionality when one or more threats materialize to

place the mission of the organization in jeopardy. Some examples of threats include, but are not limited to:

1.3.1 Damaging weather (wind/flood, etc.).
1.3.2 Civil Unrest.
1.3.3 Cyber Attack.
1.3.4 Loss of Power or Internet Service.
1.3.5 Insider Threat.

1.4 Your locality's Security Program includes the existence of a Systems Security Plan, BIA, and Contingency Planning Policy – all of which have been reviewed within the last year, provided to the locality General Registrar and Electoral Board, and comply with the standards outlined in 1.1-1.3 to cover the scope of all election-related business processes and associated information systems identified as sensitive to election-related activities, to include applications, servers, computers, and networks; that process, store, access or transmit voter registration system related information.

1.5 Your locality Contingency governance (whether your locality has some or all of the Contingency Plan, Contingency Planning Policy, Contingency Procedure) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and facilitates the implementation of the contingency planning policy and the associated contingency planning controls, to include:

1.5.1 Coordination of contingency planning with the appropriate organizational elements – leadership, technology, personnel, fiscal, maintenance.
1.5.2 Alignment with contingency plans of external service providers to ensure that contingency requirements can be satisfied.
1.5.3 Identifying alternative processing and storage sites that are separated from the primary site(s) to reduce susceptibility to the same threats.

1.6 Training is consistent with assigned roles and responsibilities in the contingency plan and any related policies, procedures or plans.

1.7 Training incorporates simulated events into contingency training to facilitate effective response by personnel in crises.

1.8 Testing the contingency plan using varying methods but at least once in the last calendar year that:

1.8.1 Tests the alternate processing site and alternate telecommunications services to familiarize personnel with the facility, resources, and to allow the evaluation of capabilities of alternative site/telecommunications services to support contingency operations.
1.8.2 Test includes full recovery and constitution of the system to a known state.

2 System Security Planning (SSP)

2.1 The locality has developed a security plan for the information systems identified as sensitive to election activities and their components. Each system security plan:

2.1.1 Maps the relevant, associated elements of the organization's enterprise architecture.
2.1.2 Explicitly defines the authorization boundary for the system.
2.1.3 Describes the operational context of the information systems in terms of missions and business processes.
2.1.4 Provides the security categorization of the information system and relationships with or connections to other information systems.
2.1.5 Provides an overview of the security requirements for the system and identifies any relevant overlays, if applicable.
2.1.6 Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions.

2.2 Within the last year, the locality's security plan has been updated to address changes to the information system, environment of operation or problems identified during security control assessments, and distributed to appropriate managers.

3 Acceptable Use Policy

3.1 Your locality Acceptable Use policy has been distributed to all elections employees and reviewed/updated in the last calendar year, and clearly:

- 3.1.1 Prohibits the use of elections assets for personal gain, to promote hatred or discriminatory tendencies, to misrepresent or make fraudulent statements, or for pornography.
- 3.1.2 Prohibits unauthorized remote connections, installation of software or any unauthorized modifications to Information System assets or hardware components; intrusive network monitoring; bypassing security mechanisms; using assets to elevate user privilege beyond what is approved and needed for business requirements.
- 3.1.3 Notifies users that their activities may be monitored, inspected and collected without user permission, prohibits the sharing of sensitive information with non-authorized individuals, on social media, or in printed materials; requires users to use encryption or another secured means to share sensitive information with authorized users; outlines responsibility to secure and dispose of sensitive material falls on individuals who whom access or materials are given.

3.2 If remote work is permitted, Remote Access policy has been reviewed and updated, as well as distributed to all elections employees, in the last calendar year.

3.3 Incident Reporting Procedure has been reviewed and updated, as well as distributed to all elections employees, in the last calendar year.

3.4 Incident Response Plan has been reviewed and updated, as well as distributed to all elections employees, in the last calendar year.

TECH 8 – PASSWORD MANAGEMENT

PURPOSE

TECH 8 outlines technical controls necessary to mitigate the risk of unauthorized access.

SCOPE

TECH 8 applies to all information systems and components used for elections or by elections staff including user productivity systems (laptops/desktops), application servers, mobile devices, network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets. TECH 8 also applies to all network-based and locally based authentication and stand-alone systems utilized to gain access to sensitive election-related systems.

MATURITY MATRIX

TECH 8 – Password Management	Baseline	Preferred	Platinum
1. Password Complexity	1.1-1.3	1.1-1.3	All
2. Password Management	2.1-2.6	2.1-2.7	All

1 Password Complexity

1.1 All system passwords to access elections workstations and systems are at least 14 characters in length.

1.2 Passwords must contain all of the following: upper case character, lower case character, number, and special character.

