★ VIRGINIA ★
STATE BOARD of ELECTIONS

BOARD MEETING

Monday, November 15, 2021
Virginia State Capitol
Senate Room 3

Video and Teleconference

Videoconference:

https://covaconf.webex.com/covaconf/j.php?MTID=m87554d976f56f557b4b9748eb08b7217

Meeting password: nsWphpNG428

Teleconference:

1-517-466-2023 US Toll

1-866-692-4530 US Toll-Free

Access Code: 178 049 5918

Richmond, VA

1:00 P.M.

STATE BOARD OF ELECTIONS
AGENDA

***DATE*: Monday, November 15, 2021**
***LOCATION:* Virginia State Capitol – Senate Room 3**
1000 Bank St.
Richmond, VA 23218
TELECONFERENCE:
+1-517-466-2023 US Toll
+1-866-692-4530 US Toll Free
Access code: 178 049 5918
VIDEO CONFERENCE:
https://covaconf.webex.com/covaconf/j.php?MTID=m87554d976f56f557b4b9748eb08b7217
Password: nsWphpNG428
***TIME*: 1:00 P.M.**

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

II. APPROVAL OF MINUTES — *Jamilah LeCruise, Secretary*
A. September 14, 2021

III. COMMISSIONER'S REPORT — *Christopher E. Piper, Commissioner*

IV. CERTIFICATION OF GENERAL ELECTION – NOVEMBER 2, 2021 — *Paul Saunders, Elections Administration Supervisor*

V. CHARLES CITY COUNTY ELECTORAL BOARD/REGISTRAR — *David Nichols, Elections Administration Manager*

VI. 2021 PERIODIC REVIEW OF REGULATIONS — *Ashley Coles, ELECT Policy Analyst*

VII. ANNUAL SECURITY STANDARDS REVIEW VA. CODE § 24.2-410.2 — *Karen Hoyt-Stewart, Locality Security Program Manager*

VIII. PUBLIC COMMENT

IX. CLOSED SESSION

X. ADJOURNMENT

NOTE: https://townhall.virginia.gov/L/ViewMeeting.cfm?MeetingID=31941

Re. Entrance to the Virginia State Capitol
All members of the public will be required to show his/her driver's license, passport or other government issued ID to enter the Capitol. Each person will go through the x-ray machine and follow the Expect the Check rules.

All State employees must have on his/her state ID badge on at all times while in the Capitol. Each employee will go through the x-ray machine and follow the Expect the Check rules.

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. 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
Secretary LeCruise

State Board of Elections
Tuesday, September 14, 2021
FINAL Meeting Minutes

The State Board of Elections ("the Board") meeting was held on Tuesday, September 14, 2021, in Senate Room 3 of the Virginia State Capitol. The meeting was also conducted electronically so the public could view and hear the meeting. In attendance: Robert Brink, Chairman, John O'Bannon, Vice Chairman, Jamilah LeCruise, Secretary, Angela Chiang, and Delegate Donald Merricks, represented the State Board of Elections ("the Board"). Christopher E. "Chris" Piper, Commissioner, represented the Department of Elections ("ELECT") and Carol Lewis represented the Office of the Attorney General ("OAG"). Chairman Brink called the meeting to order at 1:36 P.M.

The first item of business was the approval of minutes presented by Secretary LeCruise. Chairman Brink *moved that the Board approve the minutes from the August 3, 2021 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The next item of business was the Commissioner's Report presented by Commissioner Piper. The Commissioner expressed his deepest sympathy on the unexpected passing of Rodrick "Rod" Wimbley, IT Help Desk contractor with ELECT. Commissioner Piper stated that Mr. Wimbley was an upbeat and positive person who will be greatly missed.

The Commissioner informed the Board that the local General Registrars ("GRs") and

ELECT have received an increase in Freedom of Information Act ("FOIA") and National Voter Registration Act ("NVRA") requests. Commissioner Piper advised the Board that Ashley Coles, FOIA Officer/ELECT Policy Analyst, and the ELECTs training team are working to provide guidance to the local registrars. The Commissioner informed the Board that ELECT's list maintenance program has been recognized nationally for the accuracy of Virginia's voter registration lists. Commissioner Piper stated that ELECT has been a part of the Electronic Registration Information Center ("ERIC") since 2014. The Commissioner advised the Board that ELECT receives monthly updates from the Virginia State Police, and the Bureau of Vital Statistics master death file to ensure the voter list is accurate and up-to-date.

Commissioner Piper informed the Board that ELECT also works with the Secretary of the Commonwealth's office on restoration of rights for Virginians who were convicted of felonies and now seek to restore their right to vote. The Commissioner stated that ELECT works closely with those groups to ensure voters who are eligible and registered are on the list and voters who are ineligible are removed from the list, in compliance with Federal and State laws. Commissioner Piper advised the Board that ELECT is close to finalizing the Statewide Voter Registration System's Request for Proposals ("RFP") applications. The Commissioner stated that ELECT is going through a thorough process to ensure to invest in the best system for the Commonwealth, the localities, and the Department.

Commissioner Piper advised the Board that it is National Disability Voter Registration Week. The Commissioner also stated that the Office of the Governor produced the One Virginia Plan that focuses on diversity, equity, and inclusion which includes the disabled community. Commissioner Piper informed the Board that ELECT recently did a presentation on disability access to voter registration and voting. The Commissioner informed the Board that the 2020

General Assembly passed a law to assist visually disabled or print disabled voters who under previous law allowed an "assistant" to mark the ballot on behalf of a voter with visual or print disabilities. Commissioner Piper stated that now, visually disabled or print disabled voters will be able to request a ballot that can be marked with a specific tool allowing them to vote privately and independently in the comfort of their own home.

The Commissioner advised the Board that 45-day early voting starts on September 17, 2021, September 28, 2021, is National Voter Registration Day, and October 12, 2021, is the last day to register to vote. Commissioner Piper stated the General Assembly approved 3 million dollars in grants to the localities for early voting expansion. The Commissioner stated that information was sent to the localities about the required criteria to apply for the grant and applications have been received. Commissioner Piper informed the Board that the deadline to submit the applications was Friday, September 10, 2021, and they are currently being reviewed. The Commissioner informed the Board that the General Assembly appropriated $1.5 million for ELECT's Voter Education and Outreach, in addition to $300,000 provided as part of the Voting Rights Act that was passed earlier this year. Commissioner Piper presented the Voter Education and Outreach Plan to the Board. *This PowerPoint Presentation is in the Working Papers for the September 14, 2021 meeting.*

The Commissioner stated that during the 2021 Legislative Session the General Assembly requested changes to election night reporting. Commissioner Piper informed the Board that absentee by mail voting will be reported separately from early voting in-person. The Commissioner stated that there will be one count for ballots returned by mail and one count for ballots cast in-person prior to Election Day. Commissioner Piper advised the Board that ELECT will be releasing a report on how to best implement precinct-by-precinct reporting for absentee

ballots. The Commissioner also stated that absentee ballots submitted by eligible voters will be counted if postmarked by Election Day and received in the GR's office by noon on Friday, November 5th. Commissioner Piper informed the Board that the General Assembly also required GRs to pre-process and report on absentee ballots during the week preceding the election. However, the Commissioner advised the Board that vote totals cannot be tabulated until the polls close on November 2nd.

The next item of business was the consideration of Stand By Your Ad violations, presented by Tammy Alexander, Campaign Finance Compliance and Training Specialist. The first penalty assessed was against Dana Sally-Allen for Richmond School Board 8th District for one flyer without a disclosure. Mrs. Alexander stated that the Board assessed a $25 penalty. Vice Chair O'Bannon moved *to adopt the previously assessed $25 penalty against Dana Sally-Allen with regards to one flyer.* Secretary LeCruise seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The second penalty was against Hampton Roads Black Caucus for one piece of literature without a disclosure. Mrs. Alexander stated that the Board previously assessed a $50 penalty. Vice Chair O'Bannon moved *to adopt the previously assessed $50 penalty against Hampton Roads Black Caucus with regards to one piece of literature*. 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The third penalty was against Mr. Linnard Harris for two yard signs without a disclosure. Mrs. Alexander stated that the Board previously assessed a $400 penalty. Vice Chair O'Bannon moved *to adopt the previously assessed $400 penalty against Linnard Harris for two yard signs.* 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The fourth penalty was against Regie Ford for one door hanger and two yard signs without a disclosure. Mrs. Alexander stated that the Board previously assessed a $75 penalty. Secretary LeCruise moved *to adopt the previously assessed $75 penalty against Regie Ford for one door hanger and two yard signs.* 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The fifth penalty was against Glenn Youngkin for one t-shirt without a disclosure. Mrs. Alexander stated that the Board previously assessed a $100 penalty. Vice Chair O'Bannon moved *to adopt the previously assessed $100 penalty against Glenn Youngkin for one t-shirt.* 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The next item of business was the Ranked Choice Voting Regulations and Supporting Documents presented by Samantha Buckley, ELECT Policy Analyst. Chairman Brink informed the Board that the Ranked Choice Voting Regulation was presented during the June 22nd Board meeting and placed on Town Hall for public comment. *This memo is in the Working Papers for the September 14, 2021 meeting.* Chairman Brink opened the floor to public comment. Chris Hughes, Policy Director at Ranked Choice Voting Resource Center, and Chris Lavarn, Senior Legal Counselor with the Campaign Legal Center ("CLC") addressed the Board. Secretary LeCruise moved *to set the number of allowable candidate rankings at 10*. 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

Vice Chair O'Bannon moved *that the Board adopt the Department's proposal for ranked choice voting regulations and ballot standards*. Secretary LeCruise seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The next item of business was the Hampton Electoral Board Request for Electronic Pollbook Certification Extension presented by Karen Hoyt-Stewart, Voting Technology Program Manager. *This memo is in the Working Papers for the September 14, 2021 meeting.* Vice Chair O'Bannon moved *to grant a limited extension for the ExpressPoll 5000 3.2.0.0 certified version of electronic pollbooks; the extension will expire when the locality secures a certified system, or July 31, 2022, whichever occurs first.* Secretary LeCruise seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The next item of business was the Designation of Minority Languages Status for Fairfax

County presented by Samantha Buckley, ELECT Policy Analyst. *This memo is in the Working Papers for the September 14, 2021 meeting.* Secretary LeCruise moved *that the State Board of Elections designate Fairfax County, VA as a covered locality pursuant to Va. Code § 24.2-128. Moving forward, Fairfax County will be required to provide any English language voting or election materials, as defined by Va. Code § 24.2-128, in Spanish and Vietnamese languages.* 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 LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

The next item of business was the Revision to the Hand-counting Ballot Standards presented by Samantha Buckley, ELECT Policy Analyst. *This memo is in the Working Papers for the September 14, 2021 meeting.* Chairman Brink opened the floor to public comment. Chris Marston, Republican Party of Virginia, and Barbara Tabb, President, Virginia Electoral Board Association ("VEBA") addressed the Board. Delegate Merricks moved *that the State Board of Elections adopt, and make effective immediately, the proposed revisions to the Hand-counting Ballot Standards.* Secretary LeCruise seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman Brink – Aye

Vice Chair O'Bannon – Aye

Secretary LeCruise – Aye

Ms. Chiang – Aye

Delegate Merricks – Aye

Chairman Brink opened the floor to public comment. No public comment was given. Secretary LeCruise moved to adjourn the meeting. Ms. Chiang seconded the motion and the motion passed unanimously.

The meeting adjourned at approximately 3:14 P.M.

_____
Chairman

_____
Vice Chairman

_____
Secretary

_____
Board Member

_____
Board Member

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Commissioner's Report

BOARD WORKING PAPERS
Christopher Piper
Commissioner

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Certification of General Election – November 2, 2021

BOARD WORKING PAPERS
Paul Saunders
Elections Administration Supervisor

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Certification
Of
General Election
November 2, 2021

BOARD WORKING PAPERS
Paul G. Saunders, III
Elections Administration Supervisor

★ VIRGINIA ★
DEPARTMENT of ELECTIONS

Memorandum

To: Chairman Brink, Vice Chair O'Bannon, Secretary LeCruise, Delegate Merricks, Ms. Chiang

From: Paul G. Saunders, III, Elections Administration Supervisor

Date: November 15, 2021

Re: Certification of Results for the November 2, 2021 General Election

Applicable Code Sections:

- Va. Code § 24.2-679.A. "The State Board shall meet on the third Monday in November to ascertain the results of the November election."
- Va. Code § 24.2-680 "Subject to the requirements of § 24.2-948.2, the State Board shall without delay complete and transmit to each of the persons declared to be elected a certificate of his election, certified by it under its seal of office."

Background:

- Upon completion of the election, local general registrars (GRs) entered all relevant election data into the Virginia Election and Registration System (VERIS).
- In accordance with Va. Code § 24.2-671, within seven days after the election, local electoral boards conducted provisional ballot meetings and canvasses to ascertain and certify election results for their localities.
- Upon completion of canvass the GRs forwarded their localities certified Abstracts of Votes (Abstracts) and, when applicable, Write-In Certifications, to the Department of Elections (ELECT).
- Upon receipt of the localities Abstracts and Write-In Certifications, to ensure accuracy and completion, ELECT staff:
    - Confirmed all required Abstracts and Write-In Certifications were completed and submitted.
    - Ran Turnout vs. Votes Cast reports and asked localities to resolve and/or explain any issues identified.
    - Compared the results listed in the Abstracts and Write-In Certifications to the results entered in VERIS to ensure accuracy.

1100 Bank Street
Washington Building – First Floor
Richmond, VA 23219-3947
elections.virginia.gov

Toll Free: (800) 552-9745
TDD: (800) 260-3466
info@elections.virginia.gov

Suggested Motion:

"After reviewing the Abstracts of Votes Cast in the 2021 November General Election, I move that the Board certify the statements to be correct and sign the statements and certificates of election."

Offices certified by the State Board of Elections: The 2021 November General Election included races for Governor, Lieutenant Governor and Attorney General as well as all 100 District Representatives in the House of Delegates, the results of which must be endorsed and subscribed on a certified statement from the State Board of Elections. § 24.2-679.

The offices certified by the State Board of Elections are:

I. Governor

Glenn A. Youngkin	**Winner**
Terry R. McAuliffe	
Princess L. Blanding	

Elected by votes cast in all 133 cities and counties in Virginia.

II. Lieutenant Governor

Winsome E. Sears	**Winner**
Hala S. Ayala	

Elected by votes cast in all 133 cities and counties in Virginia.

III. Attorney General

Jason S. Miyares	**Winner**
Mark R. Herring	

Elected by votes cast in all 133 cities and counties in Virginia.

