★ VIRGINIA ★
STATE BOARD of ELECTIONS

BOARD MEETING

Wednesday, November 15, 2023
Martha Brissette Conference Room
Washington Building
Richmond, VA
Video and Teleconference

Videoconference:

https://covaconf.webex.com/covaconf/j.php?MTID=mdbea3ec819598698cbf45c3b2858db9a

Meeting password: Pzpfe4ZmK48

Teleconference:

1-517-466-2023 US Toll
1-866-692-4530 US Toll-Free
Access Code: 2425 936 3489

1:00 P.M.

STATE BOARD OF ELECTIONS
AGENDA

***DATE*: Wednesday, November 15, 2023**
LOCATION: 1100 Bank St.
Washington Bldg – Room B-27
Richmond, VA 23219
TELECONFERENCE:
+1-517-466-2023 US Toll
+1-866-692-4530 US Toll Free
Access code: 2425 936 3489
VIDEO CONFERENCE:
https://covaconf.webex.com/covaconf/j.php?MTID=mdbea3ec819598698cbf45c3b2858db9a
Password: Pzpfe4ZmK48
***TIME*: 1:00 P.M.**

I. CALL TO ORDER	*John O'Bannon, Chairman*
II. APPROVAL OF MINUTES **A. September 14, 2023** **B. November 7, 2023**	*Georgia Alvis-Long, Secretary*
III. PUBLIC COMMENT	
IV. COMMISSIONER'S REPORT	*Susan Beals* *Commissioner*
V. VRSS RECOMMENDATIONS REGARDING 2024 LOCALITY ELECTION SECURITY STANDARDS	*Arielle A. Schneider* *ELECT Privacy Officer*
VI. STAND BY YOUR AD POLICY REVISION	*Tammy Alexander* *Campaign Finance Compliance and Training Supervisor* *Steven Koski* *ELECT Policy Analyst*

VII. RISK LIMITING AUDIT (RLA)

A. Overview of Process

Rachel Lawless
Confidential Policy Advisor

B. Selecting a General Assembly Contest for RLA; Generating the Random Seed Number for RLA; and Setting the Risk Limit.

Claire Scott
ELECT Policy Analyst
Londo Andrews
Voting Systems Security Program Manager

C. Approving Local Races for RLA, Setting the Risk Limit, Generating the Random Seed Number for RLA and Setting the Dates for both RLAs.

Claire Scott
ELECT Policy Analyst
Londo Andrews
Voting Systems Security Program Manager

VIII. ADJOURNMENT

NOTE: https://townhall.virginia.gov/L/ViewMeeting.cfm?MeetingID=37230

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

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

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

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

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

Approval of Minutes

BOARD WORKING PAPERS

The State Board of Elections ("the Board") meeting was held on Thursday, September 14, 2023 in the Martha Brissette Conference Room of the Washington Building in Richmond, Virginia. The meeting also offered public participation through electronic communication so the remote public could view and hear the meeting. In attendance: John O'Bannon, Chairman; Rosalyn R. Dance, Vice Chair; and Delegate Donald Merricks, member; represented the State Board of Elections ("the Board"). Georgia Alvis-Long, Secretary and Matthew Weinstein, member attended the meeting electronically. Susan J. Beals, Commissioner, represented the Department of Elections ("ELECT"), and Travis Andrews represented the Office of the Attorney General ("OAG"). Chairman O'Bannon called the meeting to order at 1:00 P.M.

The first item of business was the Approval of the Minutes from the August 15, 2023 Board Meeting, presented by Secretary Alvis-Long. Delegate Merricks moved *that the Board approve the minutes from the August 15, 2023 with the correction on page 11, line 214.* Vice Chair Dance seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

The Chairman opened the floor to public comment. Ann Grigorian, Roxanna Gray and Virginia Derby Jordan addressed the Board.

The second item of business was the Commissioner's Report, presented by Commissioner Beals. Commissioner Beals informed the Board that early-voting for the November 7, 2023 Election starts September 22, 2023. The Commissioner stated that ELECT has proofed ballots to ensure ballot standards have been met. Commissioner Beals stated that localities are printing and preparing to mail out the absentee ballots next week. The Commissioner stated the ballots are for those voters that have requested an absentee ballot, those on the permanent absentee list, and military and overseas voters must be mailed out 45 days before the election.

Commissioner Beals informed the Board that the return absentee ballot, envelope B, now requires the voter to provide the last four of their Social Security number and their date of birth. The Commissioner stated that ELECT has streamlined the provisional process by creating a new provisional all-in-one ballot envelope. The provisional envelope has a side for same day registration and another side for regular provisional voters. Commissioner Beals stated that ELECT has provided new trainings to include election observers and same day registration available to Officers of Election, Electoral Board Members and General Registrars on the ELECT website. The Commissioner advised the Board that ELECT has made some improvement to the elections night reporting site and hosted a webinar to guide the registrars through the new improvements.

The third item of business was the Certification of August 29, 2023 Special Election, presented by Paul Saunders, Elections and Registration Services Supervisor. *This report is in the Working Papers for the September 14, 2023 Meeting.* Delegate Merricks stated after reviewing the Abstracts of Votes Cast in the August 29, 2023 Special Election for Member, House of Delegates, 6th District, I *move that the Board certify the results as presented and declare the winner.* Vice Chair Dance seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

The fourth item of business was the Finalization of Stand By Your Ad Decisions from the August 15th Meeting, presented by Tammy Alexander, Campaign Finance Compliance and Training Supervisor. *This memo is in the Working Papers for the September 14, 2023 Meeting.* Vice Chair Dance moved *that the Board finalize the decisions made on the fourteen Stand By Your Ad*

(SBYA) violations assessed at the August 15, 2023 State Board of Elections (SBE) meeting. Delegate Merricks seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

The fifth item of business was the Voting System Certification presented by Londo Andrews, Voting Systems Security Program Manager. *This memo is in the Working Papers for the September 14, 2023 Meeting.* Delegate Merricks *moved that the Board certify the use of Dominion voting system – version 5.17 in elections in the Commonwealth of Virginia, pursuant to the State Certification of Voting Systems: Requirements and Procedures.* Vice Chair Dance seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

The sixth item of business was the State Board of Elections Report presented by, Ashley Coles, ELECT Policy Analyst. *This report is in the Working Papers for the September 14, 2023 Meeting.* No action required.

The seventh item of business was the Petition for Rulemaking, presented by Ashley Coles, ELECT Policy Analyst. *This memo is in the Working Papers for the September 14, 2023 Meeting.* Vice Chair Dance moved *that the Board take no action on the proposed Petition for Rulemaking pursuant to §2.2-4007 and 1VAC20-10-50 of the Code of Virginia as the Board does not have the statutory authority to mandate the requested practice and that such decision be posted on Town Hall.* Delegate Merricks seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

The eight item of business was the Split Precinct Waiver Request for Northumberland County, presented by Claire Scott, ELECT Policy Analyst. *This memo is in the Working Papers for the September 14, 2023 Meeting.* Vice Chair Dance *moved that the State Board of Elections approve the split precinct waiver* *for Northumberland County.* Secretary Alvis-Long seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

At 1:38 P.M., Delegate Merricks pursuant to Virginia Code Section 2.2-3711(A)(7), I *move that the Board go into closed session for the purpose of discussing pending and threatened litigation. In accordance with Section 2.2-3712(F), Susan Beals, Commissioner of Elections, and Travis Andrews of the Office of the Attorney General, will attend the closed session because their presence will reasonably aid the Board in its consideration of the subject of the meeting.* Mr. Weinstein seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

At 1:59 P.M., Delegate Merricks moved *to reconvene the meeting in open session, and take a roll call vote certifying that to the best of each member's knowledge (i) only such public business matters lawfully exempted from open meeting requirements under this chapter and (ii) only such public business matters as were identified in the motion by which the closed meeting was convened were heard or discussed by the State Board of Elections.* Vice Chair Dance seconded the motion and the motion passed unanimously. A roll call vote was taken:

Chairman O'Bannon – Aye

Vice Chair Dance – Aye

Secretary Alvis-Long – Aye

Delegate Merricks – Aye

Mr. Weinstein – Aye

The meeting adjourned at 2:00 P.M

____
Chairman

____
Vice Chairman

____
Secretary

____
Board Member

____
Board Member

The State Board of Elections ("the Board") meeting was held on Tuesday, November 7, 2023 in the Martha Brissette Conference Room of the Washington Building in Richmond, Virginia. The meeting also offered public participation through electronic communication so the remote public could view and hear the meeting. In attendance: John O'Bannon, Chairman; Rosalyn R. Dance, Vice Chairman; Georgia Alvis-Long, Secretary, and Delegate Merricks and Matthew Weinstein members; represented the State Board of Elections ("the Board"). Susan J. Beals, Commissioner, represented the Department of Elections ("ELECT"), and Travis Andrews and Dennis Polio represented the Office of the Attorney General ("OAG"). Chairman O'Bannon called the meeting to order at 10:04 A.M.