1.3 Passwords cannot contain whole or partial user names, user ids, or repeating strings (e.g. 12341234).

1.4 Prevent easily guessable passwords by comparing against a common password list before accepting the password.

2 Password Management

2.1 Passwords are encrypted at AES 256 or higher when transmitted or stored.

2.2 Passwords are not shared.

2.3 Passwords are not displayed on screen on entry, are obscured while being entered, and cannot be unmasked.

2.4 Users authenticate with current password before changing to a new one. The previous 3 passwords may not be reused when resetting passwords.

2.5 Access to the password storage location is highly restricted.

2.6 All systems require passwords to be changed every 90 days.

2.7 All elections employees have and use a password manager approved and installed by authorized technology personnel.

2.8 Feedback for invalid credentials are vague and do not provide clues to why an authentication failed. If a user tries to log in unsuccessfully, they only receive a "Login Unsuccessful" message. Additionally, password composition is never displayed to an unauthorized user.

TECH 9 – SYSTEM AND COMMUNICATION PROTECTION

PURPOSE

TECH 9 outlines required controls to implement boundary protection devices to monitor activity, traffic, and potential attacks; ensure appropriate encryption for data in transit and at rest; and outline requirements for wireless devices.

SCOPE

TECH 9 applies to all information systems and components identified as sensitive to election-related activities and individual components.

MATURITY MATRIX

TECH 9 – System and Communication Protection	Baseline	Preferred	Platinum
1. Boundary Protection	1.1-1.2	All	All
2. Use of Cryptography	2.1-2.2	All	All
3. Wireless Devices	3.1-3.2	3.1-3.3	All

1 Boundary Protection

1.1 Boundary protection devices such as firewalls, gateways, routers, and proxies are used to manage connections to external systems and incoming requests. Localities must also have an architectural diagram of how these tools are implemented locally.

1.2 Unused network ports and physical device ports are disabled on elections equipment.

1.3 Subnetworks are implemented for publicly accessible system components to separate them from internal organizational networks.

1.4 Monitoring tools are put in place to monitor potential Distributed Denial-of-Service (DDoS) attacks. These tools are also capable of mitigating DDoS attacks.

1.5 Port protection capabilities are incorporated into the network and servers protect against attacks such as ethernet switching table overflow attacks, DHCP server attacks, ARP spoofing attacks, DHCP starvation attacks and prevent the connection of unauthorized equipment to network/servers.

2 Cryptography

2.1 All information must be encrypted while in transit.

2.2 All sensitive data must be encrypted while at rest.

2.3 Digital signatures must be part of the encryption process.

3 Wireless Network

3.1 Wireless access points are password protected in compliance with Password Management.

3.2 Encryption compliant with Federal Information Processing Standards (FIPS), such as FIPS 140-2, is enabled on wireless networks.

3.3 Wireless networks are not publicly viewable (the SSID of a locality wireless network should be hidden).

3.4 Logging is enabled on wireless networks and generating log information per System Audit Logs.

TECH 10 – SYSTEM AND INFORMATION INTEGRITY

PURPOSE

TECH 10 addresses required malicious code protections, security alerts, advisories and directives, information system monitoring, backups and recovery.

SCOPE

TECH 10 applies to all information systems identified as sensitive to election-related activities and individual components. Components include, but are not limited to: user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets.

MATURITY MATRIX

TECH 10 – System and Information Integrity	Baseline	Preferred	Platinum
1. Malicious Code Protection	All	All	All
2. Security Alerts, Advisories, and Directives	2.1-2.3	All	All
3. Information System Monitoring	3.1	3.1	All
4. Backup and Recovery	4.1-4.3	All	All

1 Malicious Code Protection

1.1 Any devices that connect to ELECT's systems must have an active malware/anti-virus/malicious code scanning tool enabled at all times. All patches/updates must occur on a monthly-basis at minimum or sooner as needed to address specific vulnerabilities.

1.2 Any devices that connect to ELECT's systems must have active anti-malware and spam controls on their email systems. This tool must be updated on a real-time basis.

2 Security Alerts, Advisories and Directives

2.1 The locality GR and/or locality IT representatives are members of the Center for Internet Security (CIS) Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) and/or Multi-State ISAC (MS-ISAC).

2.2 All information must be encrypted while in transit.

2.3 All locality equipment used to conduct elections business must encrypt its data while at rest or stored on the equipment.