1. **Member House of Delegates, District One**

Terry G. Kilgore	**Winner**

Elected by votes cast in:

NORTON CITY
SCOTT COUNTY
WISE COUNTY
LEE COUNTY

2. **Member House of Delegates, District Two**

Gina R. Ciarcia	
Candi P. M. King	**Winner**

Elected by votes cast in:

PRINCE WILLIAM COUNTY
STAFFORD COUNTY

3. **Member House of Delegates, District Three**

James W."Will" Morefield	**Winner**

Elected by votes cast in:

BLAND COUNTY
BUCHANAN COUNTY
RUSSELL COUNTY
TAZEWELL COUNTY

4. **Member House of Delegates, District Four**

William C. Wampler III	**Winner**

Elected by votes cast in:

DICKENSON COUNTY
WISE COUNTY
RUSSELL COUNTY
WASHINGTON COUNTY

5. **Member House of Delegates, District Five**

Israel D. O'Quinn	**Winner**

Elected by votes cast in:

GALAX CITY
BRISTOL CITY
GRAYSON COUNTY
SMYTH COUNTY
WASHINGTON COUNTY

6. Member House of Delegates, District Six

Jeffrey L. Campbell	**Winner**

Elected by votes cast in:

CARROLL COUNTY
SMYTH COUNTY
WYTHE COUNTY

7. Member House of Delegates, District Seven

Marie E. March	**Winner**
Derek W. Kitts	

Elected by votes cast in:

FLOYD COUNTY
PULASKI COUNTY
MONTGOMERY COUNTY

8. Member House of Delegates, District Eight

Joseph P. "Joe" McNamara	**Winner**
Dustin M. Wimbish	

Elected by votes cast in:

ROANOKE COUNTY
MONTGOMERY COUNTY
SALEM CITY
CRAIG COUNTY

9. Member House of Delegates, Ninth District

Wren M. Williams	**Winner**
Bridgette N. Craighead	

Elected by votes cast in:

PATRICK COUNTY
HENRY COUNTY
FRANKLIN COUNTY

10. Member House of Delegates, Tenth District

Nicholas S. "Nick" Clemente	
Wendy W. Gooditis	**Winner**

Elected by votes cast in:

FREDERICK COUNTY
CLARKE COUNTY
LOUDOUN COUNTY

11. Member House of Delegates, Eleventh District

Charlie H. Nave	
S. "Sam" Rasoul	**Winner**

Elected by votes cast in:

ROANOKE CITY

12. Member House of Delegates, District Twelve

Jason S. Ballard	**Winner**
Chris L. Hurst	

Elected by votes cast in:

RADFORD CITY
MONTGOMERY COUNTY
PULASKI COUNTY
GILES COUNTY

13. Member House of Delegates, Thirteenth District

Christopher M. Stone	
Danica A. Roem	**Winner**

Elected by votes cast in:

MANASSAS PARK CITY
PRINCE WILLIAM COUNTY

14. Member House of Delegates, Fourteenth District

D.W. "Danny" Marshall III	**Winner**
S.M. "Rhett" Deitz	

Elected by votes cast in:

DANVILLE CITY
PITTSYLVANIA COUNTY
HENRY COUNTY

15. Member House of Delegates, Fifteenth District

C. Todd Gilbert	**Winner**
Emily G. Scott	

Elected by votes cast in:

ROCKINGHAM COUNTY
SHENANDOAH COUNTY
WARREN COUNTY
PAGE COUNTY

16. Member House of Delegates, Sixteenth District

Les R. Adams	**Winner**
Chance B. Trevillian	

Elected by votes cast in:

MARTINSVILLE CITY
HENRY COUNTY
PITTSYLVANIA COUNTY

17. Member House of Delegates, Seventeenth District

Christopher T. Head	**Winner**

Elected by votes cast in:

ROANOKE COUNTY
BOTETOURT COUNTY
ROANOKE CITY

18. Member House of Delegates, Eighteenth District

Michael J. Webert	**Winner**
Douglas J. Ward	

Elected by votes cast in:

RAPPAHANNOCK COUNTY
CULPEPER COUNTY
FAUQUIER COUNTY
WARREN COUNTY

19. Member House of Delegates, Nineteenth District

Terry L. Austin	**Winner**
Wendy S. Rowden	
Dean D. Davison	

Elected by votes cast in:

COVINGTON CITY
BEDFORD CITY
BOTETOURT COUNTY
ALLEGHANY COUNTY
BEDFORD COUNTY

20. Member House of Delegates, Twentieth District

G. "John" Avoli	**Winner**
Randall K. Wolf	

Elected by votes cast in:

AUGUSTA COUNTY
STAUNTON CITY
NELSON COUNTY
HIGHLAND COUNTY
WAYNESBORO CITY

21. Member House of Delegates, Twenty-First District

Tanya M. Gould	
Kelly K. Convirs-Fowler	**Winner**

Elected by votes cast in:

VIRGINIA BEACH CITY
CHESAPEAKE CITY

22. Member House of Delegates, Twenty-Second District

Kathy J. Byron	**Winner**
Gregory K. "Greg" Eaton	
Sarah R. Jerose	

Elected by votes cast in:

CAMPBELL COUNTY
FRANKLIN COUNTY
LYNCHBURG CITY
BEDFORD COUNTY

23. Member House of Delegates, Twenty-Third District

Wendell S. Walker	**Winner**
Natalie A. Short	

Elected by votes cast in:

LYNCHBURG CITY
AMHERST COUNTY
BEDFORD COUNTY

24. Member House of Delegates, Twenty-Fourth District

Ronnie R. Campbell	**Winner**
Sam R. Soghor	

Elected by votes cast in:

BUENA VISTA CITY
LEXINGTON CITY
BATH COUNTY
AMHERST COUNTY
AUGUSTA COUNTY
ROCKBRIDGE COUNTY

25. Member House of Delegates, Twenty-Fifth District

Chris S. Runion	**Winner**
Jennifer L. Kitchen	

Elected by votes cast in

ROCKINGHAM COUNTY
ALBEMARLE COUNTY
AUGUSTA COUNTY

26. Member House of Delegates, Twenty-Sixth District

Tony O. Wilt	**Winner**
William W. “Bill” Helsley	

Elected by votes cast in:

ROCKINGHAM COUNTY HARRISONBURG CITY

27. Member House of Delegates, Twenty-Seventh District

Roxann L. Robinson	**Winner**
Debra D. Gardner	

Elected by votes cast in:

CHESTERFIELD COUNTY RICHMOND CITY

28. Member House of Delegates, Twenty-Eighth District

Tara A. Durant	**Winner**
Joshua G. Cole	

Elected by votes cast in:

FREDERICKSBURG CITY STAFFORD COUNTY

29. Member House of Delegates, Twenty-Ninth District

William D. “Bill” Wiley	**Winner**
Delmara F. “Deetzie” Bayliss	

Elected by votes cast in:

WINCHESTER CITY FREDERICK COUNTY
WARREN COUNTY

30. Member House of Delegates, Thirtieth District

Nick J. Freitas	**Winner**
Annette H. Hyde	

Elected by votes cast in:

MADISON COUNTY ORANGE COUNTY
CULPEPER COUNTY

31. Member House of Delegates, Thirty-First District

Benjamin W. "Ben" Baldwin	
Elizabeth R. Guzman	**Winner**

Elected by votes cast in:

FAUQUIER COUNTY

PRINCE WILLIAM COUNTY

32. Member House of Delegates, Thirty-Second District

H. Scott Pio	
David A. Reid	**Winner**
Nick M. Allegro	

Elected by votes cast in:

LOUDOUN COUNTY

33. Member House of Delegates, Thirty-Third District

Dave A. LaRock	**Winner**
Paul W. Siker	

Elected by votes cast in:

FREDERICK COUNTY

CLARKE COUNTY

LOUDOUN COUNTY

34. Member House of Delegates, Thirty-Fourth District

Gary G. Pan	
Kathleen J. Murphy	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

LOUDOUN COUNTY

35. Member House of Delegates, Thirty-Fifth District

Kevin E. McGrath	
Mark L. Keam	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

36. Member House of Delegates, Thirty-Sixth District

Matthew J. Lang	
Kenneth R. "Ken" Plum	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

37. Member House of Delegates, Thirty-Seventh District

Kenny W. Meteiver	
David L. Bulova	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY FAIRFAX CITY

38. Member House of Delegates, Thirty-Eighth District

Tom L. Pafford	
L. Kaye Kory	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

39. Member House of Delegates, Thirty-Ninth District

Maureen T. Brody	
Vivian E. Watts	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

40. Member House of Delegates, Fortieth District

Harold Y. Pyon	
Dan I. Helmer	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY PRINCE WILLIAM COUNTY

41. Member House of Delegates, Forty-First District

John M. Wolfe	
Eileen Filler-Corn	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

42. Member House of Delegates, Forty-Second District

Edward F. McGovern	
Kathy K. "KL" Tran	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

43. Member House of Delegates, Forty-Third District

Brenton H. Hammond	
Mark D. Sickles	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

44. Member House of Delegates, Forty-Forth District

Richard T. Hayden	
Paul E. Krizek	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

45. Member House of Delegates, Forty-Fifth District

Justin D. "J.D." Maddox	
Elizabeth B. Bennett-Parker	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

ALEXANDRIA CITY

ARLINGTON COUNTY

46. Member House of Delegates, Forty-Sixth District

Charniele L. Herring	**Winner**

Elected by votes cast in:

ALEXANDRIA CITY

47. Member House of Delegates, Forty-Seventh District

Laura A. Hall	
Patrick A. Hope	**Winner**

Elected by votes cast in:

ARLINGTON COUNTY

48. Member House of Delegates, Forty-Eighth District

Edward William Monroe, Jr.	
Richard C. "Rip" Sullivan, Jr.	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY ARLINGTON COUNTY

49. Member House of Delegates, Forty-Ninth District

Timothy E. Kilcullen	
Alfonso H. Lopez	**Winner**
Terry W. Modglin	

Elected by votes cast in:

FAIRFAX COUNTY ARLINGTON COUNTY

50. Member House of Delegates, Fiftieth District

Steve T. "Dr Steve" Pleickhardt	
Michelle E. Lopes-Maldonado	**Winner**

Elected by votes cast in:

PRINCE WILLIAM COUNTY MANASSAS CITY

51. Member House of Delegates, Fifty-First District

Tim D. Cox	
Briana D. Sewell	**Winner**

Elected by votes cast in:

PRINCE WILLIAM COUNTY

52. Member House of Delegates, Fifty-Second District

Maria E. Martin	
Luke E. Torian	**Winner**

Elected by votes cast in:

PRINCE WILLIAM COUNTY

53. Member House of Delegates, Fifty-Third District

Sarah White	
Marcus B. Simon	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY
FALLS CHURCH CITY

54. Member House of Delegates, Fifty-Fourth District

Robert D. "Bobby" Orrock, Sr.	**Winner**
Eric M. Butterworth	

Elected by votes cast in:

CAROLINE COUNTY
SPOTSYLVANIA COUNTY

55. Member House of Delegates, Fifty-Fifth District

H.F. "Buddy" Fowler, Jr.	**Winner**
Rachel A. Levy	

Elected by votes cast in:

CAROLINE COUNTY
HANOVER COUNTY
SPOTSYLVANIA COUNTY

56. Member House of Delegates, Fifty-Sixth District

John J. McGuire III	**Winner**
Blakely K. Lockhart	

Elected by votes cast in:

GOOCHLAND COUNTY
LOUISA COUNTY
SPOTSYLVANIA COUNTY
HENRICO COUNTY

57. Member House of Delegates, Fifty-Seventh District

Philip Andrew Hamilton	
Sally L. Hudson	**Winner**

Elected by votes cast in:

CHARLOTTESVILLE CITY
ALBEMARLE COUNTY

58. Member House of Delegates, Fifty-Eighth District

Robert Bernard Bell, III	**Winner**
Sara H. Ratcliffe	

Elected by votes cast in:

ROCKINGHAM COUNTY
GREENE COUNTY
ALBEMARLE COUNTY
FLUVANA COUNTY

59. Member House of Delegates, Fifty-Ninth District

C. Matt Fariss	**Winner**
Benjamin A. Moses	
Louis V. Scicli	

Elected by votes cast in:

CAMPBELL COUNTY
APPOMATTOX COUNTY
BUCKINGHAM COUNTY
ALBEMARLE COUNTY
NELSON COUNTY

60. Member House of Delegates, Sixtieth District

James E. Edmunds II	**Winner**

Elected by votes cast in:

CAMPBELL COUNTY
CHARLOTTE COUNTY
HALIFAX COUNTY
PRINCE EDWARD COUNTY

61. Member House of Delegates, Sixty-First District

Thomas C. Wright Jr.	**Winner**
Trudy Bell Berry	
Joe J. “Joey” Paschal	

Elected by votes cast in:

CUMBERLAND COUNTY
NOTTOWAY COUNTY
MECKLENBURG COUNTY
LUNENBURG COUNTY
AMELIA COUNTY

62. Member House of Delegates, Sixty-Second District

Carrie Emerson Coyner	**Winner**
Jasmine E. Gore	

Elected by votes cast in:

PRINCE GEORGE COUNTY
CHESTERFIELD COUNTY
HOPEWELL CITY

63. Member House of Delegates, Sixty-Third District

Kim A. Taylor	**Winner**
Lashrecse D. Aird	

Elected by votes cast in:

DINWIDDIE COUNTY
PETERSBURG CITY
PRINCE GEORGE COUNTY
CHESTERFIELD COUNTY

64. Member House of Delegates, Sixty-Fourth District

Emily M. Brewer	**Winner**
Michael H. Drewry	

Elected by votes cast in:

SUFFOLK COUNTY
PRINCE GEORGE COUNTY
SURRY COUNTY
ISLE OF WIGHT COUNTY

65. Member House of Delegates, Sixty-Fifth District

R. Lee Ware Jr.	**Winner**
Caitlin A. Coakley	

Elected by votes cast in:

GOOCHLAND COUNTY
POWHATAN COUNTY
LOUISA COUNTY
CHESTERFIELD COUNTY
FLUVANNA COUNTY

66. Member House of Delegates, Sixty-Sixth District

Mike A. Cherry	**Winner**
Katie A. Sponsler	

Elected by votes cast in:

COLONIAL HEIGHTS CITY
CHESTERFIELD COUNTY
RICHMOND CITY

67. Member House of Delegates, Sixty-Seventh District

Bob L. Frizzelle	
Karrie K. Delaney	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY

LOUDOUN COUNTY

68. Member House of Delegates, Sixty-Eighth District

Mark L. Earley, Jr.	
Dawn Marie Adams	**Winner**

Elected by votes cast in:

CHESTERFIELD COUNTY

HENRICO COUNTY

RICHMOND CITY

69. Member House of Delegates, Sixty-Ninth District

Shelia M. Furey	
Betsy B. Carr	**Winner**

Elected by votes cast in:

RICHMOND CITY

70. Member House of Delegates, Seventieth District

Delores L. McQuinn	**Winner**
David B. Vaught	

Elected by votes cast in:

CHARLES CITY COUNTY

CHESTERFIELD COUNTY

RICHMOND CITY

HENRICO COUNTY

71. Member House of Delegates, Seventy-First District

Nancye A. Hunter	
Jeffrey M. Bourne	**Winner**

Elected by votes cast in:

RICHMOND CITY

72. Member House of Delegates, Seventy-Second District

Christopher T. Holmes	
Schuyler T. VanValkenburg	**Winner**

Elected by votes cast in:

HENRICO COUNTY

73. Member House of Delegates, Seventy-Third District

Mary Margaret Kastelberg	
Rodney T. Willett	**Winner**

Elected by votes cast in:

RICHMOND CITY
HENRICO COUNTY

74. Member House of Delegates, Seventy-Fourth District

James L. "Jimmy" Brooks	
Lamont Bagby	**Winner**

Elected by votes cast in:

RICHMOND CITY
HENRICO COUNTY

75. Member House of Delegates, Seventy-Fifth District

H. Otto Wachsmann, Jr.	**Winner**
Roslyn C. Tyler	

Elected by votes cast in:

GREENSVILLE COUNTY
LUNENBURG COUNTY
FRANKLIN CITY
EMPORIA CITY
SUSSEX COUNTY
BRUNSWICK COUNTY
SOUTHAMPTON COUNTY

76. Member House of Delegates, Seventy-Sixth District

Michael J. Dillender, Sr.	
Clinton L. Jenkins	**Winner**
Craig L. Warren	

Elected by votes cast in:

SUFFOLK CITY
CHESAPEAKE CITY

77. Member House of Delegates, Seventy-Seventh District

Geoffrey R. Burke	
C.E. "Cliff" Hayes Jr.	**Winner**

Elected by votes cast in:

VIRGINIA BEACH CITY
CHESAPEAKE CITY

78. Member House of Delegates, Seventy-Eighth District

James A. "Jay" Leftwich, Jr.	**Winner**
Melanie L. Cornelisse	

Elected by votes cast in:

CHESAPEAKE CITY

79. Member House of Delegates, Seventy-Ninth District

Lawrence J. Mason	
Nadarius E. Clark	**Winner**

Elected by votes cast in:

NORFOLK CITY
CHESAPEAKE CITY
PORTSMOUTH CITY

80. Member House of Delegates, Eightieth District

Deanna R. Stanton	
Don L. Scott Jr.	**Winner**

Elected by votes cast in:

PORTSMOUTH CITY

81. Member House of Delegates, Eighty-First District

Barry D. Knight	**Winner**
Jeffrey A. "Doc" Feld	

Elected by votes cast in:

VIRGINIA BEACH CITY
CHESAPEAKE CITY

82. Member House of Delegates, Eighty-Second District

Anne Ferrell Tata	**Winner**
Scott J. Flax	

Elected by votes cast in:

VIRGINIA BEACH CITY

83. Member House of Delegates, Eighty-Third District

Timothy V. Anderson	**Winner**
Nancy D. Guy	

Elected by votes cast in:

NORFOLK CITY
VIRGINIA BEACH CITY

84. Member House of Delegates, Eighty-Fourth District

Glenn R. Davis Jr.	**Winner**
Kimberly A. Melnyk	

Elected by votes cast in:

VIRGINIA BEACH CITY

85. Member House of Delegates, Eighty-Fifth District

Karen S. Greenhalgh	**Winner**
Alex Q. Askew	

Elected by votes cast in:

VIRGINIA BEACH CITY

86. Member House of Delegates, Eighty-Sixth District

Julie Anna Perry	
Irene Shin	**Winner**

Elected by votes cast in:

FAIRFAX COUNTY
LOUDOUN COUNTY

87. Member House of Delegates, Eighty-Seventh District

Gregory J. Moulthrop	
Suhas Subramanyam	**Winner**

Elected by votes cast in:

PRINCE WILLIAM COUNTY
LOUDOUN COUNTY

88. Member House of Delegates, Eighty-Eighth District

Phillip A. "Phil" Scott	**Winner**
Kecia S. Evans	
Timothy M. Lewis	

Elected by votes cast in:

FAUQUIER COUNTY
FREDERICKSBURG CITY
SPOTSYLVANIA COUNTY
STAFFORD COUNTY

89. Member House of Delegates, Eighty-Ninth District

Hahns L. Copeland	
Jerrauld C. "Jay" Jones	**Winner**

Elected by votes cast in:

NORFOLK CITY

90. Member House of Delegates, Ninetieth District

Sylvia M. Bryant	
Angelia Williams Graves	**Winner**

Elected by votes cast in:

NORFOLK CITY
VIRGINIA BEACH CITY

91. Member House of Delegates, Ninety-First District

A.C. Cordoza	**Winner**
Martha M. Mugler	
Charles T. West IV	

Elected by votes cast in:

POQUOSON CITY
YORK COUNTY
HAMPTON CITY

92. Member House of Delegates, Ninety-Second District

Benjamin J. Siff	
Jeion A. Ward	**Winner**

Elected by votes cast in:

NEWPORT NEWS CITY
HAMPTON CITY

93. Member House of Delegates, Ninety-Third District

Jordan M. Gray	
Michael P. "Mike" Mullin	**Winner**

Elected by votes cast in:

NEWPORT NEWS CITY
JAMES CITY COUNTY
WILLIAMSBURG CITY
YORK COUNTY

94. Member House of Delegates, Ninety-Fourth District

C. Russ Harper	
Shelly A. Simonds	**Winner**

Elected by votes cast in:

NEWPORT NEWS CITY

95. Member House of Delegates, Ninety-Fifth District

David G. Wilson	
Marcia S. "Cia" Price	**Winner**

Elected by votes cast in:

NEWPORT NEWS CITY
HAMPTON CITY

96. Member House of Delegates, Ninety-Sixth District

Amanda E. Batten	**Winner**

Mark C. Downey	

Elected by votes cast in:

JAMES CITY COUNTY
YORK COUNTY

97. Member House of Delegates, Ninety-Seventh District

Scott A. Wyatt	**Winner**
R. Stanton "Stan" Scott	

Elected by votes cast in:

NEW KENT COUNTY
HANOVER COUNTY
KING WILLIAM COUNTY

98. Member House of Delegates, Ninety-Eighth District

M. Keith Hodges	**Winner**
E.B. "Ella" Webster	

Elected by votes cast in:

KING AND QUEEN COUNTY
MIDDLESEX COUNTY
KING WILLIAM COUNTY
ESSEX COUNTY
GLOUCESTER COUNTY
MATHEWS COUNTY

99. Member House of Delegates, Ninety-Ninth District

Margaret Bevans Ransone	**Winner**
Linwood T. Blizzard II	

Elected by votes cast in:

LANCASTER COUNTY
NORTHUMBERLAND COUNTY
CAROLINE COUNTY
RICHMOND COUNTY
KING GEORGE COUNTY
WESTMORELAND COUNTY

100. Member House of Delegates, One Hundredth District

Robert S. Bloxom Jr.	**Winner**
Finale M. Norton	

Elected by votes cast in:

NORFOLK CITY
NORTHAMPTON COUNTY
ACCOMACK COUNTY

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Charles City County Electoral Board/Registrar

BOARD WORKING PAPERS
David Nichols
Elections Administration Manager

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Memorandum

To: Chairman Brink, Vice Chair O'Bannon, Secretary LeCruise, Del. Merricks, and Ms. Chiang

From: Dave Nichols, Elections Services Manager

Date: November 15, 2021

Re: Early Voting and Charles City County

Background:
Pursuant to VA Code § 24.2-701.1, "Absentee voting in person shall be available on the forty-fifth day prior to any election…." For the November 2021 General and Special Elections, the forty-fifth day prior was Saturday, September 18, 2021. Most local elections offices are closed on Saturdays that far out from Election Day and choose to start absentee voting in person (early voting) on the Friday before. In this case, that date was Friday, September 17, 2021. This timing was anticipated to be the case for Charles City County.

On Thursday, September 16, 2021, I received a communication from one of ELECT's Registrar Liaisons that there were interpersonal problems in Charles City County between the General Registrar (GR) and certain other employees of the county. Details were not forthcoming, but I was given the impression that these interpersonal problems were quite serious. Because ELECT does not control employee or human resource issues at a local level, I advised the Liaison to keep me apprised if there were further developments.

On the morning of Friday, September 17, 2021, I was again contacted by a Liaison who informed me that the Charles City County GR was either resigning or had resigned, and that the office was not open for early voting. Staff was able to confirm that the GR's office was not open, and I alerted agency leadership.

I was able to make contact by phone with the Charles City County GR later that morning. She confirmed that both she and her assistant registrar were in the office, but that the doors remained locked, no voters were being allowed in, and they were packing their personal belongings. I repeatedly asked the GR if she had resigned. The only answer she would provide was that she had told "them" she would resign unless a particular individual who also worked for the locality was terminated. She would not answer the question of whether or not she was still the General Registrar. She refused to open the office and stated that she was quitting to keep herself "safe." There are unconfirmed reports that voters were turned away during the period in which the GR and her assistant were in the office.

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

ELECT had made contact with the Chair of the Charles City County Electoral Board. After several phone calls, all were determined to have the office open for early voting on Saturday, September 18, 2021, thereby meeting the requirement of Va. Code § 24.2-701.1.

ELECT staff worked for the remainder of the day to find individuals who would be willing and able to open the Charles City County office the next day. Ultimately, two ELECT staff, Garry Ellis and Tammy Alexander, and three General Registrars from other localities, Walt Latham (York Co.), Dawn Wilmoth (City of Petersburg), and Dianna Moorman (James City Co.) were all present with the Chair of the Electoral Board to open the office and make sure voters were able to vote on Saturday, September 18, 2021.

ELECT's Information Services Division worked after hours to provide the necessary files for a printed poll book which Garry Ellis delivered on Saturday morning. This ensured that voters could be checked in properly and provided the correct ballot. Mr. Latham, Ms. Wilmoth, and Ms. Moorman provided additional documents and forms that the office would need for early voting. Tammy Alexander worked to get access to VERIS for herself and Zakia Williams, Registrar Liaison. Mrs. Alexander, Mr. Ellis, and Ms. Williams returned to the office through the next week to ensure the office was open and operational and that voters were able to vote early.

The Charles City County Electoral Board worked quickly to employ a new General Registrar who began working on Monday, September 27, 2021.

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

2021 Periodic Review Of Regulations

BOARD WORKING PAPERS

Ashley Coles
ELECT Policy Analyst

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Memorandum

To: Chairman Brink, Vice-Chair O'Bannon, Secretary LeCruise, Delegate Merrick, and Ms. Chiang
From: Ashley Coles, Policy Analyst
Date: November 15, 2021
Re: Periodic Review of Regulations

Suggested Motion

"I move that the Board adopt the Department's proposed amendments to Administrative Codes 1VAC20-20; 1VAC20-40; 1VAC20-45; and 1VAC20-70."

Background:

Pursuant to Executive Order 14 (as amended July 16, 2018) and §§ 2.2-4007.1 and 2.2-4017 of the Code of Virginia, the State Board of Elections (SBE) is required to conduct a periodic review of all regulations every four years. Additionally, 1VAC20-10-120 requires the SBE to conduct a periodic review of its regulations following each presidential election.

The purpose of this review conducted in June, 2021, was to determine whether a regulation should be repealed, amended, or retained in its current form. Public comment was sought on the review of any issue relating to this regulation, including whether the regulation (i) is necessary for the protection of public health, safety, and welfare or for the economical performance of important governmental functions; (ii) minimizes the economic impact on small businesses in a manner consistent with the stated objectives of applicable law; and (iii) is clearly written and easily understandable. This review also included an examination by the Office of the Attorney General to ensure statutory authority.

As a result of the review, four Administrative Code sections require amending: 1VAC20-20; 1VAC20-40; 1VAC20-45; and 1VAC20-70.

Applicable Code Sections: § 2.2-4007.1; § 24.2-4017

Attachments

- Proposed amendments to 1VAC20-20; 1VAC20-40; 1VAC20-45; and 1VAC20-70.

Date before State Board of Elections: November 15, 2021

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Virginia Administrative Code (VAC) citation(s): 1VAC20-70-20

Regulation Title(s): Material omissions from absentee ballots.

Date before State Board of Elections: November 15, 2021

Brief Summary: The Department of Elections recommends amendments to this regulation at the advice of Carol L. Lewis, Assistant Attorney General and with consideration of public comment on the regulation below.

Regulation Text:

1VAC20-70-20. Material omissions from absentee ballots.

A. Pursuant to the requirements of § 24.2-706 of the Code of Virginia, a timely received absentee ballot contained in an Envelope B shall not be rendered invalid if it contains an error or omission not material to its proper processing.

B. The following omissions are always material and any Envelope B containing such omissions shall be rendered invalid if any of the following exists:

1. Except as provided in subdivisions C 2 and 3 of this section, the voter did not include his full first name;

2. The voter did not provide his last name;

3. The voter omitted his generational suffix when one or more individuals with the same name are registered at the same address, and it is impossible to determine the identity of the voter;

4. The voter did not provide his house number and street name or his rural route address;

5. The voter did not provide either his city or zip code;

6. The voter did not sign Envelope B; or

7. The voter's witness did not sign Envelope B~~.~~<u>, except during a declared state of emergency related to a communicable disease of public health threat pursuant to §24.2-707 of the Code of Virginia.</u>

C. The ballot shall not be rendered invalid if on the Envelope B:

1. The voter included his full name in an order other than "last, first, middle";

2. The voter used his first initial instead of his first full name, so long as the voter provided his full middle name;

3. The voter provided a derivative of his legal name as his first or middle name (e.g., "Bob" instead of "Robert");

4. If the voter provided his first name and last name, the voter did not provide a middle name or a middle initial;

5. The voter did not provide his residential street identifier (Street, Drive, etc.);

6. The voter did not provide a zip code, so long as the voter provided his city;

7. The voter did not provide his city, so long as the voter provided his zip code;

8. The voter omitted the date, or provided an incorrect or incomplete date on which he signed Envelope B; or

9. The ballot is imperfectly sealed within Envelope B, provided that the outer envelope with Envelope B and the ballot arrived sealed.

10. The illegibility of a voter's or witness' signature on an Envelope B shall not be considered an omission or error.

D. For the purposes of this regulation, "city" may include the voter's locality, town, or any acceptable mailing name for the five-digit zip code of the voter's residence.

E. Whether an error or omission on an Envelope B not specifically addressed by this regulation is material and shall render the absentee ballot invalid shall be determined by a majority of the officers of the election present.

F. If a ballot is received by the general registrar's office by noon on the third day after the election pursuant to § 24.2-709 of the Code of Virginia but the return envelope has a missing or illegible postmark, the General Registrar shall refer to the Intelligent Mail barcode on the return envelope to determine whether the ballot was mailed on or before the date of the relevant election.

1. If there is evidence from the Intelligent Mail barcode that the ballot was mailed after the close of polls for the relevant election, the ballot shall be rendered invalid.

2. If there is no evidence from the Intelligent Mail barcode that the ballot was mailed after the close of polls for the relevant election, but the return envelope has an illegible postmark, the General Registrar shall refer to the date on which the oath on Envelope B was signed to determine whether the ballot was cast on or before the date of the relevant election.

3. If there is no evidence from the Intelligent Mail barcode that the ballot was mailed after the close of polls for the relevant election and if the return envelope has a missing postmark, the ballot shall be rendered invalid.

Statutory Authority

§ 24.2-103 of the Code of Virginia.

★ VIRGINIA ★
DEPARTMENT of ELECTIONS

Virginia Administrative Code (VAC) citation(s): 1VAC20-45-40

Regulation Title(s): Material omissions from Federal Write-In Absentee Ballots.

Date before State Board of Elections: November 15, 2021

Brief Summary: The Department of Elections recommends amendments to this regulation at the advice of Carol L. Lewis, Assistant Attorney General and with consideration of public comment on the regulation below.

Regulation Text:

1VAC20-45-40. Material omissions from Federal Write-In Absentee Ballots.

A. Pursuant to the requirements of §§ 24.2-467, 24.2-702.1, and 24.2-706 of the Code of Virginia, a timely received write-in absentee ballot on a Federal Write-In Absentee Ballot (FWAB) (Form SF-186) should not be rendered invalid if it contains an error or omission not material to determining the eligibility of the applicant to vote in the election in which he offers to vote.