Chairman O'Bannon informed the Board that the only item on the agenda was oversight of the General Election and that there would be no opportunity for public comment. At 10:05 A.M., the Board went into recess.

Chairman O'Bannon opened the meeting from recess at 7:00 P.M. No business was conducted during this meeting. Mr. Weinstein moved *to adjourn the meeting.* Vice Chair Dance seconded the motion and the motion passed unanimously.

The meeting adjourned at approximately 7:01 P.M.

____
Chairman

____
Vice Chairman

____
Secretary

____
Board Member

____
Board Member

★ VIRGINIA ★
STATE BOARD *of* ELECTIONS

Public Comment

BOARD WORKING PAPERS

★ VIRGINIA ★

STATE BOARD of ELECTIONS

Commissioner Report

BOARD WORKING PAPERS

Susan Beals
Commissioner

★ VIRGINIA ★

STATE BOARD of ELECTIONS

VRSS Recommendations Regarding 2024 Locality Election Security Standards

BOARD WORKING PAPERS
Arielle Schneider
ELECT Privacy Officer

★ VIRGINIA ★

STATE BOARD *of* ELECTIONS

Memorandum

To: Chairman O'Bannon, Vice-Chair Dance, Secretary Alvis-Long, Delegate Merricks, and Mr. Weinstein

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

Date: November 15, 2023

Re: 2024 Locality Election Security Standards (LESS)

Executive Summary

In alignment with the Code of Virginia §24.2-410.2 Security of the Virginia Voter Registration System, the State Board of Elections is required to update the Locality Election Security Standards annually by November 30, after consultation with the Voter Registration System Security (VRSS) Advisory Group ("representatives of local government information technology professionals and general registrars").

Proposed Motion

I move to adopt the revised 2024 Locality Election Security Standards effective December 1, 2023.

Background

The purpose of the Locality Election Security Standards (LESS) is to ensure that each county and city meet election security standards designed to maintain the security and integrity of the Virginia voter registration system and supporting technologies through appropriate security controls, policies, practices and procedures. To help all localities work toward improving their cybersecurity stance, the Virginia Voter Registration System Security Advisory Group (VRSS) worked to make limited changes to the standards, instead focusing on tools and resources localities can use to meet baseline requirements.

The proposed 2024 Locality Election Security Standards represent a collaborative effort that included input from members of the electoral board, general registrars, city and county information technology leadership, and ELECT staff who have a wide range of expertise in election management, information technology, and cybersecurity.

Attachments

2024 Locality Election Security Standards – Draft

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

2024 LOCALITY ELECTION SECURITY STANDARDS (LESS)

Voter Registration System Security (VRSS) Advisory Group

Virginia Department of Elections

Virginia State Board of Elections

Version Number: 5

2024 TABLE OF CONTENTS

QUICK START GUIDE

BACKGROUND

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

The law (Code of Virginia § 24.2-410.2(B)) requires each locality electoral board to "develop and annually update written plans and procedures to ensure the security and integrity of those supporting technologies. All plans and procedures shall be in compliance with the security standards established by the State Board pursuant to subsection A. Each electoral board shall report annually by March 1 to the Department of Elections on its security plans and procedures." To maintain access to the Virginia Voter Registration System, localities must follow the State Board of Elections' adopted Locality Election Security Standards. Prior to restricting access to the Virginia voter registration system, the Department of Elections must provide notice to the locality of the failure to comply with the required standards or the required reporting on compliance with those standards and allow the locality seven days to correct deficiencies.

A locality has until March 1 annually to submit its report on compliance with the Locality Election Security Standards, and until April 1 to submit its full Remediation Plan in compliance with the Locality Election Security Standards GR 4 (Locality Election Security Standards Annual Audit). As per § 24.2-410.2, any record or meeting, the release of which would compromise the security of elections, shall be confidential and are prohibited from release. This includes records regarding locality security, compliance, penetration tests, and remediation planning. These records must be encrypted if provided electronically to an authorized individual.

2023 UPDATES

This year, the Voter Registration System Security (VRSS) Advisory Group sought to recommend as few changes as possible to the Locality Election Security Standards and instead focus on improving locality infrastructure through trainings with locality IT staff to support local administrators during the ongoing election season. The VRSS and ELECT worked to develop multiple resources tailored to the LESS and COV localities, including templates and guides on role-based training, incident reporting and review, patch management, privacy training for elections officials, vulnerability scanning remediation frequency, system categorization, and baseline configuration.

2022 UPDATES

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

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

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

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

REMEDIATION PLAN

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

All localities must meet the controls identified as Baseline. If a locality does not meet a Baseline controls, it must provide a remediation plan to include:

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

ROLES AND RESPONSIBILITIES

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

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

Locality Governing Body

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

Electoral Board

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

General Registrar

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

GR 1 – SECURITY AWARENESS TRAINING

BACKGROUND

74% of data breaches are tied to "human element" related security weaknesses. GR 1 outlines the requirements to develop and effectively implement Security Awareness Training (SAT) programs, to lower the risk posed by system users.

Localities must also implement role-based security training for specific information technology roles in addition to security awareness training for users. When assigning role-based training, localities should determine the appropriate training for individuals based on their roles and responsibilities, the specific security requirements of the locality, and the information systems they have access to. Suggested roles include system administrator, systems support professional, database administrator, security analyst, network administrator, software developer, security engineer, cloud architect, information security manager or help desk staff member who interacts with infrastructure and technology supporting the elections office completes appropriate role-based security training.

Please see the LESS Control Matrix, Tools and Resources document for more information and resources about role-based training to help you and your locality IT professionals implement this standard in your locality. We outline what role-based training is, explain how it's different from regular user security awareness training, and provide a chart of suggested training topics.

SCOPE

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

MATURITY MATRIX

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

1 Security Awareness Training

1.1 All locality employees *with access to the VERIS system* comply with 1 VAC 20-20-90, which establishes new user, annual, and monthly Information Security and Awareness Training to maintain access to VERIS.

1.2 All locality employees *with access to voter registration records* receive training about how to protect sensitive information.

2 Role-Based Security Training

2.1 Your locality provides role-based training to information technology professionals with access to elections systems.

3 Training Records

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

3.2 Your locality security awareness training program is documented, monitored, tested, and reviewed for improvement annually and for compliance with current ELECT VERIS access and SAT requirements.

GR 2 – INCIDENT RESPONSE

BACKGROUND

Incident response is the effort to quickly identify an attack (data breach, ransomware, malware infection, etc.), minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents. The purpose of GR 2 is to ensure each elections employee can recognize signs of a potential cyberattack, that staff knows how and what to report, and that the locality has a response plan outlining the steps to take in the event of a cyberattack. Localities should document and implement incident response plans and procedures, train users to identify and report suspicious activity from both external and internal sources, periodically test the locality incident response capabilities, and report to ELECT and the Fusion Center as required.

Please refer to the LESS Control Matrix for incident response resources and templates.

SCOPE

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

MATURITY MATRIX

GR 2 – Incident Response	Baseline	Preferred	Platinum
1. Incident Reporting	1.1	All	All
2. Incident Response	2.1	2.1-2.3	All
3. Incident Preparedness	3.1	3.1-3.2	All

1 Incident Reporting

1.1 Your office has an incident reporting procedure to ensure potential cybersecurity incidents are reported appropriately.

1.2 Your incident reporting procedure defines reportable incidents and outlines how to report the incident internally for further action.