2.4 Digital signatures must be part of the encryption process.

3 Information System Monitoring

3.1 Any devices that connect to ELECT's systems must be continuously monitored for the following:

- 3.1.1 Login Failures
- 3.1.2 Access exceptions
- 3.1.3 System exceptions
- 3.1.4 Operating System and Application patching

3.2 Any devices that connect to ELECT's systems must continuously log the following:

3.2.1 Login Failures

3.2.2 Access exceptions

3.2.3 System exceptions

3.2.4 Operating System and Application patching

4 Backup and Recovery

4.1 Provide the capability to restore system components within the Continuity of Operations Plan (COOP), from configuration-controlled and integrity-protected information.

4.2 Depending on criticality, perform monthly, quarterly and annual backups of system data and system images. The locality has and regularly updates documentation identifying the level of criticality and frequency required.

4.3 Backup copies of critical systems are stored in a separate facility or in a fire-rated container that is not co-located with the operational system.

4.4 Test data backups quarterly to ensure data recovery, integrity and usability.

4.5 Test system recovery annually to verify the integrity and usability of system backups.

TECH 11 – ACCESS CONTROL

PURPOSE

TECH 11 outlines requirements to prevent unauthorized user access by verifying and validating users are permitted to access the systems and data.

SCOPE

TECH 11 applies to all information systems identified as sensitive to election-related activities and individual components or software. Components include, but are not limited to: user productivity systems (laptops/desktops), application servers, mobile devices, network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets. This standard applies to all network-based and locally based authentication and stand-alone systems utilized to gain access to sensitive election-related systems.

MATURITY MATRIX

TECH 11 – Password Management	Baseline	Preferred	Platinum
1. Actively Manage Access	1.1-1.8	1.1-1.11	All
2. Separation of Duties and Account Creation	All	All	All
3. Access	All	All	All
4. Mobile Devices	All	All	All
5. Unsuccessful Logon Attempts	All	All	All
6. System Use Notification	All	All	All

1 Actively Manage Access

1.1 Access to systems is limited only to authorized personnel who need access to the system to perform specific assignments.

1.2 Users given access to systems are given the minimum level of access required within the system to perform their jobs, adhering to the principle of “least privilege”.

1.3 Separate accounts are created and maintained for elevated/privileged accounts. These accounts must adhere to 1.1 and 1.2 and may not be used for daily business work.

1.4 Users who change roles or positions must have their access reviewed to ensure access still complies with 1.1-1.3. Access within a system or to a system that is no longer needed is removed.

1.5 Accounts (access to systems and access within systems) are reviewed at least quarterly for terminations or inactivity. Accounts that have not been active in the last 90 days are disabled.

1.6 Requests for new accounts or access must capture a requestor’s name, date, role and supervisor name, as well as denote who approved the request and when, in addition to documenting what access was granted, both which systems and the level of access provided within those systems.

1.7 Privileged accounts are automatically logged out after five minutes of inactivity.

1.8 No temporary, test, or default accounts are permitted. If the account is necessary it is set up as a permanent account with a unique id.

1.9 Disable service and network sign-on accounts from concurrent use.

1.10 Disable user accounts within 24 hours of last active day of work. Disable user accounts immediately for involuntary termination.

1.11 Automate quarterly account reviews to ensure accounts for terminated personnel or accounts that have not been active in the last 90 days are disabled.

1.12 Use Role Based Access (RBAC) to manage access to systems and system privileges.

1.13 List the role(s) a user will need to perform business functions on the application for a new user account. Applicants or assigned Supervisors must list the systems and groups the user needs, prior to account approval and creation.

1.14 Log and track Privileged Accounts usage separately from the use of General User accounts. Review the Privileged Users' activities on the system(s) for which they are accountable, at least quarterly.

2 Separation of Duties and Account Creation

2.1 Shared accounts and passwords are prohibited.

2.2 Every user granted an account to an information system is assigned a unique ID for account access traceability.

2.3 Ensure security personnel who administer access control functions do not administer audit functions. For sensitive processes, assign different tasks of a process to more than one individual so that no one person can solely initiate, record, authorize, and reconcile a transaction without the intervention of another person.

3 Access

3.1 Employ two-factor authentication as part of the identification and authentication process for remote access or to use admin accounts.

3.2 Accounts are locked after 15 minutes of inactivity. Users must re-authenticate to regain access.

3.3 Users are identified and authenticated (including a confirmation that required training has been completed) before receiving credentials.

3.4 Every system records when users accesses a system. At a minimum it captures the user id, the action, and the date and time.

4 Mobile Devices

4.1 All mobile devices used to conduct elections business must be password protected.

4.2 All mobile devices used to conduct elections business must be configured to permit the locality to remote wipe the device.

4.3 Encrypt mobile devices that contain elections specific data to protect the confidentiality and integrity of that information. Encryption must be AES 256 compliant and applies to data storage and transmission (where applicable).