B. If the applicant is not registered, the FWAB may not be accepted as timely for registration unless the applicant has met the applicable registration deadline. Section 24.2-419 of the Code of Virginia extends the mail registration deadline for certain military applicants. All applications requesting mailed ballots are subject to the mail absentee application deadline in §§ 24.2-459 and 24.2-701 of the Code of Virginia.

C. The following omissions are always material and any FWAB containing such omissions should be rendered invalid if on the declaration/affirmation any of the following, or combination thereof, exists:

1. The applicant has omitted the signature of the voter or the notation of an assistant in the voter signature box that the voter is unable to sign;

2. The applicant has omitted the signature of the witness, except during a declared state of emergency related to a communicable disease of public health threat pursuant to §24.2-707 of the Code of Virginia;

3. The applicant did not include the declaration/affirmation page; or

4. The applicant omitted from the declaration/affirmation information required by § 24.2-702.1 of the Code of Virginia needed to determine identity or eligibility including, but not limited to, current military or overseas address.

D. The ballot should not be rendered invalid if on the FWAB any of the following, or combination thereof, exists:

1. The applicant has not listed the names specifically in the order of last, first, and middle name;

2. The applicant has listed a middle initial or maiden name, instead of the full middle name;

3. The applicant has omitted the street identifier, such as the term "road" or "street," when filling in the legal residence;

4. The applicant has omitted the county or city of registration if the county or city is clearly identifiable by the residence address information provided;

5. The applicant has omitted the zip code;

6. The applicant has omitted the date of the signature of the voter;

7. The applicant has omitted the address of the witness;

8. The applicant has omitted the date of signature of the witness;

9. The applicant did not seal the ballot within the security envelope so long as the outside envelope containing the ballot and the voter's declaration/affirmation page arrived sealed; or

10. The applicant has submitted a ballot containing offices or issues for which he is not eligible.

Statutory Authority

§ 24.2-103 of the Code of Virginia.

★ VIRGINIA ★
DEPARTMENT of ELECTIONS

Virginia Administrative Code (VAC) citation(s): 1VAC20-20

Regulation Title(s): Chapter 20 General Administration

Date before State Board of Elections: November 15, 2021

Brief Summary: The amendments to this regulation reflect the structural changes after creation of the Department of Elections (ELECT). The Commissioner of ELECT handles administrative matters for the State Board of Elections, therefore, all references to the Secretary are stricken.

Regulation Text:

1VAC20-20-10 Definitions

The following words and terms when used in this chapter shall have the following meanings unless the context clearly indicates otherwise:

"Board" means the Virginia State Board of Elections.

"Secretary" means the Secretary of the State Board of Elections.

"Commissioner" means the Commissioner of Elections. Unless the context requires otherwise, all references to the secretary in forms, regulations, and guidance documents prepared before July 1, 2014, shall include the commissioner.

1VAC20-20-30. Organization of State Board of Elections; seal.

A. The board shall have a chairman and a vice-chairman of the board, in addition to the ex-officio secretary. The chairman shall preside at all meetings and perform the usual functions of a presiding officer and such other duties as are imposed by these regulations or from time to time by the board. In the chairman's absence, the vice-chairman shall perform these functions and duties. Each member~~, except the secretary,~~ shall receive a per diem and expenses for attendance. Expenses shall be reported on forms approved by the Department of Accounts. The secretary is authorized to sign the vouchers for the payment of such expenses.

~~B. The secretary shall be authorized and it shall be the secretary's duty to employ such assistants and to purchase such equipment and supplies as are necessary from time to time, subject to the provisions of the law creating the board and the provisions of the laws and rules relating to the budgetary and personnel systems. The secretary or secretary's designee is authorized to execute necessary vouchers for the payment of the salaries of such assistants and for equipment and supplies so secured.~~

~~C.~~ B. The ~~secretary~~ Commissioner is authorized and directed to perform all duties of a routine and administrative character imposed upon the board by the law creating the same and other such duties delegated to the ~~secretary~~ Commissioner by the board.

~~D.~~ C. The ~~secretary~~ Commissioner is authorized to do all things necessary to the proper execution of the law creating and governing the board and in the performance of the duties imposed upon it insofar as the same are not from their nature such as can be performed only by the board in its corporate capacity.

~~E.~~ D. The ~~secretary~~ Commissioner is authorized and directed to consult with and obtain the advice of the Attorney General, on behalf of and in the name of the board, whenever in the ~~secretary's~~ Commissioner's judgment occasion arises.

~~F.~~ E. Routine and informal action of the board or of the ~~secretary~~ Commissioner within the scope of the ~~secretary's~~ Commissioner's authority may be evidenced merely by the signature of the ~~secretary~~ Commissioner.

~~G.~~ F. Three members of the board shall constitute a quorum for the transaction of business at any duly constituted meeting.

~~H.~~ G. Notice of each meeting of the board shall be given to all board members either by the secretary or the member calling the meeting at least three business days prior to the meeting except in the case of an emergency as defined in § 2.2-3701 of the Code of Virginia. Notice shall be given to the public as required by § 2.2-3707 of the Code of Virginia. All meetings shall be conducted in accordance with the requirements of the Virginia Freedom of Information Act (§ 2.2-3700 et seq. of the Code of Virginia). All meetings shall be open to the public unless the board goes into a closed meeting pursuant to § 2.2-3711 of the Code of Virginia.

~~I.~~ H. A record of formal official and definitive actions of the board shall be preserved in a record book which may be bound or loose leaf.

~~J.~~ I. The secretary shall keep the seal of the board and affix the seal to evidence formal action of the board.

1VAC20-20-60. Delegations to ~~Secretary of State Board~~ Commissioner of Elections.

A. In addition to the authority described in 1VAC20-20-30, the ~~secretary~~ Commissioner has the delegations of authority ~~to the secretary~~ detailed in the board's ~~minutes of December 2, 2004, as amended September 14, 2010~~ Delegation of Authority 2021. Board staff (i) may update that listing to correct citations and (ii) shall post the list to the Internet in order that additional delegations or other modifications may be proposed to the board by any interested person.

~~B. The secretary is authorized to prescribe the paper ballot reconciliation form under § 24.2-666 of the Code of Virginia and to develop, maintain, and prepare instructions for the operation of poll equipment before, during, and after the closing of the polls and in preparation of the statements of results.~~

~~C.~~ B. The ~~secretary~~ Commissioner shall monitor and control the quality and cost of the copies of Title 24.2 of the Code of Virginia and other election materials that the board provides to electoral boards for use at each precinct.

~~D.~~ C. Subject to the board's policy oversight, the ~~secretary~~ Commissioner has authority to conduct the board's administrative and programmatic operations and to discharge the board's duties consistent with specific delegations of authority.

~~E.~~ D. The ~~secretary~~ Commissioner is authorized to establish and maintain a central repository of forms and instructions approved for use in conducting elections. The forms and instructions shall be organized following a standard naming convention consisting of name taken from the first descriptive line, a statutory or other authority identifier, and revision date.

1VAC20-20-9999
DOCUMENTS INCORPORATED BY REFERENCE (1VAC20-20)

Security Requirements for Cryptographic Modules, FIPS PUB 140-2, issued May 25, 2001, including change notices through December 3, 2002, National Institute of Standards and Technology, U.S. Department of Commerce

Virginia State Plan - 2012, Help America Vote Act of 2002, adopted March 2012, Virginia State Board of Elections

Help America Vote Act of 2002 Performance Goals, Virginia State Board of Elections, June 19, 2006 (Virginia State Board of Elections Policy 2006-004)

~~State Board of Election Minutes of December 2, 2004, as amended September 14, 2010~~

Virginia State Board of Elections: Delegation of Authority, 2021

Statutory Authority

§ 24.2-103 of the Code of Virginia.

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Annual Security Standards Review VA. Code § 24.2-410.2

BOARD WORKING PAPERS
Karen Hoyt-Stewart
Locality Security Program Manager

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Memorandum

To: Chairman Brink, Vice Chair O'Bannon, Secretary LeCruise, Angela Chiang, and Donald Merricks

From: Dan Persico, CIO, Karen Hoyt-Stewart, Locality Security Program Manager

Date: November 15, 2021

Re: Approval of VRSS 2022 - Locality Election Security Standards

Motion to adopt the VRSS Advisory Group and the Department of Elections recommended changes to the Locality Election Security Standards (LESS formerly MSS) for locality compliance in 2022.

CHANGES TO STANDARDS FOR 2022 in red

State Board of Elections, Department of Elections, ELECT CIO, 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 he security standards at lease 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 (unless otherwise officially delegated; i.e. via Memorandum of Understanding (MOU)) for adherence to the Locality Election Security Standards, and documenting non-compliance via ELECT exception
- 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 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.

PASSWORD COMPOSITION

1. At least 12 characters in length.
2. Utilize at least 2 of the following 4 character types – Alphabetical characters, Numerical characters, Special characters, or Combination of uppercase and lowercase letters. [**Recommendation**: Utilize at least 3 of the 4 password character types.]

DATA PRIVACY LOCALITY ELECTION SECURITY STANDARD PURPOSE

The purpose of this security standard is to provide requirements for the protection of data to ensure its confidentiality, integrity and availability for legal purposes.

SCOPE

The Data Privacy standard applies to all data and information collected by or used for elections purposes, and to all users and locality assets and resources in scope, 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".

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

SECURITY AWARENESS TRAINING

1. Every person, employed or volunteer, including electoral board members, receive data privacy training, to include:

a. Sensitive information required to be kept confidential, both personal and security
b. Data classification protocols
c. Clean desk policy
d. Incident reporting and response for privacy incidents
e. Consequences of misuse as per §24.2-1000, et seq.

INCIDENT RESPONSE

2. Expand organizational Incident Response plan to include provisions specific to reporting and responding to a data privacy breach.

CONTINGENCY PLANNING

3. Ensure all relevant privacy controls (specifically incident response and data breach) are referenced and incorporated into organizational Contingency Plan.

PUBLIC

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Department of Elections
Locality Election Security Standards (LESS)
Voter Registration System Security (VRSS)

November 2021

Version Number: 3

Table of Contents

INTRODUCTION:

The Voter Registration System Security (VRSS) Advisory Group annually reviews and recommends updates to the Locality Election Security Standards (LESS) in alignment with the Code of Virginia *§ 24.2-410.2 Security of the Virginia voter registration system, which states in part:*

"The electoral board of each county and city that utilizes supporting technologies to maintain and record registrant information shall 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.

This document, in combination with the VRSS Assurance Model and Plan of Action & Milestones (POA&Ms) Tracker, along with its associated Guideline document, is meant to help localities understand what is required to comply with the LESS.

If there is a discrepancy between any statements within this entire document and § 24.2-410.2, the Virginia code takes precedence.

SCOPE:

The Virginia Voter Registration System & supporting technologies utilized by counties and cities to maintain and record registrant information, pursuant to the Code of Virginia *§ 24.2-410.2*.

ACCOUNTABLE:

Electoral Board of each county and city utilizing the Virginia Voter Registration System and supporting technologies.

AUTHORITY:

The State Board of Elections (*may limit access to the Virginia voter registration system if the locality fails to address security risk or comply with the LESS).*

GOVERNANCE:

The State Board of Elections, Department of Elections (ELECT), and the locality Electoral Board are the governing bodies for insuring:

- Locality compliance with State Board established LESS.

- Annual updates to written security plans and procedures to ensure the security and integrity of those supporting technologies.
- Electoral board reporting is submitted annually to ELECT, by March 1.

ASSISTANCE:

The General Registrar and ELECT shall provide assistance to the electoral board upon request by the electoral board.

LOCALITY ELECTION SECURITY STANDARDS: ROLES AND RESPONSIBILITIES

PURPOSE

The purpose of this section is to provide context to some of the key roles and responsibilities relevant to the Locality Election Security Standards (LESS).

ROLES

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

- As per the Code of Virginia §24.2-410.2the 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 (unless otherwise officially delegated; i.e. via Memorandum of Understanding (MOU)) for adherence to the Locality Election Security Standards, and documenting non-compliance via ELECT exception handling.
- 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 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.

Information & Information System User

- Accountable for keeping passwords confidential.
- Accountable for activities performed under their user account.
- Accountable for keeping any issued keys, badges, ID's, smart cards, etc. secure and not allowing others to borrow them.
- Responsible and accountable to comply; any violation may result in administrative and/or disciplinary action.
- Responsible to report any suspicious activity.
- Required to return all locality provided property or resources on last working day before leaving.

KEY RESPONSIBILITIES

- Review and revise your locality LESS procedures annually or more frequently as appropriate.
- Promptly notify ELECT of personnel transfers or terminations if the individual has a VERIS account.
- Adhere to the LESS and document non-compliance via ELECT exception handling.
- Approve and authorize access to administrative or privileged accounts, including restricted access area(s).
- Review and confirm ongoing operational need for current logical and physical access.
- Review the physical access list and logs quarterly or as appropriate.
- Periodically review locality assets and baseline configurations. [**Recommendation**: Reviews occur once a year at minimum, when an integral component is installed or upgraded, there is a significant configuration change, or demonstrated vulnerability.]
- Define access privileges for each role, review access privileges on a periodic basis, ensure that each user has only enough access to conduct their job, and prohibit privileged access by users who have not gone through the appropriate vetting processes.
- Those in charge of recruiting are responsible for ensuring that the selected applicant meets the security requirements needed on the basis of the level of access to information and assets that the job duties requires.
- Managers are responsible for performing screening during the course of the employment/contract according to the degree of sensitivity of the IT assets the individual may access.
- Managers are responsible for communicating security responsibilities to staff.

- Managers are responsible to communicate to employees and third party its security responsibilities and ensure familiarization with locality Information Security Policy and locality Security and Acceptable Use Policy.
- Managers are accountable for defining physical access privileges for each role, for reviewing the physical access privileges on a periodic basis, for ensuring that each individual has only enough physical access to conduct their job, and for prohibiting unescorted physical access to restricted areas by non-locality individuals.

SECURITY AWARENESS TRAINING LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop and effectively implement Security Awareness Training programs, to lower the risk posed by system user personnel.

SCOPE

The Security Awareness Training standard applies to all personnel having access to or responsibility for any information systems identified as sensitive to election-related activities or peripherals.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

SECURITY AWARENESS TRAINING

The Locality's Security Awareness and Training program should include but not be limited to:

1. Development, implementation, testing, coordinating, monitoring and tracking the completion of the Security Awareness Training for all employees, and reports incomplete training to the respective managers.
2. Developing an information security training program so that each IT system user is aware of and understands the following concepts (and potential penalties for violations):
    a. The locality's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data including Election information.
    b. The concept of separation of duties, least privilege, and elevated privileges.
    c. Prevention and detection of information security incidents, including those caused by malicious code. Report Cyber Incidents as follows and in alignment with locality reporting procedures:
        1. To report a potential incident, call ELECT Systems Support at **(833) 716-0001**.
        2. If you see an indication of **a virus or malware** on your laptop or any device, you have strong reason to believe that your laptop or computer is experiencing an event that puts connected systems at risk.

           If you think this is true, immediately unplug your device from all connections/wires, but leave the device powered on to preserve evidence.
           If you aren't sure whether this applies, unplug your device – *because you can always plug it back in if there is no threat* – and call ELECT Systems Support.