2 Incident Response

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

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

2.3 Your plan outlines incident handling capability for real-time incident management including preparation, detection and analysis, containment, eradication, and recovery.

2.4 Your plan requires a post-incident review to incorporate lessons learned from the incident into training and process documentation.

3 Incident Preparedness

3.1 All elections employees are provided training regarding how to detect potential cybersecurity incidents such as the below.

3.1.1 Usual files, applications, or services that cannot be accessed.

3.1.2 Accounts have been locked or the passwords have been changed without your knowledge.

3.1.3 Files or software have been deleted or installed, or the contents have been changed without your involvement.

3.1.4 Suspicious pop-ups load when you access the internet, or unknown files or programs appear.

3.1.5 Slower than normal internet speeds due to a spike in network traffic (or computers “hang” or crash).

3.1.6 Files have been unexpectedly encrypted, blocking your access to them.

3.1.7 Programs running, turning off or reconfiguring themselves.

3.1.8 Emails sent automatically without the user’s knowledge.

3.1.9 No control over functions of the computer (e.g., in instances whereby device can be controlled remotely, or computer gets locked and displays messages coaxing users into paying a ransom).

3.1.10 Requests for credentials

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

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

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

GR 3 – RISK ASSESSMENT

BACKGROUND

Localities and their administration officials must identify the potential adverse impacts on the locality's operations, assets, and individuals if election information and systems are compromised through a loss of confidentiality, integrity, or availability. Risk assessments must consider risk from external parties such as service providers or contractors that operate information systems on behalf of the locality.

Localities must maintain an information asset management system or inventory that categorizes systems according to the data stored, transmitted, or processed by the system.

Localities should conduct vulnerability scans of all information systems. The frequency and comprehensiveness of vulnerability scans should be determined by the security categorization of the information system, as this will reflect the level of risk associated with the system. Localities should ensure that their vulnerability scanning procedures are comprehensive and that they cover all potential sources of vulnerabilities. This includes scanning for patch levels, functions, ports, protocols, and services that should not be accessible, and improperly configured or incorrectly operating information flow mechanisms. By conducting regular vulnerability scans, localities can identify and address security vulnerabilities before they are exploited by attackers. This helps to protect sensitive data and ensure the availability of critical information systems.

SCOPE

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

MATURITY MATRIX

GR 3 – Risk Assessment	Baseline	Preferred	Platinum
1. Security Inventory	1.1	All	All
2. Vulnerability Scanning	2.1	All	All
3. Risk Assessment	3.1	3.1-3.2	All

1 Security Inventory

1.1 The GR has an accurate and annually reviewed inventory of information systems and assets used for elections purposes as outlined in TECH 12 – Configuration Management controls 1.1 and 1.2.

1.2 The GR and locality IT support have met to identify the systems most critical to elections operations and the systems storing sensitive data. Systems containing information about election security or highly sensitive personally identifiable information about voters are classified as "sensitive". The results of these ongoing discussions are documented in a System Security Plan for the information system.

2 Vulnerability Scanning

2.1 Your locality uses a security scanner at minimum monthly to find any vulnerabilities in systems that are exposed to the internet. Identified vulnerabilities are fixed according to the timelines specified in the locality's remediation schedule.

2.2 Your locality uses a security scanner at minimum monthly to find vulnerabilities in critical systems, such as domain servers, authentication servers, network equipment, and servers that contain sensitive data. Identified vulnerabilities are fixed according to the timeline in the locality's remediation schedule.

2.3 Vulnerabilities identified in scans are classified according to criticality and tracked. Mitigation plans for specific vulnerabilities are documented via Plan of Actions and Milestones (POA&Ms).

3 Risk Assessment

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

3.2 Risk assessments also consider third-party risk posed to operations, assets, or individuals from external parties, including service providers and contractors operating information systems on behalf of the organization.

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

3.4 An executive summary of the locality's most recent risk assessment was shared with the General Registrar and local Electoral Board in a closed session during the last calendar year.

GR 4 – LOCALITY ELECTION SECURITY STANDARDS ANNUAL AUDIT

BACKGROUND

The Code of Virginia § 24.2-410.2 requires local electoral boards to report annually on locality compliance with the Locality Election Security Standards and turn the results into an actionable Remediation Plan. Each locality is required to comply with all standards identified as Baseline and must submit a Remediation Plan to the Department of Elections by April 1 for each Baseline standard not met. Localities must perform a penetration test or penetration scan based on the categorization of their systems. A penetration test would be typically performed by humans using a variety of tools and techniques to gain unauthorized access. Automated penetration scans, a type of penetration test, scan for common vulnerabilities, but are less comprehensive and expensive than human-led penetration tests.

SCOPE

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

MATURITY MATRIX

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

1 Annual Assessment and Penetration Testing

1.1 Each locality must internally review LESS compliance annually. The audit will review the locality's overall organizational and information technology compliance to the LESS standards, showing the Baseline controls for which a Remediation Plan will need to be submitted to the Department of Elections. Compliance checklists are submitted to ELECT as required by March 1. *If your locality completed and submitted the 2023 LESS Report, you comply with this control.*

1.2 Systems with high security categorization are penetration tested annually, systems with moderate security are penetration tested every two years, and systems with low security are penetration tested as needed.

1.3 An executive summary of the external penetration test is provided to the local Electoral Board in a closed session meeting.

2 Remediation Plan

2.1 Your locality has developed a remediation plan to address each baseline control not in compliance. A new Remediation Plan is created each year. Plans not closed out from the previous year are included in the new Remediation Plan which documents the following:

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

2.2 Your locality's remediation plan is regularly updated with a progress report regarding completion efforts. Updates should include information on the age of open items.

GR 5 – PRIVACY AND DATA PROTECTION

BACKGROUND

GR 5 defines personal information, sensitive information, and sensitive system, as well as outlines requirements for the protection of data to ensure its confidentiality, integrity and availability for legal purposes. Localities must develop and implement training to ensure staff understand their responsibilities for protecting personally identifiable and other sensitive information. Localities must design and implement controls over the collection, sharing, storing, transmitting, use, and disposal of sensitive and personally identifiable information.

SCOPE

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

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

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

DEFINITIONS

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

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

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

MATURITY MATRIX

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

ELECT Locality Election Security Standards

1 Personal and Sensitive Information

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

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

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

2 Release and Transport

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

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

2.2.1 Description of information being transported.

2.2.2 Type of Information (e.g., Personally Identifiable Information) contained on the media.

2.2.3 Method(s) of transport.

2.2.4 Protection methods employed.

2.2.5 Name(s) of individual(s) transporting the information.

2.2.6 Authorized recipient(s) where practical/applicable.

2.2.7 Dates sent and received.

3 Destruction

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

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

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

BACKGROUND

GR 6 works to ensure that employees and business partners comply with the minimum-security prerequisites applicable to their function and are informed of their responsibility to protect locality information; that physical access controls adequately protect equipment and information; and that environmental factors such as emergency are considered and implemented. Localities must determine and implement proper physical security controls which may include professional security guards, keys, locks, cameras, combinations, and card readers. Localities must also ensure that appropriate background screening is performed on staff and contractors before access is granted to systems and data. Third party risk should be managed using non-disclosure, service level, and other agreements.

SCOPE

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

PHYSICAL SECURITY: PERSONNEL

MATURITY MATRIX

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

1 Personnel Screening

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

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

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

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

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

2 Personnel Termination and Transfer

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

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

3 Personnel, Vendor, and Third-Party Access Agreements

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

3.2 Develop and document access agreements including Non-Disclosure Agreements (NDAs) for sensitive systems.

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

3.3.1 Contractor shall fully cooperate with Commonwealth incident response resources and all required law enforcement personnel for assistance in the handling and reporting of security incidents.

3.3.2 Contractor shall, at all times, comply with the privacy and security requirements mandated by federal, state, and local laws and regulations.

3.3.3 Contractor shall not use any software, hardware, or services prohibited pursuant to § 2.2-5514 of the Code of Virginia.