5 Unsuccessful Logon Attempts

5.1 Invalid logon attempts are limited to three attempts within a 15 minute period. If three invalid attempts are detected within 15 minutes, then the account is time-locked for 15 minutes.

5.2 Do not provide users any indication of what the password lacked during any unsuccessful login attempt(s). For example, if a user tries to log in unsuccessfully, they only receive a "Login Unsuccessful" message. Unsuccessful login details are not provided to the user.

6 System Use Notification

6.1 Display to users a notification message or banner before granting access to a local system. This message is displayed until users acknowledge the usage conditions and takes explicit actions to log on. The message provides privacy and security notices consistent with applicable federal laws, executive orders, directives, policies, regulations, standards and guide and states at a minimum the following:

6.1.1 Users are accessing a government or private information system

6.1.2 The information system usage may be monitored, recorded, and subject to audit

6.1.3 Unauthorized use of the information system is prohibited and subject to criminal and civil penalties

6.1.4 Use of the information system indicates consent to monitoring and recording

TECH 12 – CONFIGURATION MANAGEMENT

PURPOSE

TECH 12 outlines configuration management requirements designed to help mitigate the risk of unauthorized changes being introduced into information systems without proper approval.

SCOPE

TECH 12 applies to all infrastructures owned or managed by localities (or designated third party) that are used to provide IT services in support of sensitive election-related system(s), their individual components, and any software or applications resident on those systems – or necessary to access said system(s). Components include, but are not limited to: user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets. Software includes, but is limited to: operating systems, database software, applications (including mobile), firmware, encryption software, security software, network/GSS support applications and any other software resident on (or necessary to a component to access) the sensitive elections related system(s).

MATURITY MATRIX

TECH 12 – Configuration Management	Baseline	Preferred	Platinum
1. Baseline Configuration for Elections Related Systems	1.1-1.3	1.1-1.5	All
2. Change Control	2.1	2.1	2.1

1 Baseline Configuration for Elections Related Systems

1.1 An inventory of hardware assets is maintained. The inventory should capture the following for hardware assets
- 1.1.1 Type of equipment
- 1.1.2 Manufacturer
- 1.1.3 Model
- 1.1.4 Serial Number
- 1.1.5 Manufacture Date

1.2 An inventory of software assets is maintained. The inventory should capture the following for software assets
- 1.2.1 Name of software
- 1.2.2 Software vendor
- 1.2.3 License quantity
- 1.2.4 License expiration

1.3 The baseline configuration for hardware and software is documented for each item on the inventory listed created in 1.1 and 1.2. This document is updated continually as configurations are changed. At minimum configurations for passwords and access controls are documented as outlined in Password Management, Access Controls, and Audit Accountability.

1.4 Localities with locally maintained IT services must capture configuration information for hardware and software. Below is a list configuration settings that are captured. This list is not intended to be exhaustive.
- 1.4.1 HARDWARE: Open Ports, White/Black List of IP Addresses, DNS Settings, Connected Devices, Installed Software, Installed OS, Security Policies, Processors, Memory, Diskspace
- 1.4.2 SOFTWARE: Home/Install Directory, Environment Variables/Paths, Memory Settings, CPU Settings, Plugins, Database Connections

1.5 Hardware and software inventories are updated annually with any changes that have occurred.

1.6 Technical architecture diagrams are created, maintained, and kept secure for elections systems. This diagrams should capture information about the following:

- 1.6.1 Servers (File/Database/Web/Print)
- 1.6.2 Devices (Phone/Tablets/Laptops/Desktops)
- 1.6.3 Firewalls
- 1.6.4 DMZ
- 1.6.5 Network Segmentations
- 1.6.6 Software layers
- 1.6.7 Server to Server interactions
- 1.6.8 Network Protocols

2 Change Control

2.1 A documented change control process must be in place to manage changes to hardware or software systems. The process must include a step to update relevant inventories or diagrams that may be impacted by changes. This process must capture the following information for each change.

- 2.1.1 Description of the change that include information about the hardware or software being changed
- 2.1.2 Who is requesting the change
- 2.1.3 Who is responsible for implementing the change
- 2.1.4 The date/time the change will be implemented
- 2.1.5 Who approved the change
- 2.1.6 ISO or person representing the ISO role approval

TECH 13 – MAINTENANCE

PURPOSE

TECH 13 addresses maintenance of physical assets and locations, as well as software, providing documentation requirements to ensure external parties also comply.