        3. If no one picks up, leave a voicemail providing your name, a brief description of the issue, and a good call-back number.
        4. If you have not heard back from the ELECT Systems Support team in 30 minutes, call the Virginia Fusion Center (VFC) at (804) 674-2196 to report the potential incident.

d. Proper use of encryption and disposal of data storage media.
e. Access controls, including creating and changing passwords, and the need to keep all authentication information confidential.
f. Locality's Acceptable Use and Remote Access policies.
g. Intellectual property rights, including software licensing and copyright issues.
h. Special responsibility for the security of locality/ELECT and Privacy data.
i. Social engineering and phishing and other timely IT Security topics.

3. Varieties of methods are used to deliver Security Awareness and Training to locality employees and business partners periodically throughout the year, and at least annually for full refresher training. 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.

ROLE BASED SECURITY TRAINING

1. Identify opportunities to create the appropriate role-based information security training materials and communicate the training opportunities to managers. This training should happen:
   a. Before authorizing access to the information system or performing assigned duties.
   b. When required by information system changes.
   c. As practical and necessary thereafter.
2. Ensure that locality employees and business partners, who manage, administer, operate, or design IT systems, receive additional role-based information security training commensurate with level of access.

SECURITY TRAINING RECORDS

1. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
2. Retain individual training records for period as defined by the organization's records retention policy.
3. Notify supervisors when people in their charge have missing or out of date training.

INCIDENT RESPONSE LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to mitigate security incident impact through development and dissemination of an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Accordingly, to ensure that locality incident response procedures implement required incident response policy and controls.

SCOPE

The Incident Response standard 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

INCIDENT RESPONSE TRAINING

1. Provide incident response training annually to information system users consistent with assigned roles and responsibilities. This training may be part of annual Security Awareness Training.
2. Include simulated events or real world responses to facilitate effective response by personnel.

INCIDENT RESPONSE TESTING

1. Test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies using checklists, walkthroughs and/or tabletop exercises, etc. This may or may not be accomplished as part of other locality testing, such as Business Continuity, Disaster Recovery, Continuity of Operations, etc.

INCIDENT HANDLING AND RESPONSE

1. **Recommendation**: Implement an incident handling process/procedure for security (and Privacy) incidents to include preparation, detection and analysis, containment, eradication and recovery.
2. Coordinate incident-handling activities with contingency planning activities.
3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, testing and implement resulting changes accordingly.
4. **Recommendation**: Automated mechanisms are used to support the incident handling process, such as an online incident management system.
5. **Recommendation**: Incident information and individual incident responses are correlated to achieve a locality wide perspective on incident awareness and response.

6. Identify immediate mitigation procedures, including specific instructions, based on information security incident type, addressing whether and when to shut down or disconnect affected IT systems.
7. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.
8. Require that system security incidents are tracked and documented including, but not limited to, the following information:
    a. Maintaining records about each incident.
    b. Tracking the status of the incident.
    c. Documenting information necessary for forensics if applicable.
    d. Evaluating incident details, trends, and handling.
    e. **Recommendation**: Employ automated mechanisms to track security incidents and collect and analyze incident information.

INCIDENT REPORTING

1. Ensure reporting of Election specific suspected and actual security incidents in accordance with the criteria and procedures set forth in the ELECT Incident Reporting guidelines.
2. Cyber Incidents should be reported as follows:

    NORMAL BUSINESS HOURS: Weekdays - 7AM – 6PM ET
    - Normal/Minor issues should be reported to the ELECT Systems Support team via telephone: 833-716-0001.
    - Urgent/Major issues should be immediately reported to the ELECT Systems Support team via telephone: 833-716-0001. If unable to make contact or no callback is received within 15 minutes, please use the alternate contact listed below.

    NON-BUSINESS HOURS: Weekends, Holidays and Weekdays - 6PM – 7AM ET
    - Urgent/Major issues should be immediately reported to the ELECT Systems Support team via telephone: 804-593-2268. If unable to make contact or no callback is received within 15 minutes, please use the alternate contact listed below.

    ALTERNATE CONTACT: Anytime when ELECT is unavailable for a Urgent/Major issue
    - In the event that you are unable to reach someone from the ELECT Systems Support team after 15 minutes for an Urgent/Major issue, please contact the Virginia Fusion Center (VFC) via telephone at: 804-674-2196 or via email at vfc@vsp.virginia.gov

INCIDENT RESPONSE ASSISTANCE

1. Identify an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
2. Recommend employing automated mechanisms to increase the availability of incident response-related information and support (i.e. a website, automatic email notifications, etc.).

INCIDENT RESPONSE PLAN

1. Develop a formal incident response plan that:
   a. Provides a roadmap for implementing the locality's incident response capability.
   b. Meets the unique requirements of the organization relative to mission, size, structure and functions.
   c. Defines reportable incidents.
   d. Is reviewed and approved.
2. Distribute copies of the incident response plan as appropriate.
3. Review the incident response plan at least annually and when/after there is an incident, to incorporate lessons learned.
4. Update the incident response plan to address changes or problems encountered during plan implementation, execution or testing.
5. Protect the incident response plan from unauthorized disclosure and modification.

RISK ASSESSMENT LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to regularly assess information technology systems and networks for risks, including threats and vulnerabilities, in order to protect information technology assets and manage the associated risks effectively.

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. This standard applies to any locality employees (classified or temporary), contractors and business partners who participate in election-related activities.

ROLES & RESPONSIBILITIES

Please refer to the *LESS: Roles & Responsibilities* section.

SECURITY CATEGORIZATION

1. Describe the potential adverse impacts to operations, assets, and individuals should the information and information system be compromised through a loss of confidentiality, integrity, or availability.
2. Document security categorization results (including supporting rationale) in the System Security Plan (SSP) for the information system.

RISK ASSESSMENT

1. Risk Assessments for each IT system classified as sensitive will:
    a. Identify potential threats to the confidentiality, integrity and availability of an IT system and the environment in which it operates.
    b. Determine the likelihood that threats will materialize.
    c. Identify and evaluate vulnerabilities.
    d. Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.
2. Take into account vulnerabilities, threat sources and security controls, planned or in place, to determine the level of residual risk posed to organizational operations, assets, and individuals based on the operation of the information system.
3. Take into account risk posed to operations, assets, or individuals, including but not limited to:
    a. External parties.
    b. Service providers.
    c. Contractors operating information systems on behalf of the organization.
    d. Individuals accessing locality's information systems.

4. Document results in 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.
    a. Share the executive summary, including major findings and risk mitigation recommendations, with the General Registrar and local Electoral Board in closed session.
5. Update the Risk Assessment (RA) once a year, or whenever, there are significant changes to the information system/environment of operation and/or other conditions that may impact the security state of the system.
6. Input the results of the Business Impact Analysis and Data Classification into the RA.
7. Create a risk finding for any risks identified and entered in a risk register.
8. Create a risk treatment plan for at least each critical or high-risk assessment finding.
9. To improve risk communications and strive for continual improvement, each locality:
    a. Is a member of the Center for Internet Security (CIS) Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) and/or Multi-State ISAC (MS-ISAC).
    b. Completes a self-assessment annually as requested by the Department of Elections, utilizing a tool based on best practices (i.e. NIST, CIS Top 6-20, etc.).

VULNERABILITY SCANNING

1. Scan information system and hosted applications for vulnerabilities with security categorization of the information system as guide to frequency.
2. Vulnerability scanning includes scanning for specific ports, protocols, and services that should not be accessible to users and for improper configurations.
3. Report risks identified in scans using the Risk Register and Risk Treatment Plan.

PASSWORD MANAGEMENT LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to mitigate the risk of unauthorized user access.

SCOPE

The Password Management standard 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), 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities *section.*

PASSWORD COMPOSITION

1. At least 8 characters in length.
2. Utilize at least 2 of the following 4 character types- Special characters, Alphabetical characters, Numerical characters, or Combination of uppercase and lowercase letters. [**Recommendation**: Utilize at least 3 of the 4 password character types.]
3. Password history is retained and users are unable to re-use any of the last 3 passwords. [**Recommendation**: No re-use of the last 10 passwords.]
4. **Recommendation**: Passwords cannot contain the User ID.
5. **Recommendation**: Passwords cannot contain repeating strings (e.g. 12341234)
6. **Recommendation**: Passwords avoid easily guessable text such as variations on local sports teams, pet names, spousal/child names, or organization names.
7. **Recommendation**: Login Screen does not provide information about password characteristic requirements.

PASSWORD MANAGEMENT

1. Passwords are encrypted. [**Recommendation**: AES 256 (or higher/more secure) standard.]
2. Passwords are not shared.
3. Passwords are not displayed on screen on entry.
4. Users authenticate with current password before changing to a new one.
5. **Recommendation**: Access to the password storage location is highly limited.
6. **Recommendation**: Change passwords every 90 days. [Change every 30 days if only 2 of the password character types are required (when weaker passwords are utilized.)]

7. **Recommendation**: Unsuccessful login attempts do not give the user any indication of what the password lacked. 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.
8. **Recommendation**: Review password characteristics (length, complexity, etc.) at least annually to ensure sufficient strength consistent with emerging technologies.

SECURITY ASSESSMENT AND AUTHORIZATION LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to conduct security assessments and turn the results into a risk-based report suitable for authorizing officials to approve the risk levels noted in the report.

SCOPE

The Security Assessment and Authorization standard 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

REQUIREMENTS

1. Conduct security assessments when major changes to the system(s) occur, and at least annually, to determine whether the security controls related to the scope of the assessment are working as intended to mitigate risk. Security assessments include, but are not limited to, the following:
   a. Legal, policy, standards, and procedure compliance review.
   b. Vulnerability scanning.
   c. External Penetration testing.
   d. **Recommendation**: Controls assessment (Similar to NIST 800-53 Evaluation).
   e. **Recommendation**: Review and verification of system(s) composition (HW/SW, databases, network components, Interconnection Security Agreements (ISAs)).
   f. **Recommendation**: Review of existing Plan of Action & Milestones (POA&M)/Risk register.
   g. **Recommendation**: Insider Threat evaluation.

SECURITY ASSESSMENTS

1. Base the assessment process on industry-accepted leading practice security framework, and include criteria for qualifying risk commensurate with the business mission of the organization.
2. Enforce a program of regular and periodic monitoring and testing to validate assessment findings, and include the metrics used as input to the residual risk acceptance process (POA&Ms and Risk Register).
3. Supplement the assessment program periodically with assessments conducted by independent third parties or by continuous vulnerability scanning/monitoring.

4. Provide assessment results as input to the overall enterprise risk and compliance management processes. **Recommendation**: Include assessment results within the locality's Capital Improvement/Spending plan.
5. Enhance and validate security and risk assessment processes through a program of regular and periodic review, maintenance, update, and audit.
6. Mandate the development and periodic maintenance of system-specific security assessment plan(s) which describes:
   a. System(s) under assessment.
   b. Security controls and control enhancements under assessment.
   c. Assessment procedures to be used to determine security control effectiveness.
   d. Assessment environment, assessment team, and assessment roles and responsibilities.
7. Produce and document the results of the assessment within a security assessment report.
8. Provide the results of the security control assessment to senior security and business risk management leadership, including prioritized mitigations.

SYSTEM INTERCONNECTIONS

1. Authorize connections from the information system to other information systems outside the Enterprise Security boundary or boundary for the server under assessment using Interconnection Security Agreements (ISAs) (e.g. Electronic Poll book). Note: Connections to general support systems and office productivity are excluded. In addition, connections within the enterprise to other servers (DB, Print, etc.) do not need ISAs. The security posture relative to the server in the assessment should be part of those components' assessment, which can be referenced.
2. Document for each interconnection detail, the interface characteristics and security requirements, and communicate use and sensitivity of the information.
3. **Recommendation**: The ISAs detail how the data will be protected during transport, storage, and use. Particular attention is paid to the handling of privacy or sensitive election-related data.
4. Review and update ISAs at least annually or when a major system change is planned to occur, prior to implementation.

FLAW REMEDIATION/PLAN OF ACTION AND MILESTONES

1. Develop a POA&M for the information system to document the locality's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. Prioritize POA&M's, assign personal ownership, and target completion dates.
2. Update existing POA&M's based on the findings from security controls assessments, security impact analyses and continuous monitoring activities. **Recommendation**: Any "high-dollar" mitigations are added to the locality's Capital Improvement/Spending plan.
3. Identify, report, and correct or mitigate information system flaws (e.g. removing software or disabling functions, installing patches, making changes to configuration settings).
4. Collect and maintain inventory of information systems and components in order to determine which hardware equipment, operating systems, and software applications are in operation (Hardware

Asset Management – HWAM and Software Asset Management SWAM). **Recommendation**: The inventory is continually compared to the lists of authorized HW and SW or the Configuration Management Database (CMDB).

5. Update Inventory of information systems to reflect current software configurations after remediation activities.
6. Test software updates related to flaw remediation, prior to installation, for effectiveness and potential side effects on organizational information systems; testing includes checking all related software to ensure it is operating correctly.
7. Incorporate flaw remediation into locality's configuration management process.
8. A Patch and Vulnerability Management plan exists and addresses the following:
    a. Include all equipment, operating systems, and software applications. Note: If locality has hundreds of approved programs on network (i.e. mainly through grandfathering), suggest having authorizing official sign off with being OK with that situation or develop POA&Ms around those risks (if they intend to mitigate them).
    b. Designate the responsible party for monitoring and coordinating with each vendor for patch release support.
    c. **Recommendation**: Address procedures for testing before putting into enterprise wide use.
9. Track and verify vulnerability and flaw remediation actions.

SECURITY AUTHORIZATION

1. The General Registrar, designee or appropriate responsible party serves as the authorizing official for the election-related information system; whichever is appropriate.
2. The authorizing official authorizes the information system risk testing and remediation action before commencing any implementations or return to normal operations.
3. Update the system security authorization at least annually and/or when any major system change occurs.

RECOMMENDATION: CONTINUOUS MONITORING

1. Develop and implement a continuous monitoring strategy and program that includes, but not limited to:
    a. Correlation and analysis of security-related information generated by assessments and monitoring, including but not limited to, HWAM, SWAM, IDS, log file capture and correlation (Event Management), Identity Access Management (IdAM), and the latest threats from US CSIRC.
    b. Response actions to address results of the analysis of security-related information.
2. Provide reporting for security status of organization and information system to senior security and business risk management leadership at least annually.
    a. Suggest moving over time to a dashboard format for reporting, allowing senior executives and officials to view summary issues online at their convenience or to view at regularly scheduled IT Operations meetings.

SYSTEM AND COMMUNICATION PROTECTION LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures to facilitate the implementation of the System and Communication Protection policy and the associated system and communications protection controls.

SCOPE

The System and Communication Protection standard 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

BOUNDARY PROTECTION

1. Configure the information system to monitor and control communications at the external boundary of the system and key internal boundaries within the system.
2. Manage connections to external networks or information systems via interfaces consisting of boundary protection devices (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) arranged in accordance with an effective, security architecture.
3. Implement subnetworks for publicly accessible system components to separate them from internal organizational networks.
4. Configure boundary/edge devices (e.g., firewalls, routers) to protect and control access to information resources.
5. Inspect incoming network traffic and deny requests that do not comply with applicable policy.
6. Log the occurrence of dropped packets through logging features utilized on firewalls and proxies. Locality staff or the entity managing the firewall, review logs in accordance with IT Operations procedures. For large systems, the use of log reduction and correlation software is recommended.
7. Treat firewall and router configurations and associated documentation as confidentially sensitive information and are available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).
8. Utilize a secure method that supports encryption to access a router interface in order to prevent packet sniffing.
9. Disable or remove unused or unneeded services and applications when securing networked hosts.