3.3.4 Contractor shall only store and process ELECT data within the continental United States.

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

PHYSICAL SECURITY: ENVIRONMENTAL PROTECTION

MATURITY MATRIX

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

4 Emergency Power

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

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

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

5 Location of Information System Components

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

PHYSICAL SECURITY: ACCESS

MATURITY MATRIX

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

6 Restricted Access Area

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

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

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

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

7 Monitor Physical Access

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

7.2 Review access logs monthly for anomalies.

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

8 Access Records for Secure Areas

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

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

9 Visitor Access

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

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

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

ORG 7 – ORGANIZATIONAL POLICIES AND PROCEDURES

BACKGROUND

ORG 7 exists to assist locality leadership and management, as well as technology or security personnel to prioritize, fund and establish a locality Information Security Program that will support compliance with the Locality Election Security Standards. Localities must document and implement policies and procedures for the effective implementation of the LESS controls, including but not limited to acceptable use policy, business continuity plan, etc. Localities must also document a System Security Plan that describe how security requirements for election systems and data are met.

SCOPE

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

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

1 Organizational Security Planning

1.1 Locality leadership (city/county administrator or technology leadership) has provided the General Registrar a Business Impact Assessment (BIA) within the last year, that specifically addresses the locality's elections-specific mission and goals and:

1.1.1 Lists all core functions, in order of priority with relation to organizational mission and goals.

1.1.2 Outlines impact of the loss or degradation of the functions with respect to the mission goals.

1.2 Within the last year, your locality has created and/or updated an elections-specific Contingency Plan (CP) that, among other goals, does the following:

1.2.1 Identify essential missions and business functions and associated contingency requirements.

1.2.2 Identify critical system assets supporting essential missions and business functions.

1.2.3 Provide recovery objectives, restoration priorities, and metrics.

1.2.4 Address contingency roles, responsibilities, assigned individuals with contact information.

1.2.5 Address maintaining essential missions and business functions despite a system disruption, compromise, or failure.

1.2.6 Address eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented.

1.2.7 Be reviewed and agreed to by the locality General Registrar and Electoral Board.

1.3 The Contingency Plan lists the people, tools, technologies, processes, and support functions that must be in place to resume normal or possibly degraded functionality when one or more threats materialize to place the mission of the organization in jeopardy. Some examples of threats include, but are not limited to:

1.3.1 Damaging weather (wind/flood, etc.).

1.3.2 Civil Unrest.

1.3.3 Cyber Attack.

1.3.4 Loss of Power or Internet Service.

1.3.5 Insider Threat.

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

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

1.5.1 Coordination of contingency planning with the appropriate organizational elements – leadership, technology, personnel, fiscal, maintenance.

1.5.2 Alignment with contingency plans of external service providers to ensure that contingency requirements can be satisfied.

1.5.3 Identifying alternative processing and storage sites that are separated from the primary site(s) to reduce susceptibility to the same threats.

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

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

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

1.8.1 Tests the alternate processing site and alternate telecommunications services to familiarize personnel with the facility, resources, and to allow the evaluation of capabilities of alternative site/telecommunications services to support contingency operations.

1.8.2 Test includes full recovery and constitution of the system to a known state.

2 System Security Planning (SSP)

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

2.1.1 Maps the relevant, associated elements of the organization's enterprise architecture.

2.1.2 Explicitly defines the authorization boundary for the system.

2.1.3 Describes the operational context of the information systems in terms of missions and business processes.

2.1.4 Provides the security categorization of the information system and relationships with or connections to other information systems.

2.1.5 Provides an overview of the security requirements for the system and identifies any relevant overlays, if applicable.

2.1.6 Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions.

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

3 Acceptable Use Policy

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

3.1.1 Prohibits the use of elections assets for personal gain, to promote hatred or discriminatory tendencies, to misrepresent or make fraudulent statements, or for pornography.

3.1.2 Prohibits unauthorized remote connections, installation of software or any unauthorized modifications to Information System assets or hardware components; intrusive network monitoring; bypassing security mechanisms; using assets to elevate user privilege beyond what is approved and needed for business requirements.

3.1.3 Notifies users that their activities may be monitored, inspected, and collected without user permission; prohibits the sharing of sensitive information with non-authorized individuals, on social media, or in printed materials; requires users to use encryption or another secured means to share sensitive information with authorized users; outlines responsibility to secure and dispose of sensitive material falls on individuals to whom access, or materials are given.

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

TECH 8 – PASSWORD MANAGEMENT

BACKGROUND

TECH 8 outlines technical controls necessary to mitigate the risk of unauthorized access. Password management controls help protect information systems and data from unauthorized access. By implementing and enforcing effective password management controls, localities can reduce the risk of password-related cyberattacks, such as brute-force attacks, phishing attacks, and credential stuffing attacks. Password management controls comprise of technical and administrative controls. Technical controls refer to technologies such as password managers that help users create and manage strong passwords. Administrative controls include policies and procedures that govern password usage, including change requirements and sharing prohibitions. Localities should leverage multifactor authentication (MFA) to add an extra layer of security to login processes. MFA requires users to enter two or more factors of authentication, such as a password and a one-time code before accessing systems and data.

SCOPE

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

MATURITY MATRIX

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

1 Password Complexity

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

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

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

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

2 Password Management

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

2.2 Passwords are not shared.

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

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

2.5 Access to the password storage location is highly restricted.

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

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

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

TECH 9 – SYSTEM AND COMMUNICATION PROTECTION

BACKGROUND

TECH 9 outlines controls to implement boundary protection devices to monitor activity, traffic, and potential attacks; ensure appropriate encryption for data in transit and at rest; and outline requirements for wireless devices. Boundary protection controls must be designed to protect the internal networks and systems at localities from unauthorized access and attacks. These controls should be implemented at the perimeter of the locality's network, where it connects to the internet or other external networks. Boundary protection controls may include firewalls, intrusion detection system and prevention systems (IDS/IPS), and web-filtering solutions. Boundary protection controls work by filtering and blocking traffic between the internal and external networks based on predefined rules and policies. These rules and policies may be based on source and destination IP addresses, ports, protocols, etc. To enhance the effectiveness of boundary protection controls, localities should ensure these controls are implemented in a layered manner, with a combination of different types of controls. Localities must ensure that data at rest is encrypted, and all data in-transit is wrapped in secure protocols.

SCOPE

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

MATURITY MATRIX

TECH 9 – System and Communication Protection	Baseline	Preferred	Platinum
1. Boundary Protection	1.1- 1.3	All	All
2. Use of Cryptography	2.1-2.2	All	All
3. Wireless Devices	3.1-3.2	3.1-3.3	All

1 Boundary Protection

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

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

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

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

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

2 Cryptography

2.1 All information must be encrypted while in transit.

2.2 All sensitive data must be encrypted while at rest.

2.3 Digital signatures must be part of the encryption process.

3 Wireless Network

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

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

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

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

TECH 10 – SYSTEM AND INFORMATION INTEGRITY

BACKGROUND

TECH 10 addresses required malicious code protections, security alerts, advisories and directives, information system monitoring, backups, and recovery. System and information integrity safeguards are designed to protect the integrity of election systems and data. These safeguards help ensure that election systems are operating as intended and that the related election data is accurate and reliable. System and information integrity controls can be broadly classified into these four categories:

- Malicious code protection – controls designed to prevent, detect, and remove malicious code from information systems. These controls include antivirus software, intrusion detection and prevention systems (IDS/IPS), and application whitelisting.
- Security alerts and advisories – provide localities with information on security vulnerabilities and potential threats to elections systems and data. Information or insights from these alerts/advisories can be leveraged to prioritize system remediation efforts and mitigate the risk of security breaches.
- Information system monitoring – involves collecting and analyzing data about the performance, capacity, and security of information systems. This data can help localities to identify and respond to security incidents in a timely manner.
- Backup and recovery – ensure that data can be restored in the event of a data loss or corruption. Backup and recovery controls include regular backups, offsite data storage, and data recovery procedures.

Localities should layer these controls to mitigate the risk of security breaches even if one layer is compromised.

SCOPE

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

MATURITY MATRIX

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

1 Malicious Code Protection

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

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

2 Security Alerts, Advisories and Directives

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

2.2 Locality has implemented a process to automatically review security alerts, advisories, and directives and take appropriate action, including sharing the information with relevant stakeholders or implementing required security updates.