SCOPE

The Maintenance standard addresses information security aspects of the maintenance program for information systems identified as sensitive to elections activities, and applies to all types of maintenance conducted to any system component (including equipment and applications; in-contract, warranty, in-house, software maintenance agreement, etc.). System maintenance includes those components not directly associated with information processing and/or data information retention such as scanners, copiers and printers.

MATURITY MATRIX

TECH 13 – Maintenance	Baseline	Preferred	Platinum
1. Physical Maintenance	All	All	All
2. Software Maintenance	All	All	All
3. Maintenance Documentation	All	All	All

1 Physical Maintenance

1.1 Physical elections equipment is serviced in accordance with manufacturer or vendor specifications and/or organizational requirements.

1.2 Maintenance and service performed on elections equipment is documented. The following information is captured for each device serviced:

- 1.2.1 Equipment Serviced
- 1.2.2 Equipment Identification Number
- 1.2.3 Date/time of service
- 1.2.4 Name of person that performed service
- 1.2.5 Description of service performed
- 1.2.6 If the equipment was serviced offsite
- 1.2.7 Person that authorized offsite service
- 1.2.8 Date/Time equipment was removed
- 1.2.9 Date/Time equipment was returned
- 1.2.10 Date/Time equipment was tested
- 1.2.11 Person(s) that performed the test

1.3 Elections equipment that needs to be serviced offsite must be approved before being removed. This information is documented as outlined in 1.2.

1.4 Localities test equipment and software after maintenance to verify security controls and functionality. Testing of equipment is documented on the service records in 1.2.

1.5 Equipment that is decommissioned must document the following:

- 1.5.1 Equipment decommissioned
- 1.5.2 Equipment Identification Number
- 1.5.3 Date/Time equipment decommissioned
- 1.5.4 Person(s) that decommissioned the equipment
- 1.5.5 Date/Time equipment was removed

1.6 Equipment that is decommissioned must have the following performed before being removed:

- 1.6.1 Any equipment media is sanitized as per NIST or COV guidelines
- 1.6.2 Equipment default settings are restored

2 Software Maintenance

2.1 Equipment running operating systems and/or software for elections must be updated regularly. Operating system and software should still be receiving security updates from the vendor.

2.2 Software/OS updates and diagnostic activities are approved and scheduled in accordance with Configuration Management policies.

3 Maintenance Documentation

3.1 Localities must ensure that contractors and vendors are taking appropriate measures to prevent the introduction of security vulnerabilities into their equipment. In addition to items addressed in GR 6 (Physical Security), localities must request and receive the following from vendors providing software and hardware for elections-systems.

3.1.1 Contractor/Vendors' security policies regarding their equipment and tools used to maintain the equipment.

3.1.2 Contracts that address data handling, reporting responsibilities in the event of a breach, termination conditions, necessary background checks, and remediation.

TECH 14 – SYSTEM AUDIT LOGS

PURPOSE

TECH 14 works to ensure essential system activity records are captured, reviewed, and preserved.

SCOPE

TECH 14 applies to all information systems identified as sensitive to election-related activities, individual components, services, and applications required to support those systems. Components include, but are not limited to: user productivity systems (laptops/desktops as similarly configured groups), application servers, mobile devices (with similar configurations), network peripherals (printers, scanner, etc.), network infrastructure (routers, switches, firewalls, intrusion detection systems, file servers, databases, system monitoring and security tools, etc.), and cloud assets.

MATURITY MATRIX

TECH 14 – System Audit Logs	Baseline	Preferred	Platinum
1. Audit Records: Auditable Events and Automated Alerts	1.1-1.2	All	All
2. Audit Records: Review, Analysis and Retention	2.1-2.2	All	All

1 Audit Records: Auditable Events and Automated Alerts

1.1 Event logging is enabled on all information systems and operating systems.
1.2 At minimum, the logs will include:
  1.2.1 The event
  1.2.2 The user ID associated with the event; and
  1.2.3 The time the event occurred
1.3 Whenever possible, all systems utilize Network Time Protocol (NTP) time synchronization.
1.4 Automated alerts are provided when log storage capacity reaches pre-defined levels (e.g. 50%, 80%, and 95%).

2 Audit Records: Review, Analysis and Retention

2.1 Audit records are backed up to a machine different than originating system on a quarterly basis.
2.2 Audit records are reviewed and analyzed every 30 days for inappropriate or unusual activity. Findings are reported using the Incident Response process.
2.3 Audit records, audit settings, and audit reports are protected from unauthorized access, modification, and deletion by setting appropriate access controls.
2.4 Retain audit records consistent with State and Local retention policies, to provide support for after-the-fact investigations of security incidents.

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Public Comment

BOARD WORKING PAPERS

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Closed Session

BOARD WORKING PAPERS