10. Utilize port protection capabilities (MAC Protection, Port Security, 802.1x, disabling unused ports, etc.) to prevent the connection of unauthorized equipment to the network.
11. Implement cryptographic mechanisms to prevent unauthorized disclosure or corruption of information and to detect changes to information during transmission. Highly sensitive files (e.g. Voter Registration) may need to use additional controls such as hashing.
12. Assess the risk of denial of service attacks to critical information systems and ensures that those risks are adequately addressed.
13. Manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.
14. Employ monitoring tools to detect indications of denial of service attacks against the information systems, or works with service provider for alerts of abnormal traffic levels.

USE OF CRYPTOGRAPHY

1. Define and document practices for selecting and deploying encryption technologies and for the encryption of data.
2. Ensure end-user systems (desktop, laptop, tablet, etc.) utilize encryption to protect all information on their storage device.
3. Encrypt transmission of sensitive data.
4. Utilize digital signatures for data integrity.

PERIPHERAL DEVICE ACCESS

1. Establish Acceptable Use policy for peripheral devices.
2. Disable or remove unneeded connection ports or input/output devices on information systems or information system components.

SYSTEM AND INFORMATION INTEGRITY LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures to facilitate the implementation of the System and Information Integrity policy and the associated controls. Accordingly, to ensure that the system and information integrity procedures implement the requisite control sets per locality procedure.

SCOPE

The System and Information Integrity standard 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.

ROLES & RESPONSIBILITIES

Please refer to the *LESS: Roles & Responsibilities* section.

MALICIOUS CODE PROTECTION

1. Utilize real time malware/anti-virus/malicious code scanning and provide for full system scans on a regularly scheduled basis to be determined by the locality.
2. Ensure users and developers do not knowingly develop or experiment with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.)
3. Prohibit systems from being used in production until they have been properly configured/tested and have anti-malware protections installed and updated.
4. Configure anti-malware and spam controls on email system(s) to limit unsolicited messages and update when new releases are available and tested.

   Recommendation: Employ a technical surveillance countermeasures survey tool such as EDR software (available from MS-ISAC) to detect vulnerabilities.

SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

1. Generate internal security alerts, advisories, and directives as appropriate.
2. Disseminate security alerts, advisories, and directives to appropriate locality personnel.
3. **Recommendation**: Determine risk posture by comparing compliance to security alerts, advisories, and directives against any exceptions or outliers to the aforementioned.

INFORMATION SYSTEM MONITORING

1. Monitor information systems in accordance with laws, regulations, policies, defined monitoring objectives, and implement measures to detect information system unauthorized use (local, network, and remote).
2. **Recommendation**: Test intrusion-monitoring tools and mechanisms on a periodic basis defined by locality policy.
3. **Recommendation**: Deploy a wireless intrusion detection capability to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.
4. **Recommendation**: Detect network services/applications that have not been authorized by locality policy.

ACCESS CONTROL LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to prevent unauthorized user access by verifying and validating users are permitted to access the systems and data.

SCOPE

The Access Control standard 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

CONTROL AND ACTIVELY MANAGE ACCESS

1. Limit the number of people with access to the system to who need it to complete role-based assignments.
2. Restrict user access and authorizations by using the principle of "least privilege;" users are given the minimum level of access required to perform role-based assignments.
3. Elevated permissions must not be used on a day-to-day basis; the General User/Office Productivity account is used. Similarly, Privileged Users (system, network, ISOs, database admins, etc.) do not use the General User/Office Productivity account to perform work on the system(s) assigned. Privileged Users log on and use a separate privileged account for elevated activities.
4. Remove accounts that no longer need access, regardless of privilege level. This is part of the standard transfer and off-boarding procedures for staff.
5. Review account activity and disable dormant accounts at least every 180 days.
6. **Recommendation:** 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.
7. **Recommendation:** Limit the use of Privileged Accounts for each session to 2 hours. Enforce Privileged Users logoff after 15 minutes of inactivity.
8. **Recommendation:** 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.
9. **Recommendation:** Remove any temporary, test or default accounts from network systems when not in use, or comply with the organization's policies.
10. **Recommendation:** Disable service and network sign-on accounts from concurrent use.

11. **Recommendation:** Automate the process to identify and report dormant accounts on at least a rolling 180-day frequency.

SEPARATION OF DUTIES

1. Ensure security personnel who administer access control functions do not administer audit functions, taking into consideration the unique requirements of the organization, which relate to mission, size, structure and functions.

USER ACCOUNT CREATION

1. Grant each user a unique ID for account access traceability. [**Recommendation:** The same for service accounts.]
2. Review accounts periodically and disable if not in use.
3. Document and authorize use of shared accounts and passwords. Reissue account credentials when individuals are removed from the group. [**Recommendation**: Shared/system accounts are only created or used on an "exception" basis. Exceptions are documented and noted as part of the system's Risk Assessment, and reviewed quarterly.]

REMOTE ACCESS

1. Identify, authenticate, and authorize remote access users.
2. Employ remote access two-factor authentication and session timeout after no longer than 30 minutes of inactivity. [**Recommendation:** Timeout after 15 minutes of inactivity.]
3. Maintain auditable records of remote access.

ACCESS POINTS WITH A WIRELESS NETWORK

1. Ensure Wireless Access Points and related assets conform to documented technical security controls and/or vendor recommendations.

WIRELESS NETWORK SEGREGATION

1. Logically or physically separate Wireless Access Point access control features.
2. Configure Wireless Access Points to generate security logs and monitor for security issues.
3. Use wireless traffic encryption. **[Recommendation:** Encryption that meets NIST SP 800-53 and Federal Information Processing Standards (FIPS), such as FIPS 140-2.]

MANAGEMENT REQUIREMENTS

1. As applicable, detect and mitigate rogue access points connected to the implemented wired network (i.e., via features in the Wireless Access Points or through a periodic discovery process).
2. **Recommendation**: Suspend accounts/passwords within 24 hours after a user no longer requires access (termination, reassignment, etc.). If the loss of access was involuntary, the accounts/passwords are suspended as soon as the termination occurs.
3. **Recommendation**: Validate confirmation of access controls at least annually. [Typically, the validation is confirmed by a combination of vulnerability and penetration testing.]

4. **Recommendation**: Use Role-Based Access (RBAC) to the greatest extent possible. This means promoting the use of Group Accounts based on a user's business needs and eliminating/severely restricting use of individual network and local accounts on a system's Access Control List (ACL).

SESSION LOCK OUT

1. Implement a session locking policy that prevents further access to the system by initiating a session lock out.
2. Lock accounts after a maximum of no more than 30 minutes of inactivity, and reestablished access after user authenticates. [**Recommendation**: Lock after 15 minutes of inactivity.]

MOBILE DEVICES

1. Encrypt mobile devices that contain elections specific data to protect the confidentiality and integrity of that information. [**Recommendation**: Encryption is AES 256 compliant and applies to data storage and transmission (where applicable).]

UNSUCCESSFUL LOGON ATTEMPTS

1. Enforce a limit of consecutive invalid logon attempts (to be determined by locality) by a user during a 15 minute period. [**Recommendation**: Accounts are locked after a maximum of five unsuccessful access attempts, and only the Help Desk or automated account service system can unlock the account.]
2. **Recommendation**: 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.

SYSTEM USE NOTIFICATION

1. Employ system use notification message or banner, which provides privacy and security notices, before granting access to the system.
2. **Recommendation**: Do not detail the system logon message or banner with any indication of the system name or password requirements for the system being logged into.

CONTINGENCY PLANNING LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop, document, and disseminate a Contingency Planning policy that 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.

SCOPE

Contingency Planning is conducted for 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. This standard applies to any locality employees (classified or temporary), contractors and business partners who participate in election-related activities.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

DEFINITONS

1. **Business Impact Assessment (BIA)**: Develop a list of all core functions that an organization or locality performs in support of the successful completion of their business mission or goals. Specifically excluded from the BIA are supporting functions such as IT, HR, Financial Management, and other administrative areas. Once the list of core business functions is developed, the BIA will then determine the impact of the loss or degradation of the functions with respect to the mission goals. Finally, the BIA will determine the priority of the functions in relation to the organizations mission and goals.
2. **Continuity of Operations Plan (COOP)**: Use the BIA as an input and then develops a prioritized list of tasks, activities, resources, and supporting functions that are necessary ensure that the core business can be carried out in a manner meeting the functional requirements of those business area.
3. **Contingency Plan (CP)**: Utilize the COOP and BIA to develop a list of what people, tools, technologies, processes, and support functions 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:
    - Damaging weather (wind/flood, etc.).
    - Civil Unrest.
    - Cyber Attack.
    - Loss of Power or Internet Service.
    - Insider Malfeasance.

Other plans and documents will be drawn on, by the CP, to structure a complete picture of threats and mitigate at the locality level. Some of these include a Personnel Evacuation Plan, an Alternate Processing Facility Plan, an Employee Remote Work Plan, the Enterprise Architecture Plan and others as needed.

CONTINGENCY PLAN

1. Develop a contingency plan that will:
   a. Identify essential missions and business functions and associated contingency requirements.
   b. Provide recovery objectives, restoration priorities, and metrics.
   c. Address contingency roles, responsibilities, assigned individuals with contact information.
   d. Address maintaining essential missions and business functions despite a system disruption, compromise, or failure.
   e. Address eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented.
   f. Be reviewed and approved by the locality General Registrar and Electoral Board.
2. Coordinate contingency plan development with the organizational elements responsible for related plans. Examples are Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, Insider Threat Implementation Plan, and Occupant Emergency Plan.
3. Identify critical system assets supporting essential missions and business functions.
4. Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
5. The plan accounts for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.
6. The plan accounts for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.
7. Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CONTINGENCY TRAINING

1. Provide contingency training to system users consistent with assigned roles and responsibilities in the contingency planning process.
2. Incorporate simulated events into contingency training to facilitate effective response by personnel in crises.

CONTINGENCY PLAN TESTING

1. Periodically test the contingency plan for the system using varying methods (Tabletop, partial shutdown, penetration tests, etc.) to determine the effectiveness of the plan and the organizational readiness to execute the plan review the test results and initiate corrective actions, if needed.

Recommendation: Testing of plan alternates annually between Tabletop and full recovery (i.e. Full recovery in 2021, Tabletop in 2022, etc.).

2. Coordinate contingency plan testing with other locality elements responsible for related plans.
3. Test the CP at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the capabilities of the alternate processing site to support contingency operations.
4. Include full recovery and reconstitution of the system to a known state as part of CP testing.

ALTERNATE PROCESSING AND STORAGE SITES

1. Identify alternate processing and storage sites separated from the primary site(s) to reduce susceptibility to the same threats.
2. Prepare alternate site(s) so that they ready to be used as the operational site supporting essential missions and business functions.
3. Plan and prepare for circumstances that preclude returning to the primary site(s).

TELECOMMUNICATIONS SERVICES

1. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with locality availability requirements.
2. Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.
3. Require primary and alternate telecommunications service providers have contingency plans that meet locality contingency requirements and obtain evidence of contingency testing and training by providers.
4. Test alternate telecommunication services on a regular basis consistent with locality IT requirements.

SYSTEM BACKUP

1. Create backups of user and system-level information contained in the system according to locality policy and in alignment with business requirements.
2. Protect the confidentiality, integrity, and availability of backup information at on and off-site storage locations.
3. Backup copies of all systems in scope are stored in a separate facility or in a fire-rated container that is not collocated with the operational system. Alternately, stand-by systems running in a mirror configuration at alternative processing facilities exist.
4. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of voting system data.

SYSTEM RECOVERY AND RECONSTITUTION

1. Provide the capability to restore system components within the COOP, from configuration-controlled and integrity-protected information representing a known, operational state for the components.

2. Protect system components used for backup and restoration. Protection of system backup and restoration components (hardware, firmware, and software) includes both physical and technical safeguards.
3. Ensure regular backups are performed to protect data and information.
4. Test backup media on a periodic basis (at a minimum quarterly) to ensure data recovery, integrity and usability.
    a. **Recommendation**: Perform a full backup weekly with daily incremental backups.

ALTERNATIVE SECURITY MECHANISMS

1. To ensure mission and business continuity, localities can implement alternative or supplemental security mechanisms.
2. These mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ these alternative or supplemental mechanisms enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored.
3. This control is typically applied only to critical security capabilities provided by systems, system components, or system services.

MAINTENANCE LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures facilitating the implementation of the System Maintenance policy and associated controls.

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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

CONTROLLED MAINTENANCE

1. Approve and monitor all maintenance activities, whether performed within the locality (onsite or locality-controlled) or remotely, and whether the equipment is serviced onsite or removed to another location; *including consideration of supply chain issues associated with replacement components for information systems as appropriate.*
2. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
3. Require that locality-defined personnel/roles explicitly approve the removal of the information system(s) or system component(s) from organizational facilities for offsite maintenance or repairs.
4. Sanitize equipment to remove all information from associated media prior to removal from locality facilities for off-site maintenance or repairs.
5. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
6. Include locality-defined maintenance-related information in the maintenance records, as appropriate, in addition to items such as:
    a. Date and time of maintenance.
    b. Name of individuals or group performing the maintenance.
    c. Name of escort, if necessary.
    d. Description of the maintenance performed.
    e. Information system component(s)/equipment removed or replaced (including identification numbers if applicable).
7. Ensure the level of detail included in maintenance records is appropriate to the security categories of locality information systems.

MAINTENANCE TOOLS

1. Address security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on locality information systems. Maintenance tools can include hardware, software and firmware items, and are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into locality information systems
2. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
3. Check media containing diagnostic and test programs for malicious code before the media are used in the information system. E.g. setting anti-virus to force a scan on any removable media.
4. Prevent the unauthorized removal of maintenance equipment containing locality information by one of the following:
    a. Verify that there is no locality information (specific to the locality or for which the locality serves as information stewards) contained on the equipment.
    b. Sanitize or destroying the equipment.
    c. Retain the equipment within the facility.
    d. Obtain an exemption from locality-authorized personnel explicitly authorizing removal of the equipment from the facility.
5. Restrict the use of maintenance tools to authorized personnel only. E.g., establishment of a policy stating "Use of maintenance tools are restricted to authorized personnel only" could do this.

NON-LOCAL MAINTENANCE

1. Understand non-local maintenance and diagnostic activities are activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.
2. Approve and monitor non-local maintenance and diagnostic activities.
3. Only allow the use of non-local maintenance and diagnostic tools consistent with organizational policy and documented in the security plan for the information system.
4. Employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.
5. Maintain records for nonlocal maintenance and diagnostic activities.
6. Terminate session and network connections when non-local maintenance is completed.

MAINTENANCE PERSONNEL

Applies to individuals performing hardware or software maintenance on locality information systems, whether employees or third-party contractors or service providers.

1. Ensure anyone who has access has been properly vetted and is escorted where required.

TIMELY MAINTENANCE

1. Obtain timely/predictive support and/or spare parts for information system components consistent to mitigate the negative impact caused by loss of system function or operation. This support or spare part inventory is created by the use of contracts appropriate to support the uptime requirements of the information system.

MEDIA PROTECTION LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures to facilitate implementation of risk control measures associated with various forms of media in use.