3 Information System Monitoring

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

3.1.1 Login Failures

3.1.2 Access exceptions

3.1.3 System exceptions

3.1.4 Operating System and Application patching

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

3.2.1 Login Failures

3.2.2 Access exceptions

3.2.3 System exceptions

3.2.4 Operating System and Application patching

4 Backup and Recovery

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

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

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

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

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

TECH 11 – ACCESS CONTROL

BACKGROUND

TECH 11 outlines requirements to prevent unauthorized user access by verifying and validating users are permitted to access the systems and data. Some of the requirements in this section include:

- Separation of duties – to ensure no single individual can perform all the tasks related to a process or transaction.
- Unsuccessful login attempts – to mitigate brute-force attacks or unauthorized access, monitor the number of unsuccessful logins attempts to information systems, and lock the system when the defined threshold is met.
- System use notification – to help deter users from malicious behavior by displaying messages that may include system security policy and consequences of unauthorized behavior or access.
- Least privilege – to ensure users are only granted privileges required to perform their assigned duties.
- Multifactor authentication – require users to use more than factor for authentication before access is granted. This adds an additional layer of protection from unauthorized access.

While not a specific requirement in this section, where feasible, localities should consider implementing identity and access management (IAM) systems that facilitate the management of user identities and access privileges. Localities should also consider the use of directories such as Microsoft's Active Directory in the management of access in their environments.

SCOPE

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

MATURITY MATRIX

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

1 Actively Manage Access

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

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

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

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

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

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

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

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

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

1.10Automate quarterly account reviews to ensure accounts for terminated personnel or accounts that have not been active in the last 90 days are disabled.

1.11List the role(s) a user will need to perform business functions on the application for a new user account. Applicants or assigned Supervisors must list the systems and groups the user needs, prior to account approval and creation.

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

2 Separation of Duties and Account Creation

2.1 Shared accounts and passwords are prohibited.

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

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

3 Access

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

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

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

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

4 Mobile Devices

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

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

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

5 Unsuccessful Logon Attempts

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

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

6 System Use Notification

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

6.1.1 Users are accessing a government or private information system.

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

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

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

TECH 12 – CONFIGURATION MANAGEMENT

BACKGROUND

TECH 12 outlines configuration management requirements designed to help mitigate the risk of unauthorized changes being introduced into information systems without proper approval. These controls are also essential in detecting configuration changes that have occurred and restoring systems to a known good state in the event of a security incident or system failure. Configuration management controls are particularly important for election-related systems, as these systems must be highly reliable and secure to ensure the integrity of the electoral process.

Localities must ensure that a baseline configuration, referred to as a known good state of a system that includes all installed software, security software, and configuration settings is maintained for each system component. Once a baseline configuration has been established, localities must implement change control practices to ensure that all changes to systems are authorized, documented, and tested. Change control procedures must include a process to review and approve proposed changes and test such changes before they are implemented in the production environment.

Specific examples of configuration management controls that localities can implement include:

- Establish a baseline configuration for each election-related system component – the baseline should include all installed software, security patches and configuration settings.
- Implement change control procedures – ensure all changes are documented, reviewed/approved, and tested.
- Use configuration management tools – to ensure all changes are properly documented and authorized.
- Perform regular reviews of system configuration – to detect unauthorized changes and ensure all system components are in a good known state.

SCOPE

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

MATURITY MATRIX

TECH 12 – Configuration Management	Baseline	Preferred	Platinum
1. Baseline Configuration for Elections Related Systems	1.1-1.3	1.1-1.4	All
2. Change Control	2.1	2.1	2.1

1 Baseline Configuration for Elections Related Systems

1.1 An inventory of hardware assets is maintained. The inventory should capture the following for hardware assets

1.1.1 Type of equipment

1.1.2 Manufacturer

1.1.3 Model

1.1.4 Serial Number
1.1.5 Manufacture Date

1.2 An inventory of software assets is maintained. The inventory should capture the following for software assets

1.2.1 Name of software
1.2.2 Software vendor
1.2.3 License quantity
1.2.4 License expiration

1.3 The baseline configuration for hardware and software is documented for each item on the inventory listed created in 1.1 and 1.2. This document is updated continually as configurations are changed,

1.4 Localities with locally maintained IT services must capture configuration information for hardware and software. Below is a list of configuration settings that are captured. This list is not intended to be exhaustive.

1.4.1 HARDWARE: Open Ports, White/Blacklist of IP Addresses, DNS Settings, Connected Devices, Installed Software, Installed OS, Security Policies, Processors, Memory, Diskspace

1.4.2 SOFTWARE: Home/Install Directory, Environment Variables/Paths, Memory Settings, CPU Settings, Plugins, Database Connections

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

1.5.1 Topology that captures components and their interconnections

1.5.2 Components, including their IP addresses and model or serial numbers

1.5.3 Configurations, including information on aspects such as the voter registration database

1.5.4 Information security mechanisms in place, including encryption and access control

1.5.5 Maintenance practices/procedures

1.5.6 Testing and certifications related to the system

2 Change Control

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

2.1.1 Description of the change that include information about the hardware or software being changed.

2.1.2 Who requested the change

2.1.3 Who is responsible for implementing the change

2.1.4 The date/time the change will be implemented

2.1.5 Who approved the change

2.1.6 ISO or person representing the ISO role approval

TECH 13 – MAINTENANCE

BACKGROUND

TECH 13 addresses maintenance of physical assets and locations, as well as software, providing documentation requirements to ensure external parties also comply. These controls are designed to ensure that election-related information systems and components are properly maintained and updated to keep them secure and operating as intended. The maintenance controls help prevent system failures, mitigate security vulnerabilities, and ensure the availability of election systems and data.

Maintenance controls can be classified as follows:

- Physical maintenance – involve the care and upkeep of the physical component of information systems, such as servers, workstations, network equipment, etc. Physical maintenance may include cleaning and inspecting equipment, replacing defective components, etc.
- Software maintenance – involve the updating and patching of software applications to keep them secure. Some of the related tasks include installing security patches, updating to new versions of software, and fixing bugs.
- Maintenance documentation – involve keeping a record of all maintenance activities that have been performed on information systems. Such documentation should include the date and time of maintenance activity, name of person who performed the maintenance, a description of the work that was performed, and any other information.

SCOPE

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

MATURITY MATRIX

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

1 Physical Maintenance

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

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

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

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

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

1.5 Equipment that is decommissioned must document the following:

1.5.1 Equipment decommissioned

1.5.2 Equipment Identification Number

1.5.3 Date/Time equipment decommissioned

1.5.4 Person(s) that decommissioned the equipment

1.5.5 Date/Time equipment was removed

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

1.6.1 Any equipment media is sanitized as per NIST or COV guidelines

1.6.2 Equipment default settings are restored

2 Software Maintenance

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

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

3 Maintenance Documentation

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

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

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

TECH 14 – SYSTEM AUDIT LOGS

BACKGROUND

TECH 14 works to ensure essential system activity records are captured, reviewed, and preserved. Localities must maintain system audit logs to help with the detection and investigation of security incidents, troubleshooting of system problems, and compliance with LESS requirements. System audit logs including user logins, file changes, and network traffic can be leveraged to identify suspicious or potentially malicious activity.

System log controls must be implemented in a manner that ensures security logs are generated, collected, stored, and analyzed in a secure manner. These controls should cover the lifecycle of audit logs including:

- Generation – ensure audit logs are configured and generated for all identified/defined system activities.
- Collection – logs are collected and stored in a secure/tamper-proof location.
- Storage – logs are stored for a sufficient period to support investigations of incidents.
- Analysis – logs are analyzed for suspicious activity and indicators of compromise (IOCs).

SCOPE

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

MATURITY MATRIX

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

1 Auditable Events and Automated Alerts

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

2 Review, Analysis and Retention

2.1 Audit records are backed up to a machine different than originating system on a quarterly basis.

2.2 Audit records are reviewed and analyzed every 30 days for inappropriate or unusual activity. Findings are reported using the Incident Response process.

2.3 Audit records, audit settings, and audit reports are protected from unauthorized access, modification, and deletion by setting appropriate access controls.

2.4 Retain audit records consistent with State and Local retention policies, to provide support for after-the-fact investigations of security incidents.

★ VIRGINIA ★

STATE BOARD of ELECTIONS

Stand By Your Ad Policy Revision

BOARD WORKING PAPERS

Tammy Alexander
ELECT Campaign Finance Compliance
and Training Supervisor

Steven Koski
ELECT Policy Analyst

★ VIRGINIA ★

STATE BOARD *of* ELECTIONS

Memorandum

To: Chairman O'Bannon, Vice-Chair Dance, Secretary Alvis-Long, Delegate Merricks, and Mr. Weinstein

From: Tammy Alexander, Campaign Finance Compliance and Training Supervisor
Steve Koski, Policy Analyst

Date: November 15, 2023

Re: *Stand By Your Ad* Policy Revision

Suggested Motion

"I move that the State Board of Elections directs Department of Elections staff to prepare a revised *Stand By Your Ad* Policy that: clarifies the scope of *Stand By Your Ad* to the types of advertisements expressly enumerated in the provisions of Chapter 9.5 of Title 24.2; makes necessary revisions to ensure due process in *Stand By Your Ad* proceedings; and requires *Stand By Your Ad* hearings be conducted twice per year."

Applicable Law

Title 24.2, Chapter 9.5 of the Code of Virginia (§ 24.2-955 *et seq.)* ("Stand By Your Ad") ("SBYA").

- § 24.2-955 of the Code of Virginia creates disclosure requirements that apply to "any sponsor of an advertisement in the print media, on radio or television, or placed or promoted for a fee on an online platform …."
- § 24.2-955.1 of the Code of Virginia defines "advertisement", in relevant part, as "any message appearing in the print media, on television, on radio, or on an online platform," not including "novelty items authorized by the candidate including, but not limited to, pens, pencils, magnets, and buttons to be attached to wearing apparel."

Background

The current SBYA Hearings Policy was approved by the State Board of Elections ("SBE") on February 23, 2021 ("current policy") (*see* Attached). The current policy states that, in determining the applicability of SBYA to an advertisement, it should be evaluated to determine whether it:

- Constitutes an advertisement subject to SBYA; and
- Expressly advocates for the election or defeat of a clearly identified candidate (*see* Attached, p. 5).

Under 1VAC20-90-30, "expressly advocating" means:

> *[A]ny communication that uses phrases such as "vote for," "elect," "support," "cast your ballot for," "Smith for Congress," "vote against," "defeat," "reject," or any variation thereof or any communication when taken as a whole and with limited reference to external events, such as the proximity to the election, that could only be interpreted by a reasonable person as containing advocacy of the election or defeat of one or more clearly identified candidates because (i) the electoral portion of the communication is unmistakable, unambiguous, and suggestive of only one meaning and (ii) reasonable minds could not differ as to whether it encourages actions to elect or defeat one or more clearly identified candidates.*

Relevant to this memorandum, the current policy also:

- Sets January and August as the months at which the SBE must hear SBYA complaints (*see* Attached, p. 3); and
- Provides a process by which a respondent to a complaint may request the issuance of a subpoena by the SBE (*see* Attached, p. 4).

Issues with Current Policy

Scope of Stand By Your Ad

In recent SBYA proceedings, questions have been raised about the scope of applicability of SBYA to advertisements, particularly in relation to print media. Under § 24.2-955.1 of the Code of Virginia, "print media" is defined, in relevant part, as:

> *[B]illboards, cards, newspapers, newspaper inserts, magazines, printed material disseminated through the mail, pamphlets, fliers, bumper stickers, periodicals, websites, electronic mail, non-video or non-audio messages placed or promoted for a fee on an online platform, yard signs, and outdoor advertising facilities.*

Under the current policy, ELECT has brought before the SBE all SBYA complaints related to printed materials that contain express advocacy for or against a clearly identified candidate, including printed materials beyond those specifically enumerated in the definition of "print media" in § 24.2-955.1. For example, while items like t-shirts, caps, banners, vehicle wraps, and large car magnets are not specifically enumerated in the definition of "print media," they have been subject to the disclosure requirements in SBYA and the complaint process. The SBE has indicated its desire review the required scope of SBYA to ensure that only advertisements expressly covered by the statute are subject to the SBYA complaint process.

SBYA Policy Process Revisions

Upon receipt of a subpoena request for a recent SBYA hearing, it was determined that process revisions of the current policy would better ensure full due process of participants. ELECT staff is in the process of reviewing the current policy to ensure that the SBYA hearing process fully complies with all legal requirements and is in line with standard practices for similar administrative hearings in Virginia.

SBYA Hearing Dates Adjustment

SBYA does not provide requirements related to the timing of the submission and hearing of complaints. Currently, the hearing dates for SBYA are fixed for the SBE meetings held in January (for complaints received July 1 to November 30) and August (for complaints received December 1 to June 30). Providing a more flexible timeframe for scheduling the SBYA hearings, while still requiring two hearings per year, would have the following benefits:

- Allow for more time to process all SBYA complaints following the June Primary and November General Elections;
- Ensure that participants have ample time to fully participate in the process (including when a subpoena is requested); and
- Allow greater flexibility for the SBE in setting meeting dates.

A revision to the current policy to allow this flexibility would still ensure that SBYA hearings are held in a timeframe that complies with all other aspects of Virginia law.

Recommendation

ELECT recommends that the SBE directs ELECT to do the following:

- Prepare for the SBE's consideration a revised SBYA Policy that:
    - Clarifies the scope of SBYA to advertisements;
    - Makes necessary revisions to ensure due process in SBYA proceedings; and
    - Requires two SBYA hearing dates per year.

Attachments

Stand By Your Ad Hearings Policy 2021-001 (February 23, 2021)

State Board of Elections Policy 2021-001

A meeting of the Virginia State Board of Elections (SBE) was held on February 23, 2021, during which the following policy was proposed by the Department of Elections (ELECT) and approved by the Board:

STAND BY YOUR AD HEARINGS

WHEREAS, Virginia Code § 24.2-955.3(D) provides that the SBE shall conduct a public hearing to determine whether to find a violation of Chapter 9.5 of Title 24.2 (commonly known as "Stand By Your Ad" or "SBYA") and, if the SBE finds a violation of that chapter, shall assess civil penalties in accordance with that section: now therefore let it be

RESOLVED, by the SBE under its authority to issue rules and regulations to promote the proper administration of election laws and obtain uniformity in the administration of elections pursuant to Va. Code § 24.2-103(A) that:

The policy entitled "State SBE of Elections Policy 2018-001" is rescinded; and

The below policy applies to the conduct of SBYA hearings held pursuant to Va. Code § 24.2-955.3(D).

Definitions

- "Clearly identified" means the candidate's name, nickname, photograph, or drawing or the identity of the candidate is otherwise apparent—
  - through an unambiguous reference, such as the candidate's initials (ex. FDR), nickname (ex. Ike), office (ex. "the Governor"); or
  - through an unambiguous reference to their status as a candidate such as "the Democratic Senate nominee for District 5".
- "Complainant" means the filer of a complaint.
- "Express advocacy" has the meaning given the term in 1 Va. Admin. Code 20-90-30.
- "Occurrence" means—
  - one broadcast of a radio or television political campaign advertisement[1]; or
  - with respect to print media, one print media political campaign advertisement.
- "Respondent" means a person that is the subject of a complaint.

Complaints

- SBYA is silent as to the submission process for complaints.
- Complaints may be submitted to ELECT online on the ELECT website, by sending an email to SBYA@elections.virginia.gov, or by mailing in a complaint form.

[1] Section 24.2-955.1.

- A complainant shall be notified upon submitting a complaint that the complainant may be required to appear or to produce evidence at a hearing arising from the complaint, as required under Va. Code § 2.2-4020(C).
- To allege a violation of SBYA, a complaint must contain all of the following—
    - The name of the complainant and the respondent;
    - A statement of the alleged violation; and
    - Evidence of the alleged violation, including—
        - In the case of print media, typically photographic evidence; or
        - In the case of radio or television, the complaint should identify the station and time at which the advertisement was aired.
- If the disputed conduct does not allege a violation of SBYA, ELECT will provide notice of receipt of the complaint to the complainant, but will recommend that the SBE takes no action.
- Upon receipt of a complaint containing sufficient evidence to allege a violation of SBYA, ELECT shall investigate the complaint.