SCOPE

The Media Protection standard 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, removable media, 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

MEDIA ACCESS

1. Restrict access to digital and non-digital media to authorized individuals only.
2. Risk assessment guides the selection of media and the restricted access of associated information contained on that media.
3. Document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

MEDIA STORAGE

1. Document and implement procedures to safeguard handling of all backup media containing sensitive data.
2. Employ cryptographic mechanisms to protect information in storage where the data is sensitive as related to confidentiality.
3. Physically control and secure storing of digital and non-digital media within locality-defined controlled areas using defined security measures until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

ELECTIONS SENSITIVE DATA MEDIA TRANSPORT

1. Protect and control all digital and non-digital media during transport outside of controlled areas using organization-defined security measures (i.e., locked container, cryptography).
2. Maintain accountability for information system media during transport outside of controlled areas; custodians must immediately report loss or theft of any assets.
3. Document activities associated with the transport of information system media. Employees must not remove locality or business partner owned IT assets from premises unless for a documented approved reason.

4. Document activities associated with the transport of information system media in accordance with risk assessment, using established documentation requirements. At a minimum, log or tracking mechanisms must include:
    a. Description of information being transported.
    b. Type of Information (e.g. PII) contained on the media.
    c. Method(s) of transport.
    d. Protection methods employed.
    e. Name(s) of individual(s) transporting the information.
    f. Authorized recipient(s) where practical/applicable.
    g. Dates sent and received.

MEDIA DESTRUCTION/SANITIZATION

1. Sanitize digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse.
2. Ensure media sanitization and disposal actions are tracked, documented, and verifiable.
3. One of the following three acceptable methods are used for the removal of digital data from any media commensurate with the security category or classification of the information:
    a. **DOD/NIST approved Overwriting**: Overwriting is an approved method for removal of Commonwealth data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information.
    b. **Degaussing**: A process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.
    c. **Physical Destruction:** Hard drives are physically destroyed when they are defective or cannot be economically repaired or Commonwealth data cannot be removed for reuse. Physical destruction is accomplished to an extent that precludes any possible further use of the hard drive.

PERSONNEL SECURITY MANAGEMENT LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop and implement policies and procedures 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.

SCOPE

The Personnel Security Management standard 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.

This standard applies to employees and third parties that are in scope and are:

- New hire employees
- Employees being transferred or terminated
- Third party (contractor or other) connecting to locality information system or terminated.

Recommendation: Apply this standard to all employees, third parties and individual volunteers that are in scope, regardless of when they were on-boarded (full, part-time or seasonal).

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

PERSONNEL SCREENING

1. Conduct background checks (education, work experience, criminal, credit check, etc.) prior to authorizing access to the information system.
2. **Recommendation**: Require that individuals undergo a specific 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.

PERSONNEL TERMINATION

1. The General Registrar or responsible party must notify ELECT (during working hours) within 4 hours of termination if voluntary and within 1 hour if involuntary, if the user has a VERIS account. Notifications are made via email to electit@elections.virginia.gov.
2. Terminate/revoke any authenticators/credentials associated with the individual.
3. Retrieve the appropriate assets (laptops, ID's, remote access tokens, removable media, etc.).

PERSONNEL TRANSFER

1. **Recommendation**: Require approvals and notifications to bring on new people, transfer existing personnel, and terminate existing personnel through an existing On-Boarding/Transfer/Off-Boarding process and work flow.
2. Modify access authorization as needed.
3. Initiate the transfer or reassignment actions within 4 hours of the formal transfer action.
4. Periodically review and confirm ongoing operational need for current logical and physical access.

PERSONNEL ACCESS AGREEMENT

1. Develop and document access agreements including Non-Disclosure Agreements (NDAs) for sensitive systems.
2. Ensure individuals requiring access to organizational information and information systems have signed appropriate access agreements. [**Recommendation**: 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.]

VENDOR OR THIRD PARTY PERSONNEL ACCESS – CONTRACTOR/CONSULTANT BADGE ISSUED

1. As part of contracts or 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.

PERSONNEL SANCTION

1. A sanction process exists for individuals failing to comply with established information security.

PHYSICAL AND ENVIRONMENTAL PROTECTION LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures to facilitate the implementation of the Physical and Environmental Security policy and associated controls. Accordingly, to ensure that the physical and environmental protection procedures are implemented per the requisite locality control sets and measure performance against those controls.

SCOPE

Recommendation: The Physical and Environmental Protection standard applies to all locality controlled facilities and those facilities or premises controlled by locality vendors or Third Party Associate organizations. **NOTE: None of this standard is required; recommended only.**

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

RECOMMENDATION: POWER EQUIPMENT AND POWER CABLING

Require:

1. Power equipment and power cabling for the information system to be protected from damage and destruction.
2. Power cabling to be inspected on an annual basis for the following:
    a. Power cables under raised floors and in drop ceilings are inspected for fraying or other wear, such as damage from water or pest infestation.
3. The results of the inspection to be documented.

RECOMMENDATION: EMERGENCY POWER

1. Install a short-term uninterruptible power supply (UPS) or a generator to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
2. Test the UPS and generators by a certified technician at least once a year or when any material change is made to the UPS/generator. For facilities (remote, temporary, etc.) using small or individual machine UPS backup, test the UPS as part of periodic contingency testing.
3. Protect servers and critical hardware devices with an UPS, installed either centrally or locally.

RECOMMENDATION: LOCATION OF INFORMATION SYSTEM COMPONENTS

1. Position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. E.g., if water pipes are running overhead or automatic fire suppression sprinklers, then cabling or equipment is not placed underneath the pipes, or cover equipment nightly with waterproof coverings.

2. Consider, for existing facilities, the physical and environmental hazards in the risk mitigation strategy for the information system.

RECOMMENDATION: TEMPERATURE AND HUMIDITY CONTROLS

1. Monitor and maintain the temperature and humidity levels where information system resides at organization-defined acceptable levels.

PHYSICAL ACCESS AND SECURITY LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures to facilitate implementation of the Physical Access and Security policy and associated controls. These include limiting physical access to information systems, equipment and any operating environments to only authorized individuals; whether employees or otherwise. Physical access procedures are to also implement the requisite control sets per locality procedure.

SCOPE

This Physical Access Security standard covers all facilities processing, storing, or transmitting election-related system(s), device(s) and/or data. The facilities do not have to be wholly or partially owned by the localities. Any entity whose facility or system(s) process, store, or transmit elections related system(s), device(s) and/or data, must also comply with this standard.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

PHYSICAL ACCESS AUTHORIZATIONS (RESTRICTED ACCESS AREA)

1. Restrict access to authorized personnel through keys, combinations, badges, ID's, smart cards, etc. and individuals are given minimum level of access that is required to perform their jobs.
2. Review access list quarterly or as appropriate.
3. Disable physical access for those who no longer need access, including terminated employees; immediately disable for those who are terminated by management decision, otherwise when no longer needed.
4. As appropriate, implement access control to prevent shoulder surfing for output devices (e.g. monitors, printer room).
5. Secure keys, combinations, badges, and other physical access devices.

MONITOR PHYSICAL ACCESS

1. Monitor physical access and review physical access logs.
2. Investigate violations or suspicious physical access activities.

ACCESS RECORDS FOR SECURE AREAS

1. Ensure access records are accessible where the Information System resides, and capture information such as name and organization of visitor, signature, form of ID, time of entry, departure, purpose, etc.
2. Store copies of access records at a different and secure location from the information system, in accordance with locality record retention policies.

PROGRAM MANAGEMENT LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to insure proper use and protection of information assets.

This standard is considered a Management Standard; focus is on the management of the locality Security Program and the locality management of enterprise risk.

An effective Information Security Program:

- Supports what the organization is trying to do.
- Keeps risk within acceptable levels.
- Tracks success and areas of improvement.
- Flexible to changes with the organization.

SCOPE

The Program Management standard applies to the development, implementation and governance of the locality Information Security Program and Plan related to information systems classified as sensitive to election-related activities.

Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on direction and objectives. *Establishing and maintaining a Security Program requires methodical attention to ensure that the components of the overall program are properly structured and governed to result in appropriate risk and incident management, and success.*

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

ENTERPRISE GOVERNANCE AND INFORMATION SECURITY

1. The Electoral Board of each county and city that utilizes supporting technologies to maintain and record registrant information, is the information security and privacy risk owner, per HB2178 (2019); pursuant to the Code of Virginia § 24.2-410.2 Security of the Virginia voter registration system.
2. Align Information Security governance with the locality enterprise governance, including capital planning and investment requests, and resources are available as planned; all exceptions are documented and reviewed by the electoral board.
3. Document mission/business process definitions and associated information protection requirements in accordance with locality policy and procedure.
4. Ensure information protection and privacy needs are derived from the mission/business needs defined by the locality, and are technology-independent.
5. Base protection strategies on the prioritization of critical assets and resources. Note: Elections is part of the nation's critical infrastructure.

RISK MANAGEMENT

1. Conduct risk assessments of the business process and information asset levels at least annually, and with enough lead-time to submit needs as part of the capital planning and budgeting process.
2. Identify and assess risks associated with risk assessment information assets and define a cost-effective approach to managing such risks; including, but not limited to:
   a. Risk associated with introducing new information processes, systems and technology into the locality and/or commonwealth environment.
   b. Accidental and deliberate acts on the part of locality personnel (Insider Threat), third party and outsiders.
   c. Fire, flooding, and electric disturbances.
   d. Loss or disruption of data communications capabilities.
3. Ensure Information Security Program compliance via management oversight; the method by which oversight is accomplished can be determined by locality.

INFORMATION SECURITY PROGRAM & INFORMATION SECURITY PLAN

1. Develop, implement and maintain a locality Information Security Program and Plan.
2. Review the Information Security Plan periodically to ensure ongoing alignment, at least annually for incremental improvements. **Recommendation**: Conduct a formal review of the plan quarterly.

SECURITY PLANNING LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to facilitate implementation of the Security and Privacy Planning policies and associated controls.

SCOPE

The Security Planning standard applies to all organizations, which support information systems identified as sensitive to election activities and their 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

SYSTEM SECURITY PLAN

1. Develop a security plan for the information system that:
   a. Is consistent with the organization's enterprise architecture.
   b. Explicitly defines the authorization boundary for the system.
   c. Describes the operational context of the information system in terms of missions and business processes.
   d. Provides the security categorization of the information system and relationships with or connections to other information systems.
   e. Provides an overview of the security requirements for the system.
   f. Identifies any relevant overlays, if applicable.
   g. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions.
   h. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
2. Distribute copies of the security plan and communicates subsequent changes to the plan as appropriate.
3. Review the security plan for the information system at least annually.
4. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
5. Protect the security plan from unauthorized disclosure and modification.
6. Define the security architecture.

SYSTEM AND SERVICES ACQUISITION LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop procedures to facilitate implementation of the System and Services Acquisition policy and the associated controls to mitigate risk.

SCOPE

The System and Service Acquisition standard applies to all information systems identified as sensitive to election-related activities, individual components, and services acquired 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. Services can be any kind that supports the systems, including (but not limited to) technical administrators, subject matter experts, business and management analysts, administrative assistants, and others.

ROLES & RESPONSIBILITES

Please refer to the LESS: Roles & Responsibilities section.

ACQUISITION GOVERNANCE

1. Allocate resources as part of the planning and investment control process to protect information assets such as establishment of budget line item(s) for information security in locality programming and budgeting documentation.

RECOMMENDATION: ACQUISITION PROCESS

1. Include security-specific requirements commensurate with the type (hardware, software, services) and level of assurance of items being acquired, including but not limited to:
    a. Personnel providing services are appropriately trained related to integrating security within the system development life cycle.
    b. Security requirements and security-related documentation requirements.
    c. Requirements for protecting security-related documentation in accordance with the risk management strategy.
    d. Administrator documentation for the information system, component or service that describes:
        i. Secure configuration, installation and operation of the system, component or service.
        ii. Effective use and maintenance of security functions/mechanisms.
        iii. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
        iv. Methods for user interaction, which enables individuals to use the system, component or service in a more secure manner.
        v. User responsibilities in maintaining the security of the system, component or service.

e. Description of the information system development environment and environment in which the system is intended to operate.
   i. Acceptance criteria.
   ii. Personnel Security.
   iii. Requires compliance with locality information security requirements and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.
   iv. Defines and documents government oversight and user roles and responsibilities with regard to information system services and monitoring on an ongoing basis.

2. Utilize threats, vulnerabilities, and consequences to identify the security requirements of the hardware, software and/or services in terms of business requirements.

ACQUISITION MANAGEMENT

1. Periodically assess the procurement process, identify improvement areas and implement enhancements.
2. Replace information system components when components can no longer be appropriately supported or it is cost prohibitive.
3. Provide justification with documented approval for the continued use of unsupported system components required to satisfy mission/business needs.

CONFIGURATION MANAGEMENT LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements for configuration management, to help mitigate the risk of unauthorized changes being introduced into information systems without proper approval.

SCOPE

The Configuration Management standard 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).

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

BASELINE CONFIGURATION FOR ELECTIONS RELATED SYSTEM – HARDWARE AND SOFTWARE (e.g., operating systems, applications, firewalls, and routers)

1. Maintain a list of approved hardware and software assets (preferably within a secure Configuration Management Database (CMDB) or spreadsheet).
2. Maintain baseline configuration data, which documents the application of security configurations; including over time as changes are made.
3. Periodically review the list of discovered hardware and software assets against known/approved lists.
4. **Recommendation:** Report differences in discovered versus approved configurations in alignment with locality policy.

CHANGE CONTROL

1. The approval process includes consideration for the security impact of configuration changes.
2. Analyze system and architectural changes for security ramifications.
3. Document configuration change decisions and only implement approved changes.
4. Ensure before and after change activities are audited against activities required to make changes, as appropriate.

5. Require third parties to implement configuration management and change control practices as part of contract Terms and Conditions or SLAs, where appropriate.

ACCESS RESTRICTION FOR CHANGE

1. Only qualified and authorized individuals are allowed access to initiating changes.
2. Record and maintain changes to access in accordance with localities' records retention policies.
3. Utilize Separation of Duties (SOD), least privilege, and restrict access to change hardware/software within a production environment.
4. **Recommendation**: Ensure escalation of user privileges for the change expire at the completion of the change. The duration of that time period is determined as part of the change request approval cycle. Privilege rights are renewed/extended if the change work takes longer than anticipated.

INFORMATION SYSTEM COMPONENT INVENTORY

1. Document and maintain approved system (HW/SW) component information in a format usable/consumable by the localities' Asset Management system.
2. **Recommendation**: Develop and implement a process to detect and investigate any device or software found on the network or components not listed as "Approved" in the Asset Management system.

CONFIGURATION MANAGEMENT PLAN

1. Implement a Configuration Management plan that defines and assigns responsibility for developing, implementing, maintaining, testing, and decommissioning configuration items throughout the System Development Life Cycle.
2. Configuration Management approval includes stakeholders who are responsible for reviewing and approving proposed changes, including security personnel that would conduct an impact analysis.

USER-INSTALLED SOFTWARE

1. Establish, monitor, test and enforce software authorization/approval policies.
2. Alert appropriate personnel when unauthorized software is detected, in alignment with locality policy.

AUDIT AND ACCOUNTABILITY LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide the requirements to develop and deploy procedures to facilitate implementation of the Audit and Accountability policy and associated controls.