Notice

Method

- If a person is alleged to have violated SBYA, ELECT shall provide notice to the respondent via certified mail not later than 10 days before the date on which a hearing on the matter will be held.[2]
- If the respondent is a registered voter, ELECT shall send such notice via certified mail to the most recent physical address provided in the respondent's voter registration statement.
- If the respondent is a registered committee, ELECT shall send such notice via certified mail to the most recent physical address provided in the respondent's statement of organization.
- If ELECT is aware of an electronic mail address for the respondent, ELECT shall also send such notification via electronic mail.

Contents

- Each notice shall include—
    - The time[3], date[4], location[5], and nature of the hearing[6];
    - The basic law under which the SBE contemplates its possible exercise of authority[7];
    - The matters of fact and law asserted or questioned by the SBE[8], including an explanation of the alleged violation[9];

[2] Section 24.2-955.3(D).

[3] Sections 24.2-955.3(D) and 2.2-4020(B).

[4] *Id.*

[5] Section 2.2-4020(B).

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Section 24.2-955.3(D).

    - A statement of the maximum civil penalty that may be assessed with respect to the alleged violation;[10]
    - Contact information consisting of the name, phone number, and government email address of the person designated by the SBE to respond to questions or otherwise assist a named party;[11] and
    - Notice that a default order may be issued pursuant to Va. Code § 2.2-4020.2(A) against the respondent if the respondent fails without good cause to attend or appear at the hearing and, if such a default order is issued, the SBE may conduct all further proceedings necessary to complete the hearing without the defaulting respondent's presence at the hearing.[12]

Hearings

Timing of Hearings

- The SBE will meet in January of each year to consider SBYA complaints received between the previous July 1 and November 30.
- The SBE will meet in August of each year to consider SBYA complaints received between the previous December 1 and June 30.

Rights of respondents

- A respondent shall be entitled to—
    - Be accompanied by and represented by counsel;
    - Submit oral and documentary evidence and rebuttal proofs;
    - Conduct such cross-examination as may elicit a full and fair disclosure of the facts; and
    - Have the proceedings completed and a decision made with dispatch.[13]
- A respondent shall be given the opportunity to, on request and before the recommendations of ELECT are presented, submit in writing for the record—
    - Proposed findings and conclusions; and
    - Statements of reasons for the proposed findings and conclusions.[14]
- If a respondent intends to conduct cross-examination of any person at the hearing, the respondent shall provide reasonable notice of such proposed cross-examination to the SBE prior to the hearing.

Rights of the Board

- The SBE may—
    - Administer oaths and affirmations;
    - Receive probative evidence;
    - Exclude irrelevant, immaterial, insubstantial, privileged, or repetitive proofs, rebuttal, or cross-examination;
    - Rule upon offers of proof;

[10] *Id.*

[11] Section 2.2-4020(B)

[12] Section 2.2-4020.2(B).

[13] Section 2.2-4020(C).

[14] Section 2.2-4020(D).

    - Oversee a verbatim recording of the evidence;
    - Hold conferences for the settlement or simplification of issues by consent;
    - Dispose of procedural requests; and
    - Regulate and expedite the course of the hearing.[15]

Default orders

- If a respondent without good cause fails to attend or appear at a hearing, the SBE may issue a default order against the respondent.[16]
- If the SBE issues a default order, the SBE may conduct all further proceedings necessary to complete the hearing without the defaulting respondent's presence at the hearing.[17]
- Not later than 15 days after the SBE gives notice to a respondent subject to a default order that an initial or final order has been rendered against the respondent, the respondent may petition the SBE to vacate the order.[18]
    - If good cause is shown for the respondent's failure to appear, the SBE shall vacate the order and, after proper service of notice, conduct another hearing.[19]
    - If good cause is not shown for the respondent's failure to appear, the SBE shall deny the motion to vacate.[20]

Continuance

- A scheduled hearing shall not be delayed by the inability of the respondent to attend the hearing unless a request for a continuance is made in writing to the SBE not less than 7 days before the scheduled hearing date.
- A continuance shall not be granted unless the request, in the opinion of the Chair, sets forth good and sufficient cause for the continuance.
- If a continuance is granted, ELECT staff shall notify all members of the SBE and document the grant in the official record of the meeting for continuity.

Subpoenas

- The SBE may, and on the request of a respondent shall, issue a subpoena requiring testimony or the production of other evidence.[21]
- Any person who receives a subpoena issued by the SBE to appear or produce evidence with respect to a hearing and who objects to the subpoena may procure by petition a decision on the validity of the subpoena in the Circuit Court for the City of Richmond.[22]
- If any person refuses or neglects to comply with a subpoena issued by the SBE with respect to a hearing, the SBE may procure an order of enforcement from the Circuit Court for the City of Richmond.[23]

[15] Section 2.2-4020(C).

[16] Section 2.2-4020.2(A).

[17] Section 2.2-4020.2(C).

[18] Section 2.2-4020.2(E).

[19] *Id.*

[20] *Id.*

[21] Section 2.2-4022.

[22] See *id.*

[23] *Id.*

Interpreter services

- If an interpreter is required, ELECT will make appropriate arrangements to ensure an interpreter is present during the hearing.

Presentation of complaints

- With respect to each complaint, ELECT shall present information to assist the SBE in making a determination as to whether a violation has occurred and, if so, the civil penalty that should be assessed, and the respondent shall be entitled to appear and present information in response.
- In presenting each complaint, ELECT shall include—
    - The evidence submitted regarding the complaint and such other evidence as ELECT discovered during its investigation of the complaint;
    - The names of the complainant and the respondent;
    - The provision of SBYA that the respondent is alleged to have violated;
    - The manner in which SBYA is alleged to have been violated;
    - The date of the alleged violation;
    - Whether the respondent has previously violated SBYA during any election cycle;
    - The manner in which the complaint was received (i.e. online, via USPS, via FedEx, etc.);
    - A statement of whether any written explanation or proposed findings and conclusions, and statements of reasons for the proposed findings and conclusions, have been received from the respondent; and
    - The action that ELECT recommends the SBE take with respect to the complaint, including the amount of civil penalty to be assessed if ELECT recommends finding that a provision of SBYA has been violated.

Initial decision

- At a hearing at which a complaint is presented, after the complaint is presented, the SBE shall—
    - Carry out further deliberation as necessary; and
    - Conduct a vote relating to an initial decision as to whether a violation has occurred and, if so, the civil penalty that should be assessed.
- To assess a civil penalty for a violation of SBYA, the SBE must find that SBYA requirements apply to the communication in question, and that the communication fails to comply with SBYA requirements.
    - The SBE should consider whether the communication—
        - constitutes an advertisement subject to SBYA; and
        - expressly advocates for the election or defeat of a clearly identified candidate.
    - Upon such finding, the SBE may then determine whether the advertisement complies with SBYA disclosure requirements, and if not, what civil penalty to assess.

- An initial decision of the SBE may be modified or vacated subject to the requirement that a final decision shall be rendered not later than 90 days after the date on which the hearing occurs.

Final decisions

- The SBE shall render any final decision not later than 90 days after the date on which a hearing occurs.[24]
- The SBE shall provide notice to the respondent not later than 5 days after the date of its final decision,[25] and such notice shall be signed by the SBE and served upon the respondent by mail.[26]
- The original signed copy of a final decision of the SBE shall remain in the custody of the agency as a public record.[27]
- A decision shall briefly state—
  - The findings, conclusions, reasons, or basis therefor upon the evidence presented by the record and relevant to the basic law under which the agency is operating;
  - The appropriate order for a penalty under Va. Code § 24.2-955.3 or denial thereof; and [28]
  - The time for filing a notice of appeal under Va. S.Ct. Rule 2A:2.