SCOPE

The Audit and Accountability standard 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.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

AUDITABLE EVENTS

1. Configure information systems with the capability to produce audit logs with the necessary event information, at a minimum.
2. End-user workstations, including but not limited to desktop and laptops, must maintain logs of security related events.

CONTENT OF AUDIT RECORDS

1. Configure the system such that the audit records contain sufficient information to meet the unique requirements of the organization, which relate to mission, size, structure and functions at a minimum to:
   a. Establish what actions were taken, who took the actions, and on what date/time the actions were taken on the system.
   b. Provide forensic results and reporting capabilities.
   c. Log additional information commensurate with the sensitivity of information system.
   d. The system is configured to generate time stamps to include both date and time.
   e. Whenever possible, all systems utilize Network Time Protocol (NTP) time synchronization.

AUDIT STORAGE CAPABILITY

1. Allocate audit storage capacity such that capacity is not exceeded or information overwritten.
2. **Recommendation**: Provide automated alerts when log storage capacity reaches pre-defined levels (50%, 80%, and 95%).
3. Configure information systems classified as sensitive to off-load audit records at least once every 30 days onto a different system or media than the system being audited. **Recommendation**: Off-

loaded data is stored offsite on a media or system that is not accessible to the same users (including privileged users) of the information system that produced the audit records.

RESPONSE TO AUDIT PROCESSING FAILURES

1. Provide the capability to inform the appropriate designee in the event of an audit failure.
2. Provide real-time alerts when the following events occur:
   a. Recording of authentication attempts, and/or
   b. Unauthorized escalation of privileges. E.g., Syslog sending an email alert. Privilege use as part of change requests should be examined as part of request close out by QA audit.
3. **Recommendation**: Provide data for trend analysis over longer period of time.
4. Respond to events that are considered potential security events, as outlined in a Security Incident Response policy.

AUDIT REVIEW, ANALYSIS, AND REPORTING

1. Review and analyze information system audit records at least every 30 days for indications of inappropriate or unusual activity, and findings are reported to the appropriate designee.
2. Monitor Infrastructure log files on a continuous basis and document the activity.
3. **Recommendation**: Provide log trend analysis over longer time periods.
4. **Recommendation**: Review log standards annually for sufficiency to meet changing requirements.
5. **Recommendation**: Adjust auditing review and analysis in response to threat information received from credible sources (law enforcement, intelligence, or commercial providers).

PROTECTION OF AUDIT INFORMATION

1. Protect audit records, audit settings, and audit reports from unauthorized access, modification, and deletion.
2. Backup audit records to a different system or media (preferably a different location) than the system being audited at a frequency determined by the locality.

AUDIT RECORD RETENTION

1. Retain audit records consistent with the retention policy, to provide support for after-the-fact investigations of security incidents, and to meet regulatory information retention requirements.

POLICIES AND PROCEDURES LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide requirements to develop baseline security requirements to facilitate implementation of internal administrative, personnel, operational and technical policies and procedures to support Information Security Program goals, objectives and

compliance. Where policies and procedures are not in alignment or missing, they will be updated or created.

SCOPE

The Policies and Procedures standard applies to the locality leadership and management personnel supporting the establishment and governance of the locality Information Security Program. These policies and procedures shall be applicable to personnel, technologies, and other resources supporting locality voting IT systems.

The application of this standard must be aligned with locality governance related to Information Security (and Privacy) policies and procedures, to ensure its operations conform to business requirements, laws, and administrative policies. This applies to localities, vendors, and associated third parties.

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

LOCALITY RESPONSIBILITIES

1. Information security is a shared responsibility. All personnel have a role and responsibility in the proper use and protection of locality information assets.
2. Ensure the information security program roles and responsibilities identified in the locality Information Security Program Management Standard are acknowledged and understood by all locality personnel, vendors, and associated third parties.
3. Identify roles and responsibilities, and assign management responsibilities for information security program management consistent with the roles and responsibilities described in the Information Security Program Management Standard.

ACCOUNTABILITY

1. Assign accountability to ensure compliance with this standard.
2. Compliance with this standard must be measured by both internal and external audits of the localities' IT security policies and procedures against the Locality Election Security Standards adopted by the VA State Board of Elections.

GENERAL IT SECURITY POLICY AND PROCEDURE

1. Provide protection for information assets by establishing appropriate policies, standards, and procedures to ensure its operations conform to business requirements, laws, regulations, and administrative policies.
2. Maintain a standard of due care by all personnel, vendors, and associated third parties to prevent misuse, loss, disruption or compromise of locality and commonwealth information assets.

ADMINISTRATIVE POLICIES AND PROCEDURES

Define and implement:

1. Security Planning policy and procedures, which provide for the effective planning and implementation of security controls. Included in this policy is the security classification of data based on the information processed, stored, or transmitted by the system.
2. Security Awareness and Training policy and procedures, which ensures a well-trained workforce, is employed as part of a defense-in-depth strategy to protect organizations against a variety of threats targeting or leveraging personnel. Additionally, this policy provides for continuous improvement by the use of course feedback and student skills assessment.
3. Contingency Planning policy and procedures, which are part of an overall organizational program for achieving continuity of operations for vital mission/business functions.
4. Risk Assessment policy and procedures which ensure the locality is effectively measuring and managing risk. Risk tracking, via a Risk Register, and mitigation management, via Plan of Actions and Milestones (POA&Ms) are also required as the risk assessment process.
5. System and Services Acquisition policy and procedures facilitating the implementation of the system and services acquisition tasks and the associated controls to mitigate risk.
6. Security Assessment and Authorization policy and procedures which detail how to analyze various levels of risk posed by the localities' IT implementations, and how that risk been accepted as authorized by locality and Department of Elections heads or their designees. This policy also details how residual risk is defined and tracked through mitigation activities.
7. Audit and Accountability policy and procedures identify requirements for information security related audit review, analysis, and reporting performed by the locality. Also, outlines reporting and alerting requirements.
8. Security and Acceptable Use (rules of behavior) and disclosure policies and procedures which clearly delineate appropriate use and the limitations and restrictions associated with the use of locality owned information assets, including potential penalties for misuse or policy violations.
9. Personnel Security Management standards establish security standards for localities to develop and implement policies and procedures to minimize the risks associated with personnel management.
10. IT Security Program Management standards establish security standards providing an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
11. Configuration Management establishes security standards for localities to develop policies and procedures facilitating the implementation of the configuration management policy and the associated configuration management controls.

OPERATIONAL AND TECHNICAL POLICIES AND PROCEDURES

Define and implement:

1. Access Control policy and procedures, which ensure the identification of authorized users and the specification of access privileges. This standard also covers the topics of Least Privilege, Separation of Duties, and Privileged User Management.
2. System and Communications Protection standards seek to develop procedures to facilitate the implementation of the system and communications protection policy and the associated controls. Boundary protection, cryptography, and peripheral device access standards are covered in detail.

3. Incident Response standards which the localities to develop, document, and disseminate to localities an incident response policy addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
4. Media Protection policy and procedures, which address media access, marking, storage, destruction/sanitization, and transport security.
5. Physical and Environmental Protection policies and procedures, which outline requirements for the locality's facility access and environmental protection controls. Power, locations, and temperature/humidity controls are discussed in detail.
6. Password Management policy which establishes security standards for localities to develop policies and procedures minimizing the risk posed by password management practices within the locality's voting system(s). Also covered in detail are password composition and administration/management.
7. System and Information Integrity standard establishes security standards for localities to develop procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls. This standard also details requirements around malicious code, security alerts, and system monitoring.
8. Physical Access and Security establishes security standards for localities to develop procedures to facilitate the implementation of physical access and security policy and the associated physical controls.
9. Maintenance standard establishes security standards for localities to develop procedures facilitating the implementation of the system maintenance policy and the associated controls.

COMPLIANCE AND AUDIT

1. Locality Election Security standards are those, which must be met by all localities' voting systems in order to comply with VA Board of Elections security standards. While complete compliance is the objective of the security program, it is recognized that all localities have constraints around funding, schedules, and resources (both technical and human) and may not be fully compliant at the beginning of the program.
2. It is incumbent on the localities to implement a program of continuous improvement for their IT security programs in order to meet current standards and to be able to meet future standards evolving from continuously changing risk environments.
3. The localities must institute programs of testing and auditing in order to meet current and future standards. Testing is used as an internal measure of compliance, while external audits give a different view of how well the locality is meeting these standards. Over time, the internal testing and external audit results will begin to merge.
4. Utilize testing and audit results as feedback to the IT Security Program to identify risk and develop plans to mitigate those risks based on severity, priority, and resource availability. Mitigation of residual risks are rolled into IT planning including funding/capital, release schedules, acquisitions, and hiring.

SECURITY AND ACCEPTABLE USE LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide requirements for the user of, and protection of, assets and resources. It is based on the principle that the localities provide users with assets and resources to support election purposes.

SCOPE

The Security and Acceptable Use standard applies to all information systems identified as sensitive to election-related 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 (including mobile), 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.*

This standard applies to all users and locality assets and resources in scope, including the following:

- Locality users.
- External partners.
- Consultants.
- Suppliers.
- Any other individual with access to in scope locality assets and resources.

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

ROLES & RESPONSIBILITIES

Please refer to the LESS: Roles & Responsibilities section.

ACCEPTABLE USE

Permit:

1. Usage of Information System resources for career advancement, work related business, e-mail usage, incidental personal use (non-commercial) or other use as approved by designated leadership.

UNACCEPTABLE BEHAVIOR

Does not permit:

1. Using assets for personal gain, promote hatred or discriminatory tendencies, misrepresent or make fraudulent statements, or pornography.

2. Using assets in violation of any Local, State, Tribal, or Federal law.
3. Without prior documented approval through the locality change management process, modify Information System assets or hardware components, conduct an intrusive network monitoring, cause security breach, or bypass security mechanisms.
4. Use assets to elevate user privilege beyond what is approved and needed for business requirements.

PRIVACY AND SHARING SENSITIVE INFORMATION

1. User activities may be monitored, inspected and collected without user permission.
2. Prohibit sharing of sensitive information with non-authorized individuals.
3. Sensitive information must be shared in a secured means (encryption) with authorized users.
4. Do not share sensitive information on social media, no matter the circumstance.
5. Collect printed materials immediately to avoid exposure. Destroy excess printed materials in accordance with locality policy. Responsibility for sensitive material on printed materials falls on the individuals to whom the material is given, to handle and dispose of appropriately.

CONNECTING TO NETWORK ASSETS

1. Use only authorized remote connections to connect.
2. Prohibit unauthorized installation of software.
3. **Recommendation**: Establish network connection to assets via the network authentication mechanism (Active Directory, LDAP, etc.) instead of local accounts in component Access Control Lists (ACLs). Preferably, individual network accounts are placed in network Group Accounts. The Group Accounts are role based (system ZXY Admin, Power User, etc.).
4. **Recommendation**: Technologies are in place to detect failed network logon attempts. Localities have processes to investigate and escalate (if necessary) logon attempts flagged by the system(s).
5. **Recommendation**: Logically (and physically if possible) segment Guest Wireless segments apart from any networks that are used to connect to sensitive elections related system(s). Only pre-registered/approved wireless devices are allowed inside the sensitive elections related system/enterprise network. Guest Wireless devices have no access to any elections related system component devices.
6. **Recommendation**: Public access to sensitive elections related system "Public" information should only be available via a DMZ architecture segmented off the interior elections related system/enterprise network.

PERSONNEL SANCTION

1. A sanction process exists for individuals failing to comply with established information security and acceptable use.

DATA PRIVACY LOCALITY ELECTION SECURITY STANDARD

PURPOSE

The purpose of this security standard is to provide requirements for the protection of data to ensure its confidentiality, integrity and availability for legal purposes.

SCOPE

The Data Privacy standard applies to all data and information collected by or used for elections purposes, and to all users and locality assets and resources in scope, 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".

ROLES & RESPONSIBILITIES

Please refer to the *LESS: Roles & Responsibilities* section.

SECURITY AWARENESS TRAINING

1. Every person, employed or volunteer, including electoral board members, receive data privacy training, to include:
    a. Sensitive information required to be kept confidential, both personal and security
    b. Data classification protocols
    c. Clean desk policy
    d. Incident reporting and response for privacy incidents
    e. Consequences of misuse as per §24.2-1000, et seq.

INCIDENT RESPONSE

2. Expand organizational Incident Response plan to include provisions specific to reporting and responding to a data privacy breach.

CONTINGENCY PLANNING

3. Ensure all relevant privacy controls (specifically incident response and data breach) are referenced and incorporated into organizational Contingency Plan.

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Voter Registration System Security

(VRSS)

2021Updates and 2022 Proposed Changes

Daniel Persico, Chief Information Officer & VRSS Chair
Karen Hoyt-Stewart, Locality Security Program Manager

Agenda

- VRSS Updates
- LESS (formerly MSS) Proposed Changes
- Cyber Navigator Program
- Integra Update
- Closed Session Security Update
- Questions
- Adoption

VRSS Updates

VRSS Advisory Group

- 14 - Members (majority locality IT)
- 3 - General Registrars
- 3 - Electoral Board Members
- 1 - Chairperson ELECT CIO
- Other individuals invited to participate:
  - 1 - VML – Virginia Municipal League
  - 1 - VACo - Virginia Association of Counties
  - 2 - ELECT participants

VRSS Updates

Moving it Forward!

- **2021**
- Plan of Actions Milestones
- Developed Plans, Policies & Procedures Templates
- Innovative Solutions to Assist Localities

- **2022**
- Rebranding LESS (formerly MSS)
- Roles and Responsibilities
- Data Privacy
- Core Compliance Items
- Cyber Navigator Program

VRSS Updates

Rebranding and Culture Change

- Minimum Security Standards (MSS) changing to Locality Elections Security Standards (LESS)
- Localities perspectives to meet all the standards to be in compliance
- Emphasis on locality's role in security standards.

VRSS Updates

Re-emphasize roles and responsibilities

- Clear the Confusion
- Locality Governing Body
  - Boards
  - Administration
  - Information Technology
  - Information Security
- Electoral Boards
  - General Registrar
  - Staff

VRSS Updates

Core Compliance Items

- Establish a balanced means to maturing security programs while focusing on the highest risk areas based on the current threat landscape
- Request delegation of SBE to VRSS to make emergency changes to CCI based on emerging threat(s)

VRSS Updates

Introducing Data Privacy

- Protecting Data is equally important as protecting the systems but require a different approach
- Training
- Best Practices

Virginia Cyber Navigator Program

- Program Overview
- NSA Grant - $ 3 million
- Universities leadership and participants
  - UVA, VT, ODU, GMU, NSU
  - JMU, W&M, Radford, UVA at Wise
- Pilot Program
- Full Implementation

Integra Updates

- Integra (GRC Tool) has come a LONG way!
- The responses to the Not Mets in Integra will guide us to determine which localities may need prioritization for assistance with the Cyber Navigator Program.
- We will be coordinating with localities interested in participating with university interns.

Integra Updates

- The changes to the LESS Checklist provided by the VRSS Advisory Group need to be updated in Integra (December/January).
- The changes clarified controls and added the Core Compliance Items as a separate module.

ENTER CLOSED SESSION

RETURN FROM CLOSED SESSION

QUESTIONS?

Proposed Motion

- Motion: To adopt the VRSS Advisory Group and the Department of Elections recommended changes to the Locality Election Security Standards (LESS formerly MSS) for locality compliance in 2022.