Reconsideration

- A respondent may file a petition for reconsideration with the SBE of a final decision of the SBE made pursuant to Va. Code § 2.2-4020.[29]
- A petition for reconsideration shall be filed with the SBE not later than 15 days after service of the final decision.[30]
- A petition for reconsideration shall include—
  - A full and clear statement of the facts pertaining to the reasons for reconsideration;
  - The grounds in support thereof; and
  - A statement of the relief desired.[31]
- Not later than 30 days after the date on which the SBE receives a respondent's timely petition for reconsideration, the SBE shall render a written decision on the petition, which shall—
  - Deny the petition;
  - Modify the case decision; or
  - Vacate the case decision and set a new hearing for further proceedings.[32]

[24] Section 2.2-4021(B).
[25] *Id.*
[26] Section 2.2-4023.
[27] *Id.*
[28] See 2.2-4020(E).
[29] Section 2.2-4023.1(A).
[30] *Id.*
[31] *Id.*
[32] Section 2.2-4023.1(B).

- The SBE may reconsider a final decision on its own initiative for good cause within 30 days of the date of the final decision.[33]

[33] Section 2.2-4023.1(E).

★ VIRGINIA ★
STATE BOARD of ELECTIONS

Risk Limiting Audit Drawing

- Overview of Process
- Selecting a General Assembly Contest for RLA; Generating the Random Seed Number for RLA; and Setting the Risk Limit.
- Approving Local Races for RLA, Setting the Risk Limit, Generating the Random Seed Number for RLA, and Setting the Dates for both RLAs.

BOARD WORKING PAPERS

Rachel Lawless
ELECT Confidential Policy Advisor

Claire Scott
ELECT Policy Analyst

Londo Andrews
ELECT Voting Systems Security Program Manager

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Memorandum

To: Chairman O’Bannon, Vice-Chair Dance, Secretary Alvis-Long, Delegate Merricks, and Mr. Weinstein

From: Claire Scott, Policy Analyst, Londo Andrews, Voting Systems Security Manager

Date: November 15, 2023

Re: Selecting a General Assembly Contest for the RLA; Generating the Random Seed Number for the RLA; and Setting the Risk Limit

---

Suggested Motions:
“I move that the State Board of Elections direct ELECT staff to generate the random seed numbers for the randomly selected General Assembly district race.”

“I move the State Board of Elections to set the risk limit to 10% for the Risk-Limiting Audit for the randomly selected General Assembly district race for the November 2023 general election.”

Applicable Code Section:
§24.2-671.2 Risking-Limiting Audits

Overview
Pursuant to §24.2-671.2, the State Board of Elections (SBE) determines the contested races that will conduct a Risk-Limiting Audit (RLA). For the November 2023 General Election, a General Assembly district race, either from the House of Delegates or the Senate, will be randomly selected for an RLA. RLAs conducted pursuant to this section will be performed by local Electoral Boards and general registrars under the supervision of the Department of Elections (ELECT).

Selecting a Random General Assembly District Race
The member(s) of the SBE will randomly select a General Assembly district race for an RLA. A list of eligible General Assembly district races has been attached to this memorandum for consideration.

ELECT has placed the eligible district races, for both the House of Delegates and the Senate, on raffle tickets in a tumbler. Each ticket has a different qualifying General Assembly district race. The Chair of the SBE will turn the tumbler, mixing the General Assembly district races, and the

Vice-Chair of the SBE will then select a single raffle ticket out of the tumbler and state the selected district.

ELECT staff recommends selecting the random General Assembly district race in accordance with the instructions provided in this memorandum.

Generating a Random Seed Number Randomly Selected General Assembly District Race

The RLA software uses a 20-digit random seed number to generate a random sequence of ballots to be selected for retrieval. This seed number is created by rolling a 10-sided die 20 times and recording each number. The 20-digit number generated by this activity will be inputted into the RLA software by the RLA Administrator and used for the races previously selected. Once this number is inputted, the auditing software will randomly select and generate a list of ballots to be retrieved based on the sample size.

ELECT staff recommends having staff members roll a 10-sided die 20 times to generate the random seed number.

Setting the Risk Limit

Pursuant to §24.2-671.2(F), the SBE will set the risk limit for the RLA. A risk limit is the maximum chance that the RLA will fail to correct an incorrectly reported outcome. For example, a 10% risk limit means that there is a 90% chance that the RLA will correct an incorrect outcome. Every RLA that has been held in the Commonwealth of Virginia has used a 10% risk limit.

ELECT recommends that the risk limit be set to 10% for the randomly selected General Assembly district race.

Attachment:

- List of Eligible General Assembly Races

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Memorandum

To: Chairman O'Bannon, Vice-Chair Dance, Secretary Alvis-Long, Delegate Merricks, and Mr. Weinstein

From: Claire Scott, Policy Analyst, Londo Andrews, Voting Systems Security Manager

Date: November 15, 2023

Re: Approving Local Races for an RLA; Generating the Random Seed Number; Setting the Risk Limit; and Setting the Dates of the RLA

Suggested Motions:

"Pursuant to §24.2-671.2(D) and 1VAC20-60-80, I move that the State Board of Elections approve the SBE24.2-671.2(D) Form(s) as presented and grant a two-week extension of the local Electoral Board's certification deadline under §24.2-671."

"I move that the State Board of Elections direct ELECT staff to generate the random seed numbers needed to conduct the Risk-Limiting Audit(s) for the approved races."

"I move the State Board of Elections to set the risk limit to 10% for the Risk-Limiting Audit(s) to be performed pursuant to §24.2-671.2(D)."

Applicable Code Sections:

§24.2-671.2 Risk-limiting audits; 1VAC20-60-80 Request for a risk-limiting audit for a contested race within a jurisdiction

Approving Local Races Applied for by Local Electoral Boards

Pursuant to §24.2-671.2(D) and 1VAC20-60-80 of the Code of Virginia, a local Electoral Board may request a Risk-Limiting Audit (RLA) for a local contested race wholly contained within their jurisdiction, by submitting the SBE 24.2-671.2(D) Form. The SBE must grant the request if all the requirements and conditions outlined in the regulation are met. The approved RLA(s) will be performed by the local Electoral Boards and general registrars under the supervision of the Department of Elections (ELECT).

These are the SBE-671.2(D) Forms that have been submitted and meet the requirements of 1VAC20-60-80:

Locality	Race	Margin

ELECT staff recommends approving the requested RLAs pursuant to §24.2-671.2(D) and 1VAC20-60-80 of the Code of Virginia.

Granting Certification Extensions to Local Electoral Boards for the RLAs Approved Pursuant to §24.2-671.2(D)

Pursuant to §24.2-671.2(D) and 1VAC20-60-80, the SBE may grant an extension not to exceed two weeks of the local Electoral Board's certification deadline for those who have applied for an

RLA. This is to allow local Electoral Boards time to prepare for and execute the RLA in addition to submitting their abstracts for certification by the SBE.

ELECT staff recommends granting a two-week extension for the presented races pursuant to §24.2-671.2(D) and 1VAC20-60-80 of the Code of Virginia.

Generating a Random Seed Number for the Selection of Ballots to be Audited in the RLA Pursuant to §24.2-671.2(D)

The RLA software uses a 20-digit random seed number to generate a random sequence of ballots to be selected for retrieval. This seed number is created by rolling a 10-sided die 20 times and recording each number. The 20-digit number generated by this activity will be inputted into the RLA software by the RLA Administrator and used for the races previously selected. Once this number is inputted, the auditing software will randomly select and generate a list of ballots to be retrieved based on the sample size.

ELECT staff recommends having staff roll a 10-sided die 20 times to generate the random seed number.

Setting the Risk Limit

Pursuant to §24.2-671.2(F), the SBE will set the risk limit for the RLA. A risk limit is the maximum chance that the RLA will fail to correct an incorrectly reported outcome. For example, a 10% risk limit means that there is a 90% chance that the RLA will correct an incorrect outcome. Every RLA held in the Commonwealth of Virginia has used a 10% risk limit.

ELECT recommends that the risk limit be set to 10% for any approved race using the SBE 671.2(D) Form.

Setting the Dates of the RLA(s)

Pursuant to §24.2-671.2(G), ELECT will set the dates for the RLAs. The RLAs selected and approved during this meeting will begin on Monday, November 27th at 9 AM and will be completed before Monday, December 4th. Notice of the start date, time, and locations for the RLAs will be posted on ELECT's website.

Attachment(s):

- SBE-671.2(D) Form(s) Submitted for Approval